TLfDI

Thüringer Landesbeauftragter
für den Datenschutz und die Informationsfreiheit



12. Tätigkeitsbericht zum Datenschutz: Öffentlicher Bereich

12. Tätigkeitsbericht zum Datenschutz: Öffentlicher Bereich

des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit

Berichtszeitraum: 1. Januar 2016 bis 31. Dezember 2017
Zitiervorschlag: 12. TB LfDI Thüringen

Der 12. Tätigkeitsbericht steht im Internet unter der Adresse www.tlfdi.de zum Abruf bereit.

Erfurt, im Dezember 2017

Dr. Lutz Hasse
Thüringer Landesbeauftragter für den Datenschutz
und die Informationsfreiheit

Inhaltsverzeichnis

Vorwort 19

1. Schwerpunkte im Berichtszeitraum 22

2. Allgemeine Entwicklungen im Datenschutz 27
2.1 Spitze der Bewegung: Arbeitskreis (AK) Datenschutz und Bildung und Unterarbeitskreis (UAK) Datenschutz und Schule 27
2.2 Runder Tisch Medienkompetenz 32
2.3 Gesetz zur Neuregelung des Mikrozensus 34
2.4 Videoüberwachung im privaten und öffentlichen Raum – der TLfDI berät in jedem Einzelfall gern, gerade auch zur neuen Rechtslage der Datenschutz-Grundverordnung 35
2.5 Thüringer Meldeverordnung 39

3. Europäischer und Internationaler Datenschutz ... 41
3.1 Die Datenschutz-Grundverordnung (DS-GVO) kommt 41
3.2 Das neue BDSG – eine schwere Geburt 47
3.3 Umsetzung JI-Richtlinie in nationales Recht 50
3.4 EU-US-Privacy Shield – vom unsicheren Hafen ([un-] Safe Harbor) zum löchrigen Schutzschild! 54
3.5 Verabschiedung des Fluggastdatengesetzes der Bundesregierung – Privatsphäre von Reisenden adé . 58
3.6 Anpassung des ThürDSG an die DS-GVO – auf dem Weg in den Thüringer Landtag 59

4. Neue Medien – Rundfunk – Telekommunikation . 64
4.1 Heiße Debatte um den Entwurf einer EU-e-Privacy-Verordnung 64
4.2 Google-Analytics 66
4.3 Pflichten sozialer Netzwerke 67
4.4 Datenweitergabe aus dem Melderegister 69
4.5 Die DS-GVO hat auch Auswirkungen auf den Mitteldeutschen Rundfunk (MDR) 71
4.6 Wenn Kühlschränke eiskalt angreifen 73

5. Landtag 76
5.1 Erhebung der Personalausweisnummer von Besuchern des Thüringer Landtages zum Zwecke der Einlasskontrolle 76
5.2 Auskunftsverpflichtung des Landesamtes für Statistik? 77
5.3 Freier W-LAN-Zugang im Thüringer Landtag doch nicht frei 80
5.4 Zuständig oder nicht zuständig, das ist hier die Frage – Unterschriftenlisten auf dem Abgeordneten-Twitter-Account 81

6. Kommunales 84
6.1 Reichsbürger – Datenübermittlung an den Verfassungsschutz 84
6.2 Live-Streaming von Stadtratssitzungen 86
6.3 „Meininger Streetview“ 87
6.4 Problematische Betriebsvereinbarung zu einem GPS-System 89
6.5 Vom Winde verweht ... – Aufgefundene Dokumente von Stadt und Landkreis im Umfeld eines Papierentsorgungsunternehmens 90
6.6 Demokratieverständnis eines Bürgermeisters versus Rechtslage 92
6.7 Sehr beliebt: das Posten von Unterschriftenlisten 95
6.8 Einwohnermeldeamt: Einvernahme von Minderjährigen als Zeugen 96
6.9 Videoüberwachung im Internat – Videogaga 1 99
6.10 Videogaga 2 – Gefilmter Müll 103
6.11 Videoüberwachung durch eine Ampelanlage in Erfurt? 104
6.12 Videoüberwachung durch Stadtverwaltung 105
6.13 Videoüberwachung mittels Webcam? 106
6.14 Videoüberwachung und -aufzeichnung im Stadtgebiet – per Gesetz auch für die Ordnungsbehörde erlaubt 108
6.15 Abwahl eines Bürgermeisters nach § 28 Absatz 6 ThürKO – Transparenz versus Schutz personenbezogener Daten 109

6.16 Schwachstelle Internet: Veröffentlichung personenbezogener Daten in Amtsblättern eines Landkreises 116
6.17 Biene Maja oder Captain Chaos? – Anzeige von Namen auf elektronischer Anzeigetafel 117
6.18 Fotosafari im Schlafzimmer – Folge 2 118
6.19 Was darf die Meldebehörde nach dem Bundesmeldegesetz? 119
6.20 Keine Auskunft vom Einwohnermeldeamt: ein Missverständnis 122
6.21 Glückwunschschreiben vom Oberbürgermeister zur Schuleinführung: nicht gewünscht und datenschutzrechtlich unzulässig! 124
6.22 Nebenkostenschuldner einer Wohnungseigentümergesellschaft wird von der Verwaltungs-GmbH verpetzt 125
6.23 Ausspionieren eines Facebook-Accounts durch einen Mitarbeiter einer Wohnungsbaufirma? 128
6.24 Videokamera in der Gemeinde Piesau – reloaded 129
6.25 Speicherung von personenbezogenen Daten bei der Vergabe eines roten Kennzeichens 130
6.26 Ein wichtiger Schritt zur Integration: TLfDI hilft 132
6.27 Angst vor waffenbesitzendem Ehemann 133
6.28 „Offene“ Unterschriftensammlung zur Kreisfreiheit im Einkaufscenter 135
6.29 Information der Gemeinde an das Kreditinstitut wegen beabsichtigter Kontopfändung? 137
6.30 „Falsch geschwärzte“ Daten bei der Stadt Jena 138
6.31 Pistole auf die Brust: Vorkaufsrecht gegen Begleichung der Steuerschuld 139
6.32 KoWo kooperativ! 140
6.33 Anfrage zur geplanten Identifikationskarte für Geflüchtete 146
6.34 Wenn das Jugendamt Erkundigungen einzieht 149
6.35 Persönliche Daten vor Gericht 151
6.36 Herausgabe der Liste von Gewerbesteuerzahlern an den Bürgermeister – datenschutzrechtlich zulässig? 152
6.37 Manipulationen am USB-Stick einer Kindergartenmitarbeiterin? 153
6.38 Keine Daten bei Hundebiss? 154

6.39 Nichtlöschbarkeit personenbezogener Daten im Internet....155
6.40 Weiterleitung einer Beschwerde-E-Mail von Behörde zu Behörde....156
6.41 Datenübermittlung gem. § 9 ThürUIG – TLfDI nicht zuständig....157
6.42 Ordnungswidrigkeitsverfahren gegen Stadtratsmitglieder....158
6.43 Was weiß die Stadtverwaltung?....158
6.44 Anfrage zur etwaigen Anonymität von Zeugen....160
6.45 Foto von der Teilnehmerliste einer Bürgerversammlung: Was macht der Bürgermeister? 162
6.46 Beschwerde über die Übermittlung eines Wertgutachtens....163
6.47 Betreibermodell für das Handyparken....165
6.48 Wasser- und Abwasserzweckverband will es wissen 167
6.49 Datenschutz beim Theater....169
6.50 Unberechtigte Speicherung, Nutzung und Auswertung von Druckerdaten im Linienverkehr einer kommunalen Busgesellschaft?....170
6.51 Neues Personalausweis-Gesetz: Daten in Hülle und Fülle für den Staat....172

7. Personaldaten....174
7.1 Kein Einblick in den kompletten Mutterpass....174
7.2 Personalakten oder die wundersame Datenvermehrung 177
7.3 Mitarbeiter krank? – Da fragen wir doch mal den Arzt! 179
7.4 Der mitteilsame Amtsarzt....183
7.5 Doppelte Kontrollen der Arbeitszeit zulässig? 185
7.6 Personalnachrichten am schwarzen Brett im Kindergarten: TLfDI sieht schwarz....187
7.7 KollegInnen müssen nicht alles wissen....189
7.8 Ausscheiden aus dem Dienst: An die große Glocke? 191
7.9 Aufnahme von Disziplinarvorgängen in die Personalakte....193

7.10 Aufzeichnungen und Auswertung von Telefongesprächen in einer Rettungsleitstelle 195
7.11 Ist denn auch genug Personal da?.....197
7.12 Namen an den Amtsstuben.....199
7.13 Daten gegen Fördermittel.....201
7.14 Dienstvereinbarung zur elektronischen Kommunikation: dienstlich und privat dem Datenschutz verpflichtet.....202
7.15 Beschwerde über Zugriff auf Personalakten beim Landgericht.....204
7.16 Der Justiz-Postweg einer „vertraulichen Personalsache“.....206
7.17 Die Stadtverwaltung als Personalvermittler: (kein) Datenschutz für Bewerbungsunterlagen.....209

8. Polizei.....212
8.1 Immelborn – Ad Acta: Zwischenbericht des Untersuchungsausschusses 6/2 liegt jetzt vor: Handeln des TLfDI rechtmäßig – Amtshilfeverweigerung durch das ehemals CDU-geführte Innenministerium rechtswidrig!.....212
8.2 Wer hört wann, wo und auf welcher Rechtsgrundlage mit? – Aufzeichnung von Telefonaten auf den Dienstapparaten der Thüringer Polizei.....213
8.3 Wer kopiert oder importiert Daten bei PCs der Polizei? – DeviceWatch weiß alles.....218
8.4 Gemeinsames Kompetenz- und Dienstleistungszentrum auf dem Gebiet der polizeilichen Telekommunikationsüberwachung....221
8.5 "Bodycams" in der Thüringer Polizei.....223
8.6 Erste gemeinsame Kontrolle der bundesweiten Rauschgiftdatei durch die Datenschutzbeauftragten von Bund und Ländern.....226
8.7 Kopie des Personalausweises zulässig?.....227
8.8 Keine beglaubigte Kopie des Personalausweises für Auskunftsersuchen beim TLKA.....229
8.9 Elektronische Fußfesseln und der Datenschutz.....231
8.10 Fallbearbeitungssystem der Polizei – auch hier gilt Datensparsamkeit – Teil 2.....231
8.11 Presse als Facebook-Fahnder?.....232

8.12 DNA-Datei und Datenschutz – Teil 2 233
8.13 Funkzellenabfrage durch Privatunternehmen? 235
8.14 Eine Polizeibeamtin auf Abwegen 236
8.15 Polizeiproblem: Kontaktdaten von Journalisten 238
8.16 Verdienstausfall durch Zeugenaussage: In welchem Umfang sind personenbezogene Daten Dritter anzugeben? 241
8.17 Ermittlungsverfahren gegen Faschings-Cowboy 244
8.18 Kindeswohl steht an erster Stelle – auch für den Datenschutz 246
8.19 Datenerhebung der Behörde = Datenübermittlung des Unternehmens 248
8.20 Polizeiliche Akten nicht beim TLfDI 250
8.21 Polizeivideo bei Facebook 250
8.22 Landrat im Zentrum der Daten 251

9. Verfassungsschutz 251
9.1 Stellungnahme des TLfDI gem. § 5 Abs. 2 Satz 4 Thüringer Verfassungsschutzgesetz 254
9.2 Kontrollen der Antiterrordatei beim Thüringer Landeskriminalamt und beim Amt für Verfassungsschutz 256

10. Finanzwesen 258
10.1 Thüringer Verwaltung wird digital 258

11. Justiz 262
11.1 „Moha“: Nur Essensgewohnheit oder doch ein Rückschluss auf das Glaubensbekenntnis 262
11.2 Datenschutzrechtliche Belange gelten auch für Bescheide der Staatsanwaltschaft 265
11.3 Insolvent – und alle wissen es 266
11.4 Sichere Telearbeitsplätze für Richter und Staatsanwälte 269
11.5 Akteneinsicht bei der Staatsanwaltschaft – aber nur mit Rücksicht auf die schutzwürdigen Interessen der Beschuldigten 270
11.6 Datenlöschung aus dem Zentralen Staatsanwaltlichen Verfahrensregister: Fehlanzeige 272

11.7 Ein behördlicher Datenschutzbeauftragter für das Amtsgericht? 274
11.8 Richterliche Unabhängigkeit für TLfDI unantastbar 275
11.9 Personalakte: Übermittlungsersuchen eines Gerichts 276
11.10 Adressenverkauf durch das Grundbuchamt? 277

12. Gesundheits- und Sozialdatenschutz 279
12.1 Krebsregistergesetz – datenschutzgerecht?! 279
12.2 Staatsvertrag zum epidemiologischen Krebsregister 282
12.3 Wearables und Gesundheits-Apps immer datenschutzkonform? 283
12.4 Arbeitsvermittlung gegen Datensammlung 284
12.5 Patientenportal – modern, aber datenschutzgerecht? 286
12.6 Integrierte Teilhabeplanung als App – Kontrolle vor Ort 288
12.7 Biete medizinische Werbung, suche ärztliche Daten … 291
12.8 Wenn das Amt die Miete zahlt – der Vermieter erfährt alles, oder? 293
12.9 Reha-Entlassungsbericht: Daten an den MDK? 295
12.10 Löschungsresistente Daten im Gesundheitsamt – Teil 2 296
12.11 Alte Arztstempel – die Lizenz zur Rezeptausstellung? 298
12.12 Urkundenverifikationsdienst Approbationsurkunden 299
12.13 Qualität versus Datenschutz im Gesundheitswesen? 301
12.14 Telemedizin: Datenschützer begleiten Nutzung der Gesundheitskarte für elektronische Patientenakte ... 303
12.15 Wenn die Konfession für die stationäre Aufnahme im Klinikum entscheidend ist 306
12.16 Auch wenn sich alle Beteiligten kennen: Datenschutz nicht vergessen! 307

12.17 Auskunft der Einkommens- und Vermögenverhältnisse gegenüber unterhaltspflichtigen Geschwistern bei Unterhaltsforderungen 309
12.18 Auch das Sozialamt verlangt Daten 311
12.19 Sozialamt – Agentur für Arbeit – Jobcenter – Optionskommune: Datenschutz-Dschungelbuch 313
12.20 Datenschutzrechtliche Skepsis bei der Sepsis? 314
12.21 Sozialdaten – Schweigepflicht besteht auch gegenüber dem Landrat 315
12.22 Schwärzungen bei Kontoauszügen 317
12.23 Einwilligung im Rahmen der Unfallversicherung? 319
12.24 Welche Daten darf die Krankenkasse bei Renteneintritt erheben? 320
12.25 Wenn alle Behörden Fragen haben 322
12.26 Kontoauszüge für das Jobcenter 324
12.27 Immer wieder Kontoauszüge 327
12.28 Weitergabe von Sozialdaten zur Rechnungsprüfung: kein Verstoß gegen den Datenschutz 328
12.29 Qualitätssicherung versus Datenschutz? 330
12.30 Übermittlung von Sozialdaten 332
12.31 Silver Economy 333
12.32 Besonders zu schützende Daten Dritter als Zugabe 335
12.33 Kamera an bei psychiatrischer Begutachtung? 337
12.34 Unerlaubter Datenaustausch zwischen Krankenkasse und MDK? 339
12.35 Informationsflyer zum Neugeborenen-Sreening 340
12.36 Zentralregister für Gesundheitsberufe zum Abgleich von Mehrfachantragsstellungen 342
12.37 Personenbezogene Daten sind beim Versand auch durch Brief- und Postgeheimnis geschützt 343
12.38 Gemeinsam für den Datenschutz: Workshops mit der Landeskrankenhausgesellschaft Thüringen 345
12.39 Datenschutz wirkt über den Tod hinaus 347
12.40 Wissenschaftliche Forschung und Sozialdaten 348
12.41 ESF-Programm „JUGEND STÄRKEN im Quartier“ 350
12.42 Wann kommen und gehen die Mitarbeiter? – Doppelte Buchführung in der Stadtverwaltung 352
12.43 Kindergeld – was muss die Familienkasse wissen? 354
12.44 Feuchte Akten brennen schlecht 357

13. Infrastruktur und Landwirtschaft 360
13.1 Anfrage zur Bestellung von mehreren Personen für die Stelle eines Datenschutzbeauftragten 360
13.2 Einsatz funkbasierter „intelligenter“ Wasserzähler . 361
13.3 Verkehrsbeobachtung: immer diese Radfahrer – und ihre Daten 363
13.4 Bericht aus dem Arbeitskreis Verkehr: Anwohnerparken nach § 45 Abs. 1b Nr. 2a StVO) . 365
13.5 Elektronisches Wohngeldverfahren – Verbundverfahren oder nicht? 367
13.6 Wer darf was sehen? – Die Last mit dem Baulastenverzeichnis 369
13.7 Verwendung von Vordrucken im Wohngeldbereich 370

14. Umwelt, Energie und Naturschutz 373
14.1 Wildwuchs: Wildkameras 373
14.2 Immissionsschutzbehörde versus Schornsteinfegerinnung: entrußter Datenschutz 375
14.3 Erstellung eines Solarkatasters – datenschutzrechtlich sonnenklar 376
14.4 Webcam: Kraniche versus Segler 378

15. Wirtschaft, Wissenschaft und digitale Gesellschaft 381
15.1 Thüringer Zentrum für Existenzgründungen und Unternehmertum (ThEx) 381
15.2 GFAW will Daten der Verbraucherzentrale 383
15.3 Untersagung der Berufsausübung per E-Mail? 387
15.4 Schutz vor Spielsucht – Einführung einer Sperrdatei für Spielhallen datenschutzrechtlich unbedenklich? 389

16. Bildung, Jugend und Sport 392
16.1 Schule online – die Zweite 392
16.2 KITA-Eintritt: unklare Rechtslage zu Impfschutz-Daten 393
16.3 Fotos von KITA-Kindern: brisant! 396
16.4 Einsatz von Office 365 an Schulen? 398
16.5 Cloud-Lösung für Schulen – TLfDI mitten drin 400
16.6 Evaluation Kurs Medienkunde 402

16.7 WhatsApp in der Jugendsozialarbeit und Schule? ... 403
16.8 E-Mail-Nutzung zwischen Lehrern und Schülern ... 405
16.9 Schule 2.0 – Schuldatenschutzgesetz notwendig ... 406
16.10 Kultusministerkonferenz macht Medienkompetenz verbindlich ... 408
16.11 Datenschutz für junge Lehrer!!! ... 411
16.12 Online-Klassenbuch ... 413
16.13 Schulserver: geklaut! ... 414
16.14 Schulnoten für kommunale Sozialplanung – nur anonymisiert ... 417
16.15 Notenspiegel in Facebook: mangelhaft! ... 419
16.16 Jeder muss wissen, wenn der Kollege krank ist ... oder doch nicht? ... 421
16.17 Lehrergespräche über schulische Leistungen: keine gute Leistung ... 424
16.18 Datenschutz in der Thüringer Schulgesetzgebung ... 427
16.19 Hochschuleigene E-Mail-Adresse ... 429
16.20 Wie geht Datenschutz? – Da fragen wir doch den TLfDI! ... 432
16.21 Sitzpläne mit Matrikelnummern – zulässig? ... 433
16.22 Online-Gremienwahlen an der Friedrich-Schiller-Universität Jena ... 434
16.23 Immatrikulation – welche Speicherfrist gilt denn nun? ... 437
16.24 Adresslisten mit personenbezogenen Daten in Papiermüllcontainern einer Universität? ... 439
16.25 Kontoauszüge – welche darf das Amt sehen? ... 440
16.26 Beschwerde über BAföG-Stelle ... 443
16.27 Plagiatsprüfung ... 444
16.28 Mediendatenbank für Thüringer Schulen 2.0 ... 446
16.29 Nutzung sozialer Netzwerke und Messenger-Dienste in Schulen oft problematisch ... 447
16.30 Zweites Gesetz zur Änderung des Thüringer Erwachsenenbildungsgesetzes ... 450
16.31 PISA-Feldtest 2017 ... 451
16.32 Gesundheitsvorsorge in der Schule: Welche Daten darf die Schule dem Gesundheitsamt im Vorfeld übermitteln? ... 452
16.33 Erweiterte Sozialdatenerhebung im Rahmen der Schuleingangsuntersuchung – Ausforschung von Kind

	und Eltern durch den Gesundheitsdienst oder sinnvolle Ergänzung zur Gesundheitsvorsorge der Bevölkerung?	454
16.34	Schulaufsichtliche Prüfung – doppelt hält besser?	456
16.35	Schule stellt Schülern E-Mail-Adressen zur Verfügung - Klasse, oder?	458
16.36	Klassenbuch und Co.	460
16.37	Big Brother in der Schule? Unterrichtsvideografie in der Lehrerausbildung	462
16.38	Beschwerde über eine Schule in Bezug auf die Inanspruchnahme des Bildung- und Teilhabepaketes – Die finanzielle Situation des Elternhauses geht Dritte nichts an	464
16.39	Wann dürfen Prüfungsunterlagen kopiert und Prüfungsergebnisse weitergegeben werden?	465
16.40	Fotoaufnahmen beim Projekttag – „Entweder du lässt dich fotografieren oder du darfst nicht mitmachen!“	467
16.41	Einschulungsuntersuchung: Datenschutz in der Schulgesundheitspflege	469
16.42	Einbehalten von Klassenarbeiten von Schülern der 9. und 10. Klasse	470
16.43	Unterstützung von Amtsärzten durch niedergelassene Ärzte verstößt grundsätzlich nicht gegen den Datenschutz	472
17.	**Technische Entwicklung allgemein**	**474**
17.1	Datenschutz beim Bürger-Konto (Servicekonto)	474
17.2	Speicherung von IP-Adressen – Sicherheit oder Datenschutz?	475
17.3	eIDAS – was ist das?	478
17.4	EU- und nationale Cybersicherheit	479
17.5	Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation („Berlin Group“)	482
17.6	Canvas-Fingerprinting	483
18.	**Technischer Datenschutz im Freistaat Thüringen**	**485**
18.1	Angriffe auf das Netzwerk der Thüringer Landesverwaltung	485

18.2 BSI-Richtlinie: Kryptographische Verfahren 487
18.3 Windows 10, Microsoft-Cloud Deutschland und Windows Office 365.....488
18.4 Kritische Infrastruktur – Sektor Gesundheit.....490
18.5 Datenschleudern – vom vernetzten Auto.....491
18.6 WannaCry.....495

19. Parlamentarische Anfragen gem. § 112a Geschäftsordnung des Thüringer Landtags.....497
19.1 Parlamentarische Anfragen gem. § 40 Abs. 6 Satz 2 ThürDSG 497

20. Vorträge – der TLfDI ist unterwegs! 499

Anlagen

Entschließungen der 91. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 6./7. April 2016 in Schwerin

Anlage 1 Stärkung des Datenschutzes in Europa – nationale Spielräume nutzen 516
Anlage 2 Datenschutz bei Servicekonten.....518
Anlage 3 Wearables und Gesundheits-Apps – Sensible Gesundheitsdaten effektiv schützen! 521
Anlage 4 Wahrung der Freiheits- und Persönlichkeitsrechte bei der Bekämpfung des internationalen Terrorismus...524

Entschließungen zwischen den Konferenzen 2016

Anlage 5 Klagerecht für Datenschutzbehörden EU-Kommissionentscheidungen müssen gerichtlich überprüfbar sein.....526
Anlage 6 Zur Entschließung der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 20. April 2016 „Klagerecht für Datenschutzbehörden“.....528
Anlage 7 EU-Datenschutz-Grundverordnung erfordert zusätzliche Ressourcen für Datenschutzbehörden...529

Entschließungen der 92. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 9./10. November 2016 in Kühlungsborn

Anlage 8 Gemeinsame Prüfung der „Falldatei Rauschgift“ deckt gravierende Mängel auf Konsequenzen für polizeiliche Datenverarbeitung notwendig.....531
Anlage 9 „Videoüberwachungsverbesserungsgesetz“ zurückziehen! 533

Entschließungen zwischen den Konferenzen 2017

Anlage 10 Novellierung des Personalausweisgesetzes – Änderungen müssen bürger- und datenschutz-freundlich realisiert werden!.....535
Anlage 11 Neues Bundeskriminalamtgesetz – Informationspool beschneidet Grundrechte 537
Anlage 12 Gesetzesentwurf zur Aufzeichnung von Fahrdaten ist völlig unzureichend! 539

Entschließungen der 93. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 29./30. März 2017 in Göttingen

Anlage 13 Einsatz von Videokameras zur biometrischen Gesichtserkennung birgt erhebliche Risiken 541
Anlage 14 Göttinger Erklärung Vom Wert des Datenschutzes in der digitalen Gesellschaft 544

Entschließungen zwischen den Konferenzen 2017

Anlage 15 Grundsatzpositionen zum Datenschutz für die neue Legislaturperiode Datenschutzkonferenz formuliert elf handlungsorientierte Grundforderungen.....546

Entschließungen der 94. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 8./9. November 2017 in Oldenburg

Anlage 16 Umsetzung der DS-GVO im Medienrecht.....548

Anlage 17 Keine anlasslose Vorratsdatenspeicherung von Reisedaten....550
Anlage 18 Datenschutzbehörden erteilen der anlasslosen Vorratsdatenspeicherung von Reisedaten eine Absage und fordern die datenschutzrechtliche Anpassung von Rundfunk-Staatsverträgen sowie der Presse- und Mediengesetze....552

Pressemitteilungen 2016

Anlage 19 Zwei auf einen Streich: Transparenzgesetz und Digitale Selbstverteidigung....555
Anlage 20 Unterrichtsmaterial per Knopfdruck....556
Anlage 21 Datenschutz und Polizei optimieren ihre Zusammenarbeit: Polizistin abgeordnet zum Landesdatenschützer....558
Anlage 22 Pressemitteilung der 91. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder....559
Anlage 23 Privacy Shield: Geplantes Schutzschild-Abkommen zum Datenverkehr zwischen EU und USA noch immer zu löchrig....562
Press Release Privacy Shield – New Deal.... Effectiveness remains to be seen....564
Anlage 24 Datenschutz-Grundverordnung verabschiedet – Countdown läuft....565
Anlage 25 Forderung des Bundesrates: Klagerecht für die Datenschutzaufsichtsbehörden!....567
Anlage 26 Einladung zur Pressekonferenz: Es kommt dicker…! Der TLfDI stellt seine neuen Tätigkeitsberichte für die Jahre 2014 und 2015 vor!....568
Anlage 27 Gericht bestätigt: Videoüberwachung durch Private in öffentlich zugänglichen Räumen meldepflichtig!....570
Anlage 28 Upgrade auf Windows 10 – TLfDI gibt hilfreiche Tipps....571
Anlage 29 US-Gericht verbietet Zugriff der amerikanischen Dienste aufeuropäische Server....572
Anlage 30 Datenschutz konkret: Unternehmen im Fokus....573
Anlage 31 Reaktion des Datenschutzbeauftragten auf Spekulationen in der „Abhöraffäre“....574
Anlage 32 „DeviceWatch“....575

Anlage 33 Apple im Visier – Sicherheitslücke „Pegasus“ gefährdet iPhone-Nutzer 576
Anlage 34 Telefonaufzeichnungen in der Thüringer Polizei: Thüringer Landesbeauftragter für den Datenschutz und die Informationsfreiheit (TLfDI) rügt Falschauskunft durch ehemaliges TIM 577
Anlage 35 Medienkompetenz: Unterrichtsmaterial aktualisiert! 578
Anlage 36 Save the Date: Profiling Big Data – Small Privacy Zum Niedergang der Privatsphäre 579
Anlage 37 Dashcams: Selbsternannten Rittern des Rechts wird datenschutzrechtliche Abfuhr erteilt! 581
Anlage 38 Kontrollfreie Zonen für besonders sensible Daten .. 583
Anlage 39 Wearables mit „Gesundheitsfunktion“ 584
Anlage 40 Kooperation zwischen Kultusministerkonferenz und Datenschutzbeauftragtem macht große Fortschritte 586
Anlage 41 Polizei: Aufzeichnung von Telefongesprächen/„DeviceWatch“ 588

Pressemitteilungen 2017

Anlage 42 Polizei: Telefonatmitschnitte und „DeviceWatch“ – TLfDI ermittelt weiter 590
Anlage 43 Entwurf zum Bundesdatenschutzgesetz verspielt Chance auf besseren Datenschutz! 591
Anlage 44 Small sister is watching you! 594
Anlage 45 Vernetzung fördern – Medienkompetenz stärken Landesdatenschützer unterzeichnet Kooperationsvereinbarung 595
Anlage 46 Medieninformation – Einladung 596
Anlage 47 2. Tätigkeitsbericht zur Informationsfreiheit 597
Anlage 48 Gericht kippt Vorratsdatenspeicherung in Deutschland – ein guter Tag für den Datenschutz 598
Anlage 49 Bundesnetzagentur dreht Vorratsdatenspeicherung die Luft ab 600
Anlage 50 Drohnenverordnung: Keine Peepshow mehr mit Drohnen! 601
Anlage 51 Keine Weitergabe von Fluggastdaten: EuGH stärkt Datenschutzrechte 603

Anlage 52 Keine Kündigung infolge illegaler Überwachung des PC! 605
Anlage 53 EU-US Privacy Shield:Informationen und Beschwerdeformulare für Betroffene veröffentlicht 607
Anlage 54 Richtigstellung des Datenschutzbeauftragten Anlage zur Pressemitteilung vom 22. August 2017 610
Anlage 55 Meldepflicht für (Wild-)Kameras bestätigt! 611
Anlage 56 Trust – Wem kann ich trauen im Netz und warum? 612
Anlage 57 Für Kleine kein Persönlichkeitsrecht – In sozialen Netzwerken lassen Eltern die Hüllen der Kinder fallen! 613
Anlage 58 TLfDI warnt: Diese Kinder-Uhren ticken anders! - Appell an Eltern: Vernichten Sie smart getarnte Abhöranlagen - 615
Anlage 59 Microsoft trifft TLfDI-Wirtschaft und Datenschutzaufsicht – geht das zusammen?- 616
Anlage 60 Immelborn – AdActa 617

Kurzpapiere

Anlage 61 Verzeichnis von Verarbeitungstätigkeiten –Art. 30 DS-GVO 619
Anlage 62 Aufsichtsbefugnisse/Sanktionen 623
Anlage 63 Verarbeitung personenbezogener Daten für Werbung 627
Anlage 64 Datenübermittlung in Drittländer 631
Anlage 65 Datenschutz-Folgenabschätzung, Art. 35 DS-GVO 637
Anlage 66 Auskunftsrecht der betroffenen Person, Art. 15 DS-GVO 646
Anlage 67 Marktortprinzip: Regelungen für außereuropäische Unternehmen 650
Anlage 68 Maßnahmenplan „DS-GVO“ für Unternehmen 654
Anlage 69 Zertifizierung nach Art. 42 DS-GVO 659
Anlage 70 Informationspflichten bei Dritt- und Direkterhebung 663
Anlage 71 Recht auf Löschung / „Recht auf Vergessenwerden“ 669

Abkürzungsverzeichnis.....673

Stichwortverzeichnis/Index 682

B Öffentlicher Bereich



Vorwort

Im Vergleich zum 11. Tätigkeitsbericht hat sich der Arbeitsumfang des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) im Berichtszeitraum 2016/2017 wiederum stark erhöht. Wie die nachfolgende Statistik zeigt, hat sich die Zahl der registrierten Posteingänge des TLfDI von 2011 bis 2017 ca. verdreifacht. Offenbar ist es gelungen, Bürger, Unternehmen, aber auch Behörden für den Schutz der Privatsphäre, für die der Datenschutz immer bedeutender wird, zu sensibilisieren.

Diese zunehmenden Aufgaben sind nur mit einem funktionierenden Team zu bewältigen. Die dauerhafte und außergewöhnliche Belastung der Mitarbeiterinnen und Mitarbeiter hinterlässt jedoch erste Spuren. Zwar ist der Krankenstand noch niedrig und die Motivation ungebrochen hoch, zudem gibt es viele Bewerber, die ihre berufliche Zukunft beim TLfDI sehen – auch möchte niemand die Behörde des TLfDI wieder verlassen. Dennoch ist angesichts des Arbeitsanfalls die Leistungsgrenze überschritten und die Hoffnungen der Behörde ruhen auf der Einsicht der Abgeordneten des Thüringer Landtages, den TLfDI personell und finanziell zu stärken.

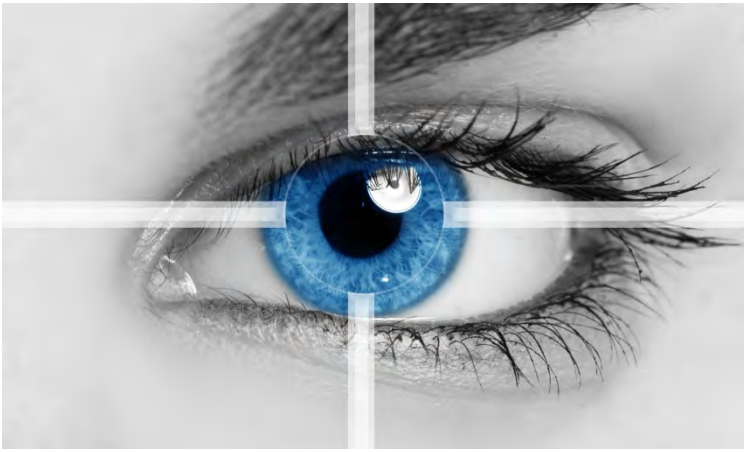


Der erwähnte signifikante Anstieg der Posteingänge von knapp 50 Prozent von 2016 zu 2017 ist auch auf die Europäische Datenschutz-Grundverordnung (EU-DS-GVO) zurückzuführen, die als neues und unmittelbar geltendes Datenschutzrecht im Mai 2018 ihre Wirkung entfalten wird. Diesbezügliche Fragestellungen, aber auch Anfragen für Vorträge zur EU-DS-GVO seitens der Behörden und Kommunen, nehmen stetig zu, auch vor dem Hintergrund, dass das Thüringer Datenschutzgesetz dem neuen europäischen Datenschutzrecht anzupassen ist. Der TLfDI ist mit dem Thüringer Ministerium für Inneres und Kommunales eine Kooperation eingegangen, um den Informationsbedürfnissen gerecht werden zu können. Das gilt auch für die neue EU-Richtlinie für Justiz und Inneres (JI-Richtlinie),

durch die der Datenschutz für die Erhebung, Speicherung, Weitergabe und Verarbeitung für Polizei, Justiz und Inneres europaweit vereinheitlicht werden soll und entsprechende Berücksichtigung unter anderem im neuen Thüringer Datenschutzgesetz finden muss. Der TLfDI hat sich in der Behördenlandschaft Respekt verschafft und das ist gut für die Bürgerinnen und Bürger unseres Freistaats.
Das gilt auch für die Thüringer Polizei. Obwohl es – wie nachfolgend dargestellt – hier einige Großbaustellen gab, kann doch konstatiert werden, dass die Kooperation zur Behebung der Fehler weitgehend funktionierte.
Schließlich ist die Förderung der Medienkompetenz im Freistaat eines der Hauptziele des TLfDI. Er hat hier wichtige Verbündete gewonnen, insbesondere den Bildungsminister Holter, auf dem als neuen Vorsitzenden der Kultusministerkonferenz die große Hoffnung ruht, hier weitere notwendige Schritte machen zu können.
Zur einfacheren Navigierbarkeit wurden die in diesem Tätigkeitsbericht verwendeten Links zusätzlich mit QR-Codes codiert. Die QR-Codes enthalten den Link in gerätelesbarer Form (beispielsweise der QR-Code links: https://www.tlfdi.de/tlfdi/).



Dadurch kann auf Geräten mit Kamera (z. B. Smartphones oder Tablets) und einer entsprechenden Software der Link durch das Gerät wieder decodiert werden und „Abschreibfehler“ können vermieden werden. Für Android-Smartphones kann der „Barcode Scanner“ des Entwicklers „Marty Mouse“ in der Version 1.0 empfohlen werden, da hier Open-Source-Software genutzt wird und die App nur minimale Funktionen besitzt. Für iOS ist dem TLfDI keine datenschutzgerechte App bekannt.



Eye close-up – © Minerva Studio / Fotolia.com

1. Schwerpunkte im Berichtszeitraum

Auch in diesem Berichtszeitraum wurden viele Kapazitäten des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) leider durch die Thüringer Polizei gebunden. Ausgelöst durch ein Telefonat zwischen einem Polizeibeamten und einem Staatsanwalt wurde der Umstand publik, dass auch solche Telefonate, die keine Notrufe darstellten, von polizeilichen Telefonapparaten aufgezeichnet wurden, obwohl eine entsprechende Dienstanweisung dieses gerade nicht vorsah. Hierfür gab es mehrere Ursachen. Etwa die, dass die erwähnte Dienstanweisung unzureichend umgesetzt wurde oder auch die, dass neue und vorhandene Technik nicht aufeinander abgestimmt waren. Der TLfDI hat zusammen mit dem Thüringer Ministerium für Inneres und Kommunales (TMIK) eine neue Dienstanweisung entwickelt, die künftig derartige Vorkommnisse ausschließen soll. Allerdings musste festgestellt werden, dass der TLfDI vom vorhergehenden Innenministerium über die Telefontechnik falsch informiert worden war – insoweit wurde eine Beanstandung ausgesprochen. Ausgestanden ist die sogenannte Abhöraffäre noch nicht, da technische Fragen weiterhin noch offen sind. Eine weitere Affäre stellte der Einsatz der Software „Device Watch“ dar. Diese Software ist – je nach Konfiguration – in der Lage, Verhalten von Mitarbeiterinnen und Mitarbeitern am PC zu kontrollieren. Hier mussten wegen zahlreicher Verstöße gegen das

Datenschutzrecht, aber auch gegen das Personalvertretungsrecht, Beanstandungen ausgesprochen werden. Ebenfalls aufwändig war und ist die datenschutzrechtliche Betreuung des Gemeinsamen Kompetenz- und Dienstleistungszentrums (GKDZ). Die parlamentarische Umsetzung des hierzu von den Ländern Thüringen, Sachsen, Sachsen-Anhalt, Brandenburg und Berlin geschlossenen Staatsvertrages wirft viele Fragen auf. Die datenschutzrechtlichen Fragestellungen werden erst dann überhaupt abzusehen sein, wenn die sogenannte Feinplanung der Innenministerien hierfür den Landesdatenschutzbeauftragten zur Verfügung gestellt werden wird. Das ist bisher nicht der Fall. Fragen der eingesetzten Hardware und Software, des Sicherheitskonzepts, des Verfahrensverzeichnisses, der Zugriffsberechtigungskonzepte, der Datenflüsse sowie der Nutzungsregelungen dieser neuen Einrichtung sind nicht im Ansatz geklärt. Das gilt auch hinsichtlich der Kosten dieser Einrichtung; um alles datenschutzrechtlich und datenschutzsicherheitsrechtlich rechtskonform auszugestalten, ist auch angesichts der Sensibilität der verarbeiteten Daten ein erhöhter Kostenaufwand absehbar. Die beteiligten Länderparlamente stellen insoweit zurecht Fragen – so ist der TLfDI als Sachverständiger von den Parlamenten der Länder Sachsen und Sachsen-Anhalt zur Stellungnahme zu diesem Projekt aufgefordert worden. Moderne Polizeiarbeit ist ohne entsprechende Technik nicht mehr vorstellbar – der TLfDI begleitet die Thüringer Polizei auf ihrem Weg gern.

Die Kooperation mit den Kommunen hat sich aus Sicht des TLfDI weiter verbessert. So gehen die Kommunen bei datenschutzrechtlichen Fragestellungen mehr und mehr dazu über, den TLfDI bereits vor der Datenverarbeitung zu Rate zu ziehen und nicht erst, wenn das datenschutzrechtliche Kind in den Brunnen gefallen ist. Eine erfreuliche Entwicklung, die sich auch in den festen Zusammenkünften zwischen Vertretern des TLfDI und zahlreichen Kommunalvertretern widerspiegelt – in diesen Diskussionsrunden werden drängende praktische Datenschutzprobleme erörtert und wenn möglich gelöst. Solche regelmäßigen Arbeitskreise schaffen zudem gegenseitiges Vertrauen, auf dessen Basis die Umsetzung des Datenschutzrechts besser funktioniert.

Um die Vertrauensbildung zu intensivieren, ist der TLfDI neue Wege gegangen: So werden stetig Polizeibeamte bzw. Polizeibeamtinnen an den TLfDI entsandt, um dessen Arbeitsweise und Arbeitsinhalte kennen zu lernen – gerade auch im Polizeibereich –, damit die

Gedankengänge des TLfDI besser nachvollzogen werden können. Der TLfDI profitiert von dem Gedankenaustausch mit den an seine Behörde entsandten Polizeikräften, und auf diese Weise entwickelt sich ein besseres wechselseitiges Verständnis, welches für den Transport datenschutzrechtlicher Inhalte ideal ist. Überdies werden die in die Polizei zurückkehrenden Polizeikräfte sodann als behördliche Datenschutzbeauftrage eingesetzt, sodass auf diesem Wege eine datenschutzrechtliche Nachhaltigkeit erzeugt wird.
Von vergleichbarer hoher Effizienz ist die Abordnung eines Lehrers an den TLfDI, der auf diese Weise einen besseren Einblick in die Schulstrukturen erlangt. Dieser Lehrer fungiert als Mittler zwischen der Datenschutz- und der Schulwelt, und das mit großem Erfolg! Um die Probleme der Lehrerinnen und Lehrer in der Praxis wissend, können datenschutzrechtliche Fragestellungen eingehender erörtert und damit für alle Beteiligten einer konsensualen Lösung zugeführt werden.
Die erwähnten Personalmaßnahmen sollen auch signalisieren, dass der TLfDI sich den Argumenten der Praxis nicht verschließt, sondern dass ihm daran gelegen ist, Lösungen zu finden, die in der Praxis auch Akzeptanz finden.
Akzeptanz hat inzwischen auch die Position des TLfDI gefunden, dass der Kurs Medienkunde in Thüringer Schulen nur unzureichend umgesetzt wird. Dieser Befund deckt sich mit entsprechenden Feststellungen in anderen Bundesländern, die im Arbeitskreis „Datenschutz und Bildung“ sowie im Unterarbeitskreis „Datenschutz und Schule“ der Landesdatenschutzbeauftragten, deren Vorsitzender der TLfDI ist, zusammengetragen werden. In Thüringen wird der Kurs Medienkunde extern evaluiert – unter Beteiligung des TLfDI –, was bundesweit einmalig sein dürfte. Kultus-Staatssekretärin Ohler hat hier die Zeichen der Zeit erkannt und richtet Schule insoweit neu aus. Unterstützt wird sie dabei von vielen Akteuren, natürlich auch dem TLfDI. Ihr zur Seite steht die von Staatskanzlei-Staatssekretär Krückels ins Leben gerufene Kooperationsvereinbarung zwischen unterschiedlichen Akteuren auf dem Feld der Medienkompetenz, die sich zum Ziel gesetzt haben, die nunmehr erkannten Defizite abzustellen. Anzusetzen ist hierbei nicht nur bei der Lehrerfortbildung und der Erstellung von Unterrichtsmaterialien im Bereich Medienkompetenz, sondern auch und gerade in der Lehrerausbildung. Der TLfDI konnte hier Kontakte zur Kultusministerkonferenz nutzen, um den Schutz der Privatsphäre bzw. den Datenschutz auch in der Leh-

rerausbildung zu verankern. Das neue Strategiepapier der Kultusministerkonferenz sieht insoweit nunmehr verpflichtende Studieninhalte für angehende Lehrer vor – das ist neu! Der für Hochschulausbildung und auch für Digitales zuständige Minister Tiefensee steht im Kontakt mit dem TLfDI, um auch hier die Weichen richtig zu stellen. Als Lehr- bzw. Lernmittel wird das analoge Schulbuch in absehbarer Zeit ausgedient haben. Die digitale Vermittlung von Lernstoff ist (bundes-)politisches Ziel, zu dessen Umsetzung man auf Plattformen großer Player zurückgreifen will. Auch an dieser Stelle zeigen sich weitreichende datenschutzrechtliche Fragestellungen. Der TLfDI als Vorsitzender der genannten Arbeitskreise setzt sich mit Unterstützung seiner Länderkollegen dafür ein, dass in diesem Zusammenhang keine personenbezogenen Schülerdaten verarbeitet werden, um etwa eine mithilfe von Algorithmen erzeugte Schüler-Daten-Vita mit ihren Missbrauchsmöglichkeiten auszuschließen. Daher ist die Bemerkung der Bundeskanzlerin Merkel, Daten seien der Rohstoff der Zukunft, mit dem Zusatz zu versehen: solange das Grundrecht der informationellen Selbstbestimmung nicht verletzt wird. Die allseits galoppierende Ökonomisierung personenbezogener Daten darf sich nicht in der Normativität des Faktischen häuslich einrichten, sondern hat – was leider zunehmend aus dem Blickfeld gerät – das Recht zu beachten! Gehörige Beachtung finden auch die Bestrebungen des Freistaats Thüringen, zu einem E-Government überzugehen. Ein entsprechender Gesetzesentwurf hierzu ist bereits unterwegs und der TLfDI freut sich auf die bereits eingeleitete Kooperation mit dem Thüringer Finanzministerium.

Das Grundrecht der informationellen Selbstbestimmung ist bettlägerig geworden. Schnelle Heilung ist nicht in Sicht – im Gegenteil: Neue Gesetze zur Sicherheitsarchitektur drängen den Schutz der Privatsphäre des Individuums zunehmend zurück. Um das Sicherheits*gefühl* der Bürgerinnen und Bürger zu stärken, wird das Grundrecht der informationellen Selbstbestimmung zur Ader gelassen. Um das Sicherheitsgefühl der Bürgerinnen und Bürger zu stärken, spukt in manchen Köpfen das Szenario einer flächendeckenden Videoüberwachung mit biometrischer Gesichtserkennung herum. Der TLfDI nimmt das mit großer Sorge wahr. Schnelle und billige Angebote zur Beruhigung des anscheinend lädierten Sicherheitsgefühls der Bürgerinnen und Bürger ohne fundierte Fakten zur Effizienz solcher Mittel entlarven sich denn auch schnell als bloßer Aktionismus. Es geht nicht um die Behandlung eines anscheinend schlechten

Sicherheitsgefühls, sondern um die tatsächliche Gewährung staatlicher Sicherheit. Hightech-Videokameras ersetzen nicht Polizeikräfte zur Aufrechterhaltung der öffentlichen Sicherheit.



Datenschutz – © fotodo / Fotolia.com

2. Allgemeine Entwicklungen im Datenschutz

2.1 Spitze der Bewegung: Arbeitskreis (AK) Datenschutz und Bildung und Unterarbeitskreis (UAK) Datenschutz und Schule

Unter Vorsitz des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) haben sich auch in den vergangenen zwei Jahren der Arbeitskreis (AK) Datenschutz und Bildung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder und der Unterarbeitskreis (UAK) Datenschutz und Schule länderübergreifend darüber ausgetauscht, wie die Menschen aller Altersgruppen für das Thema Datenschutz interessiert und für das Ergreifen geeigneter Maßnahmen zum Schutz der Privatsphäre sensibilisiert werden können. Kinder und Jugendliche sind aufgrund der in dieser Altersgruppe besonders intensiven und unvoreingenommenen Nutzung von neuen Medien, wie Smartphones, Tablets und Notebooks sowie den darauf installierten Anwendungen in Form von Apps, sozialen Netzwerken und Messenger-Diensten besonders mit datenschutzrechtlich relevanten Sachverhalten konfrontiert. Ein großes Thema beider Arbeitskreise war die Mitarbeit am Entwurf

des Strategiepapiers der Kultusministerkonferenz „Bildung in der digitalen Welt“. Das inzwischen von der Kultusministerkonferenz veröffentlichte Strategiepapier macht den Schulen bundesweit Vorgaben für deren Bildungs- und Erziehungsauftrag im Bereich der digitalen Medien. Im Rahmen der Vermittlung von Medienkompetenz ist Datenschutz in einem von insgesamt sechs Kompetenzbereichen als ein Ziel der Schule in dem Strategiepapier ausdrücklich aufgeführt. Es besteht nun die ausdrückliche Verpflichtung der Länder, Referendare in Medienkompetenz auszubilden. Darüber hinaus wird die Schule verpflichtet, ihren Schülern nur Plattformen, Lernumgebungen und Netzwerke zur Verfügung zu stellen, die datenschutzkonform sind.

Ein weiteres Thema war der Einsatz von Messenger-Diensten und hier praktisch ausschließlich WhatsApp bei der Kommunikation zwischen Schülern und Lehrkräften. Der AK war sich darüber einig, dass es auf dem Markt auch datenschutzgerechtere Messenger-Dienste gibt, wegen des damit verbundenen Eingriffs in den Wettbewerb jedoch keine konkreten Dienste genannt werden können. Wer sich über die unterschiedlichen Messenger-Dienste informieren will, kann dies auf Youngdata unter https://www.youngdata.de, dem Jugendportal der unabhängigen Datenschutzbehörden des Bundes und der Länder sowie des Kantons Zürich, tun.

Den AK-Mitgliedern wurde ein Medienprojekt des TLfDI in Zusammenarbeit mit dem MDR vorgestellt. Der MDR hatte es sich zur Aufgabe gemacht, einen Film zum Thema Videoüberwachung und Privatsphäre zu erstellen und dabei die Idee gehabt, den Einsatz von Videodrohnen in Form eines Animationsfilms aus datenschutzrechtlicher Sicht zu problematisieren. Der TLfDI unterstützte auf Anfrage des MDR das Projekt inhaltlich. In diesem Zusammenhang entstand unter den AK-Mitgliedern eine Diskussion darüber, wie erreicht werden könnte, dass Datenschutzthemen von den Massenmedien aufgegriffen werden. Es wurde die Nutzung von Videokanälen vorgeschlagen, da hiermit die Zielgruppe der Jugendlichen erreicht werden kann.

Schließlich wurde eine mögliche Kooperation der Thüringer Landesmedienanstalt mit dem AK Datenschutz und Bildung im Bereich Medienbildung ausgelotet. Hierzu hatte der TLfDI Vertreter der

Thüringer Landesmedienanstalt eingeladen, die einen Vortrag über die Aufgaben der Landesmedienanstalten, deren Organisationsstruktur sowie den hierzu bestehenden Rechtsvorschriften hielten.

Der UAK Datenschutz und Schule beschäftigte sich auch in den vergangenen zwei Jahren mit zahlreichen, speziell die Schulen betreffenden Datenschutzthemen. Die UAK-Mitglieder tauschten sich über die möglichen Konsequenzen aus, die sich aus der ab 25. Mai 2018 wirksam werdenden EU-Datenschutz-Grundverordnung (DS-GVO) ergeben. Dies betrifft zum einen die im Kultusbereich erforderlichen Anpassungen der bestehenden Gesetze, Verordnungen, Erlasse usw. an die Bestimmungen der DS-GVO. Zum anderen sind auch alle von den Datenschutzbeauftragten des Bundes und der Länder aktuell herausgegebenen Orientierungshilfen, Broschüren, Informationsblätter, Internetauftritte usw. unter dem Gesichtspunkt der geänderten Rechtslage zu überarbeiten. Zu einer arbeitsintensiven Angelegenheit hat sich auch der Einsatz von Microsoft Office 365 in Schulen entwickelt. Die Beschäftigung mit diesem Onlinedienst war erforderlich geworden, weil sich viele Schulen mit Fragen an die Landesdatenschutzbeauftragten gewandt hatten, ob der Einsatz des Verfahrens aus datenschutzrechtlicher Sicht zulässig ist. Da es sich bei Microsoft um ein Unternehmen mit Hauptsitz in den USA handelt, ist bisher nicht eindeutig zu klären, ob das Unternehmen einen Zugriff auf innerhalb der EU gespeicherte Daten durch US-Geheimdienste sicher ausschließen kann. Eine endgültige Stellungnahme des UAK steht noch aus. Darüber hinaus ist das Thema auch in weitere Arbeitskreise verwiesen worden. Erst nach einer Abstimmung der Positionen aller beteiligten Arbeitskreise werden gesicherte Aussagen zur Zulässigkeit der Verwendung von Microsoft Office 365 in den Schulen erfolgen können. Als eine Entscheidungshilfe für Schulen hat der UAK Datenschutz und Schule den Entwurf einer Orientierungshilfe für Online-Lernplattformen im Schulunterricht gemeinsam erarbeitet und unter Einbeziehung weiterer Arbeitskreise abgestimmt und der Datenschutzkonferenz zur Prüfung vorgelegt. Die Orientierungshilfe wurde auf der 91. Datenschutzkonferenz am 6./7. April 2016 beschlossen und kann auf der Homepage des TLfDI unter www.tlfdi.de/mam/tlfdi/gesetze/orientierungshilfen/oh-lernplattformen.pdf abgerufen werden. In diesem Zusammenhang stellte der TLfDI zur Diskussion, wie mit den zahlreichen schuli-



schen Anfragen zur Nutzung von Cloud-Diensten für schulische Zwecke umzugehen ist.
Ein weiteres datenschutzrechtliches Problem stellt sich bei der Verarbeitung der Daten von Kindern beruflich Reisender. In Deutschland gibt es ungefähr 10.000 bis 12.000 Kinder von beruflich Reisenden, die ihrer Schulpflicht nachkommen müssen. Da diese Kinder an verschiedenen Orten in ganz Deutschland geschult werden, müssen die Schüler ein Schultagebuch führen, das auf Reisen den jeweils zuständigen Lehrkräften vorgelegt wird. In den Bundesländern bestehen Bestrebungen, dieses Schultagebuch durch ein automatisiertes Verfahren zu ersetzen. Die Datenschutzbeauftragten stellten hierzu unterschiedliche Konzepte vor. Es wird davon ausgegangen, dass die Schaffung einer speziellen Rechtsgrundlage für den Betrieb solcher automatisierter Verfahren erforderlich ist, z. B. in Form des Abschlusses eines Staatsvertrags durch die teilnehmenden Bundesländer.
Bereits im 11. Tätigkeitsbericht (TB) hatte der TLfDI darüber berichtet, dass in Thüringen das Einrichten und Führen von Girokonten zu schulischen Zwecken nicht geregelt ist und deshalb häufig die Lehrkräfte z. B. für die finanzielle Abwicklung von Klassenfahrten ein Privatkonto eröffnen müssen. Der TLfDI hatte gegenüber dem Thüringer Ministerium für Bildung, Jugend und Sport (TMBJS) um eine entsprechende Regelung gebeten, die das Eröffnen von Schulkonten erlaubt (11. TB unter 14.18). Die UAK-Mitglieder tauschten sich über die in den Bundesländern bestehenden Regelungen aus. Der TLfDI hat das TMBJS bereits mehrfach an die noch ausstehende Regelung des Sachverhalts erinnert. Nach Auskunft von dort können sich das TMBJS und das Thüringer Finanzministerium bislang nicht darüber einigen, ob die Kontoinhaberschaft von Schulkonten beim Land oder aber bei den Schulträgern liegen soll. Es bestand lediglich Einigkeit darüber, dass die Lehrkräfte keine Privatkonten für schulische Zwecke eröffnen dürfen.
Ein datenschutzrechtliches Problem erwächst auch aus der fortschreitenden Nutzung von mobilen Endgeräten durch Lehrkräfte für schulische Zwecke – „Bring Your Own Device“ (BYOD). Unter dem Vorsitz des TLfDI hatte sich eine Unterarbeitsgruppe zusammengefunden, die ein Informationsblatt „Einsatz von privaten mobilen Datenverarbeitungsgeräten von Lehrkräften zu dienstlichen Zwecken“ erarbeitet, welches sich an Lehrkräfte richtet, die bereits für ihre dienstliche Arbeit private mobile Endgeräte, also Smartphones

und Tablets, verwenden oder diesen Einsatz planen. Der Entwurf ist bereits mehrfach überarbeitet worden und soll demnächst veröffentlicht werden. Insgesamt hat der UAK eine weitere Anzahl von Themen behandelt, die im vorliegenden Tätigkeitsbericht als eigene Beiträge aufgenommen wurden.

Der AK Datenschutz und Bildung ist wie in den vergangenen Jahren das Gremium, in dem sich die Datenschutzaufsichtsbehörden darüber austauschen, wie der Datenschutzgedanke in der Bevölkerung noch mehr Verbreitung und Beachtung finden kann. Der UAK Datenschutz und Schule wird sich weiterhin allen datenschutzrechtlichen Themen widmen, die im Schulbereich relevant sind und einer datenschutzgerechten Lösung bedürfen.

2.2 Runder Tisch Medienkompetenz

Runde Tische sind zumindest den reiferen Bürgerinnen und Bürgern der neuen Bundesländer aus der Wendezeit gut in Erinnerung. Manche waren erfolgreich, andere blieben in endlosen Verfahrensdiskussionen stecken und ohne sichtbare Wirkung. Allen gemeinsam war die Begeisterung über nicht gekannte Teilnahmemöglichkeit am gesellschaftlichen Sein jenseits von staatlicher Indoktrination in einer Zeit, als echte Mitbestimmung noch ein Fremdwort war. Mit ähnlichem Enthusiasmus startete im Oktober 2015 der „Runde Tisch Medienkompetenz“ als diskussionsoffene, öffentliche Gesprächs- und Veranstaltungsreihe. Die Initiative ging von der Thüringer Staatskanzlei und dem Bildungsministerium aus.
Praktiker und Fachexperten aus Schule, Jugendarbeit, Gesellschaft, Wissenschaft, Wirtschaft, Politik und Verwaltung waren angesprochen, unter dem Eindruck des digitalen Wandels über Erreichtes in Sachen Medienkompetenzentwicklung von Kindern und Jugendlichen zu diskutieren und Schwerpunkte für die Zukunft abzuleiten. Erfreulich: Auch der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) war gefragt, sich aktiv zu beteiligen. Die Veranstaltungen in der Folgezeit widmeten sich unterschiedlichen Facetten und Problemen, wie der Stärkung von Lese- und Medienkompetenz durch Unterstützungsangebote von Zeitungsverlagen über praktische Angebote von Kinder- und Jugendsozialarbeit bis hin zur Problematik der medienpädagogisch unzureichenden Aus- und Weiterbildung von Lehrern. Der bundes-

weit festgestellte Nachholbedarf an Hochschulen mit Lehramtsstudiengängen wurde in verschiedenen Veranstaltungen des Runden Tisches immer wieder betont.
Der TLfDI hat auf das Problem schon oft hingewiesen, so auch im September 2016 in Nordhausen. Bei diesem Runden Tisch standen Datenschutz und Datensicherheit als untrennbarer Bestandteil von Medienkompetenz im Mittelpunkt. Die Medienbildungslücke in den Schulen und Lehrerbildungsstudiengängen der Thüringer Universitäten wird der TLfDI allein nicht lösen können. Aber sein klares Angebot, bei der Vermittlung schulrelevanter Datenschutzaspekte im Rahmen des Vorbereitungsdienstes von angehenden Lehrern an den Studienseminaren zu unterstützen, bekräftigte der TLfDI an diesem Tag nochmals gegenüber der Staatsekretärin und weiteren Vertretern des Bildungsministeriums. Der TLfDI nutzte auch die Möglichkeit, die anwesenden Lehrerinnen und Lehrer auf die Unterstützungsangebote für den Unterricht, z. B. die Mediendatenbank, hinzuweisen. Datenschutz und Medienbildung gehören in einer Zeit digitalen Wandels untrennbar zusammen. Das stellte die abschließende Podiumsdiskussion mit dem TLfDI, den Direktoren vom Thüringer Institut für Lehrerfortbildung, Lehrplanentwicklung und Medien (ThILLM) und Thüringer Landesmedienanstalt (TLM), einem Staatsanwalt und einer Lehrerin klar. Erfreulicher Nebeneffekt: Die Lehrerin – auch am Erfurter Studienseminar tätig – nahm den TLfDI gleich beim Wort. So wurde eine erste Veranstaltung zum Thema „Datenschutz an Schulen“ für Lehramtsanwärter an Regelschulen und Gymnasien vereinbart. Über ihren erfolgreichen Verlauf wird im Beitrag 16.11 berichtet. Runde Tische haben doch manchmal tatsächlich kleine Wirkungen.
Große Wirkungen erhofft sich der TLfDI vom wichtigsten Ergebnis des Runden Tisches, das auf der Abschlussveranstaltung im Februar vorgestellt wurde: Staatskanzlei, verschiedene Ministerien, der TLfDI, die TLM sowie das ThILLM unterzeichneten eine Landeskooperationsvereinbarung zur nachhaltigen Weiterentwicklung von Medienkompetenz in Thüringen. Die Arbeit hat im Juni 2017 begonnen. Der TLfDI wird hier klare Akzente setzen. Im nächsten Tätigkeitsbericht wird von den Ergebnissen zu berichten sein.

Der TLfDI beteiligte sich von September 2015 bis Februar 2017 aktiv am „Runden Tisch Medienkompetenz“. In der Veranstaltungsreihe diskutierten Praktiker und Fachexperten mit Vertretern aus

Politik und Verwaltung über die neuen Herausforderungen von Medienbildung im digitalen Zeitalter und ihre Antworten darauf. Datenschutz und Datensicherheit sind untrennbarer Bestandteil zeitgemäßer Medienbildung. Deshalb beschäftigte sich ein Runder Tisch explizit mit dem Thema. Der TLfDI wies dabei erneut auf die unzureichende Ausbildung von Lehrern in diesem Bereich hin und unterbreitete Unterstützungsangebote. Wichtigstes Ergebnis des Runden Tisches Medienkompetenz ist die Unterzeichnung einer Landeskooperationsvereinbarung zur nachhaltigen Weiterentwicklung von Medienkompetenz durch verschiedene Landesbehörden. Das Gremium hat seine Arbeit im Juni 2017 begonnen.

2.3 Gesetz zur Neuregelung des Mikrozensus

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) übersandte dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) im Berichtszeitraum den Entwurf für ein Gesetz zur Durchführung einer Repräsentativstatistik über die Bevölkerung und die Arbeitsmarktbeteiligung sowie die Wohnsituation der Haushalte (Mikrozensusgesetz – MZG), den das Bundesministerium des Innern (BMI) zur Verfügung gestellt hatte. Stellungnahmen zum Gesetzentwurf sollten kurzfristig mitgeteilt werden.
In Anbetracht des minimalen Zeitfensters hatte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) nach kursorischer Durchsicht des übersandten Gesetzentwurfs zwei kritische Anmerkungen:
Zu § 13 Abs. 7 MZG-E, der die Auskunftspflicht regelt, hielt es der TLfDI für besonders bedeutsam, die Freiwilligkeit der Auskünfte bei besonders sensiblen Fragen und Themen hervorzuheben. Bürgerbeschwerden wären sonst in Folge vorprogrammiert. Zudem hielt der TLfDI die in § 8 Abs. 1 Nr. 4 MZG-E geregelte Erhebung der Merkmale zur wirtschaftlichen Belastung (materielle Deprivation) unter dem Gesichtspunkt des tiefen Eingriffs in das informationelle Selbstbestimmungsrecht der Betroffenen für zu weitgehend, zumal diese Erhebungsmerkmale zum Großteil zu unbestimmt waren und damit nicht den Vorgaben des Bundesverfassungsgerichts genügten. Gefragt waren hier z. B. Angaben zur finanziellen Kapazität, sich eine einwöchige Ferienreise jährlich leisten zu können.

Im Übrigen schloss sich der TLfDI den Stellungnahmen der anderen Datenschutzbeauftragten der Länder an.
Zum Bedauern des TLfDI hat die Prüfung des zum 1. Januar 2017 in Kraft getretenen Mikrozensusgesetzes ergeben, dass sich das BMI im Wesentlichen nicht dazu entschließen konnte, die unterbreiteten datenschutzrelevanten Änderungsvorschläge der Datenschutzbeauftragten des Bundes und der Länder aufzugreifen.

Zum einen Ohr rein, zum anderen Ohr heraus: Der TLfDI ist es gewohnt, dass seine wohlgemeinten datenschutzrechtlichen Ratschläge nicht immer Gehör finden oder bewusst unbeachtet bleiben. Gerade wenn, wie im konkreten Fall dargelegt, gesetzliche Neuerungen im Bundestag auf den Weg gebracht werden sollen, ist es besonders bemerkenswert, wenn ein Bundesministerium nicht die Expertise von siebzehn(!) Datenschutzbehörden aus Bund und Ländern berücksichtigt. Der TLfDI ist nicht verwundert – das Bundesverfassungsgericht wird es wieder einmal richten müssen.

2.4 Videoüberwachung im privaten und öffentlichen Raum – der TLfDI berät in jedem Einzelfall gern, gerade auch zur neuen Rechtslage der Datenschutz-Grundverordnung

Gem. § 40 Abs. 7 ThürDSG berät der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) alle öffentlichen Stellen des Freistaats Thüringen, worunter gem. § 2 Abs. 2 Satz 1 ThürDSG auch alle juristischen Personen und sonstige Vereinigungen des privaten Rechts zu zählen sind, die Aufgaben der öffentlichen Verwaltung wahrnehmen und an denen eine oder mehrere juristische Personen des öffentlichen Rechts beteiligt sind.
Beratungsbedarf hatte im August 2017 auch die Stadt Erfurt, die im Rahmen einer Sitzung ihres Kriminalpräventiven Rates alle interessierten (kommunalen) Wohnungsunternehmen an einen Tisch geholt hatte und vom TLfDI über die Möglichkeiten der Videoüberwachung in Mietshäusern, und dort insbesondere in Hauseingängen, Treppenfluren und Aufzügen, informiert werden wollte.
Die Vertreter des TLfDI informierten die Vertreter der Wohnungsunternehmen und der Stadt Erfurt zunächst über ausgewählte Urteile zur Zulässigkeit der Videoüberwachung in den genannten Bereichen eines Mietshauses. Dabei machte der TLfDI insbesondere deutlich, dass die datenschutzrechtliche Zulässigkeit einer Videoüberwachung

stets nach den Gegebenheiten im konkreten Mietshaus zu beurteilen ist. Denn sowohl in § 25a ThürDSG, der die Videoüberwachung durch öffentliche Stellen regelt, als auch in § 6b BDSG, der die Voraussetzungen einer Videoüberwachung durch nicht-öffentliche Stellen bestimmt, ist jeweils das Tatbestandsmerkmal der Erforderlichkeit enthalten. Erforderlich ist daher der Einsatz einer Videoüberwachung – entweder in Form der Videobeobachtung (Monitoring) oder in Form der Videoaufzeichnung – nur dann, wenn sie unabdingbar ist, um den Zweck – im Fall des § 25a ThürDSG die Wahrnehmung des Hausrechts und im Fall des § 6b BDSG darüber hinaus auch zur Aufgabenerfüllung öffentlicher Stellen sowie zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke – zu erreichen und keine anderen gleichermaßen wirksamen Maßnahmen, die weniger in das Recht auf informationelle Selbstbestimmung des Betroffenen eingreifen, zur Verfügung stehen. Alternativen zur Videoüberwachung, die weniger in das Recht auf informationelle Selbstbestimmung eingreifen, können z. B. Gegensprechanlagen an Haustüreingängen für die Mieter eines Hauses darstellen, mit denen der Zweck, unbefugtes Betreten des Mietshauses zu verhindern, ebenfalls erfüllt werden kann.

Am Kriterium der Erforderlichkeit scheiterte auch der Wunsch einiger Teilnehmer der Gesprächsrunde, eine datenschutzrechtlich zulässige Videoüberwachung in einem Mietshaus eines bestimmten Bautyps auf eine andere Immobilie desselben Bautyps übertragen zu können. Die Vertreter des TLfDI wiesen ausdrücklich darauf hin, dass die Einrichtung und der Betrieb einer Videoüberwachungsanlage immer auf den Einzelfall abzustimmen seien. Nur weil in einem Mietshaus eines bestimmten Gebäudetyps die Videoüberwachung datenschutzrechtlich zulässig sei, bedeute dies noch lange nicht, dass die Videobeobachtung oder -aufzeichnung in einem anderen Mietshaus desselben Gebäudetyps genauso datenschutzrechtlich zulässig ist. Grund dafür sind z. B. die unterschiedlichen Vorfälle in unterschiedlicher Anzahl und Intensität, die im Rahmen jeder datenschutzrechtlichen Prüfung zu berücksichtigen sind.



Abschließend wiesen die Datenschützer auf die Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen“ des Düsseldorfer Kreises (https://www.tlfdi.de/mam/tlfdi/datenschutz/video/oh-v -durch-nicht- ffentliche-stellen.pdf) und auf die Orientierungshilfe „Sehen und gesehen werden“ zur Videoüberwachung durch Private der Landesbeauftragten für Datenschutz und Informationsfreiheit in Nordrhein-Westfalen (https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Datenschutz-recht/Inhalt/Videoueberwachung/Inhalt/_Sehen_und_gesehen_werden_-_Video__berwachung_durch_Private_in_NRW/Sehen_und_gesehen_werden1.pdf) hin.



Ein weiteres Thema, das die Vertreter des TLfDI in der Sitzung des Kriminalpräventiven Rates gegenüber den Vertretern der Wohnungsunternehmen ansprachen, war die Regelung zur Videoüberwachung in der neuen Datenschutz-Grundverordnung (DS-GVO). Eine eigene Rechtsgrundlage zur Beurteilung der Zulässigkeit von Videoüberwachungen wie im Bundesdatenschutzgesetz (BDSG) existiert in der DS-GVO nicht. Im Rahmen der DS-GVO ist für die Rechtmäßigkeit der Verarbeitungsvorgänge Art. 6 DS-GVO heranzuziehen. Der nationale Gesetzgeber hat jedoch mit § 4 des neuen BDSG eine Regelung für Videoüberwachungen öffentlich zugänglicher Räume getroffen, welche dem jetzigen § 6b BDSG entspricht. Ein Großteil der Aufsichtsbehörden ist sich darüber einig, dass dieser neue § 4 BDSG europarechtswidrig ist, da Art. 6e DS-GVO lediglich eine Öffnungsklausel zu nationalen Regelungen im öffentlichen Bereich vorsieht. Für den nicht-öffentlichen Bereich gilt daher die DS-GVO unmittelbar. Hier ist fraglich, ob die Aufsichtsbehörden den § 4 des Anpassungsgesetzes anwenden werden. Wenn nicht, werden Videoüberwachungen zukünftig nach Art. 6f DS-GVO für öffentlich zugängliche Bereiche, wie für nicht-öffentlich zugängliche Bereiche beurteilt. Nach Art. 6f DS-GVO ist die Verarbeitung von personenbezogenen Daten zulässig, wenn sie

zur Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten erforderlich ist und die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, nicht überwiegen. Es ergeben sich hier nur geringe Unterschiede, zu der jetzigen Zulässigkeitsprüfung. Die Aufsichtsbehörden erarbeiten hierzu derzeit in einem Arbeitskreis ein sogenanntes Kurzpapier hinsichtlich der Anwendung auf die Videoüberwachungsproblematik. Grundsätzlich neu ist hier, dass Drittinteressen bei den berechtigten Interessen nunmehr zu berücksichtigen sind. Einigkeit besteht darüber, dass Betroffene nicht Dritte sein können. Ansonsten steht noch offen, wer alles Dritter sein kann. Im Rahmen der Interessenabwägung sind zusätzlich nach Erwägungsgrund 47 der DS-GVO die vernünftigen Erwartungen der betroffenen Person bei den schutzwürdigen Interessen zu berücksichtigen. Im Bereich der Videoüberwachung wird sich dies danach richten, ob die Videoüberwachung in bestimmten Bereichen typischerweise akzeptiert wird. Problematisch wird das in Individualbereichen wie Wohnen, Sanitär, Fitness, Sauna usw. gesehen. Ebenso bei öffentlich zugänglichen Räumen, welche zur Erholung, Entspannung und Freizeitgestaltung dienen, da sich die Betroffenen dort länger aufhalten um zu kommunizieren. Dort erwartet ein Betroffener nicht, mit optisch-elektronischen Mitteln überwacht zu werden. Einigkeit besteht darin, dass das Aufstellen von Hinweisschildern nicht dazu führt, dass die Betroffenen diese hinnehmen müssen und als Akzeptanz der Videoüberwachung umzudeuten ist.
Der Aufbau der Prüfung erfolgt nach dem jetzigen Schema des § 6b BDSG: Prüfung berechtigter Interessen. Auch hier werden wieder konkrete Tatsachen gefordert, die eine Gefährdung belegen, die Erforderlichkeit (mildere Mittel, Geeignetheit und das „Wie“ der Videoüberwachung) und die Abwägung von berechtigtem Interesse und schutzwürdigen Interessen der Betroffenen, wobei nicht nur Anhaltspunkte für das Überwiegen der schutzwürdigen Interessen vorliegen dürfen. Hier ist eine tatsächliche Interessenabwägung durchzuführen. Inwieweit sich dies bei der Zulässigkeitsprüfung auswirkt, ist noch nicht absehbar. Die hier gemachten Hinweise sind nicht abschließend und aufgrund der Erarbeitung von weiteren Kriterien noch im Fluss. Die bisher erarbeitete Orientierungshilfe „Videoüberwachung für nicht-öffentliche Stellen“ wird hinsichtlich der Vorgaben des neuen Gesetzes überarbeitet und gleichzeitig wird es ein Kurzpapier „Videoüberwachung“ geben, welches die wichtigsten

Neuerungen darstellen wird. Beides wird, sobald vorhanden, auf der Website des TLfDI bereitgestellt. Sofern sich weitere Fragen hierzu ergeben, wird der TLfDI gerne erneut beratend tätig.
Zusammenfassend lässt sich sagen, dass sich die Wohnungsunternehmungen darauf einstellen müssen, dass auch nach der neuen Rechtslage strenge Anforderungen an das Betreiben einer Videoüberwachungsanlage seitens der Aufsichtsbehörden gestellt werden. Es bleibt dabei: Jede Videoüberwachung ist eine Einzelfallbetrachtung.

Sowohl § 25a ThürDSG als auch § 6b BDSG verlangen für die Zulässigkeit einer Videoüberwachung, dass diese erforderlich sein muss. Was erforderlich ist, ist immer einer Frage des Einzelfalls. Denn hier kommt es darauf, welche Vorfälle aus der Vergangenheit den Einsatz einer Videoüberwachung rechtfertigen. Ob der neue § 4 BDSG den europarechtlichen Vorgaben genügt, wird mit Sicherheit ein Gericht entscheiden.

2.5 Thüringer Meldeverordnung

Mit dem Gesetz zur Fortentwicklung des Meldewesens vom 3. Mai 2013 hatte der Bund durch das Inkrafttreten des Bundesmeldegesetzes von seiner ausschließlichen Gesetzgebungskompetenz Gebrauch gemacht und damit die Länder zur entsprechenden Aufhebung ihrer Meldegesetze verpflichtet. Ferner war das Thüringer Ausführungsgesetz zum Bundesmeldegesetz erlassen worden, das zeitgleich (1. November 2015) mit dem Bundesmeldegesetz in Kraft treten musste. Ergänzend dazu war zur Ausfüllung der Regelungsbefugnis eine Rechtsverordnung erforderlich.
Im vorherigen Berichtszeitraum (11. TB) war der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) vom Thüringer Ministerium für Inneres und Kommunales (TMIK) gebeten worden, zum Referentenentwurf einer neuen Thüringer Meldeverordnung (ThürMeldeVO) Stellung zu nehmen.
Der TLfDI hat dem TMIK nach entsprechender Prüfung zum Entwurf der neuen ThürMeldeVO empfohlen, für Zwecke der Protokollierung des Datenein- und -ausgangs sowie zur Absicherung langfristig angelegter Datenübermittlungsmaßnahmen den Altdatensatz längstens für zwölf Monate und nicht, wie im Entwurf ursprünglich vorgesehen, bis „längstens zum Ende des Jahres, welches der Aktua-

lisierung …folgt“ aufzubewahren (§ 3 Abs. 2 Satz 3 ThürMeldeVO). Dies ergab sich für den TLfDI unter anderem aus § 16 Abs. 1 Nr. 2 Thüringer Datenschutzgesetz, wonach personenbezogene Daten zu löschen sind, wenn ihre Kenntnis für die Daten verarbeitende Stelle zur Erfüllung ihrer Aufgaben nicht mehr erforderlich ist.
Dieser Empfehlung des TLfDI war das TMIK gefolgt.
Aus technischer Datenschutzsicht hatte der TLfDI keine Einwendungen.
Die Thüringer Meldeverordnung (ThürMeldeVO) trat zwar am 1. November 2015 in Kraft, war aber zum Berichtszeitraum-Ende des 11. Tätigkeitsberichtes noch nicht ausgefertigt (Ausfertigungsdatum: 21. Januar 2016).

Sind für Zwecke der Protokollierung des Datenein- und -ausgangs sowie zur Absicherung langfristig angelegter Datenübermittlungsmaßnahmen Altdatensätze nicht mehr erforderlich, müssen sie gemäß § 16 Abs. 1 Nr. 2 ThürDSG gelöscht werden.



Schilder Datenaustausch zwischen USA und EU – © kamasigns / Fotolia.com

3. Europäischer und Internationaler Datenschutz

3.1 Die Datenschutz-Grundverordnung (DS-GVO) kommt ...

Die bahnbrechende Neuerung auf dem Gebiet des Datenschutzrechts ist im Berichtszeitraum die „Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG“, kurz: die Datenschutz-Grundverordnung (DS-GVO), die am 25. Mai 2016 in Kraft getreten ist und ab dem 25. Mai 2018 innerhalb der Europäischen Union Geltung erlangen wird.
Sie ersetzt die aus dem Jahr 1995 stammende „Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr“ (EG – Datenschutz-Richtlinie), die von den EU-Mitgliedstaaten in nationales Recht umgesetzt werden musste. Mit dieser Richtlinie wollte der europäische Gesetzgeber die verschiedenen Datenschutzregeln der Mitgliedstaaten auf einem hohen Schutzniveau vereinheitlichen und beste-

hende Handelshemmnisse im Binnenmarkt abbauen (siehe EG 11 DS-RL). Diese kommt derzeit noch zur Anwendung und ihre Umsetzung in nationales Recht findet sich im Bundesdatenschutzgesetz (BDSG) und im Thüringer Datenschutzgesetz (ThürDSG).
Da die Umsetzung der EU-Richtlinie in der Praxis nicht immer in allen Mitgliedstaaten zufriedenstellend funktionierte, wurde nun zur Regelung des EU-Datenschutzes auf die Rechtsform einer Verordnung (DS-GVO) zurückgegriffen. Im Gegensatz zu Richtlinien sind Verordnungen allgemein und unmittelbar geltende und in allen Teilen verbindliche Rechtsakte. Die Datenschutz-Grundverordnung gilt damit unmittelbar in allen EU-Mitgliedstaaten.
Die DS-GVO hat trotz der gewählten Rechtsform als Verordnung insgesamt 48 Öffnungsklauseln, die den Mitgliedstaaten ähnlich wie eine Richtlinie einen Gesetzgebungsspielraum einräumen, wie sie das nationale Datenschutzrecht ausgestalten. Um diese Öffnungsklauseln mit Leben zu füllen, wurde das Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 am 30. Juni 2017 vom deutschen Bundestag mit Zustimmung des Bundesrates verabschiedet, kurz: Datenschutz-Anpassungs- und Umsetzungsgesetz EU (DSAnpUG-EU). Siehe hierzu auch Punkt 3.2. Als Artikel 1 dieses Gesetzes wurde das neue Bundesdatenschutzgesetz (BDSG-neu) verabschiedet, welches ebenfalls ab dem 25. Mai 2018 gilt und die nationalen Regelungen, also die Ausfüllung der Öffnungsklauseln, enthält. Weiterhin ist es natürlich auch notwendig, alle landesgesetzlichen Regelungen zum Datenschutz an die neue Verordnung anzupassen. In Thüringen wird dies mit dem neuen Thüringer Datenschutzgesetz geschehen, welches derzeit im Entwurf vom 19. September 2017 vorliegt. Siehe hierzu auch Punkt 3.6. Auch alle anderen bestehenden Gesetze mit datenschutzrechtlichen Bezügen müssen auf den Prüfstand, um ihre Vereinbarkeit mit der DS-GVO abzuklären. Dies wird ein umfangreicher und spannender Prozess, der bis zur Geltung der DS-GVO am 25. Mai 2018 zum Abschluss gebracht werden muss.
In diesem Prozess ist der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) stark gefordert. Alle Arbeitskreise und Arbeitsgruppen der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) beschäftigen sich damit, wie die Umsetzung der Richtlinie bis zu ihrem Wirksamwerden effektiv begleitet werden kann. Dazu werden gemeinsa-

me Arbeitspapiere erarbeitet und zur Verfügung gestellt. Die von der DSK gemeinsam erstellten und verabschiedeten „Kurzpapiere“ zu den verschiedenen Neuerungen der DS-GVO (siehe Anlage 61 bis Anlage 71) beziehen sich auf den nicht-öffentlichen Bereich und werden fortlaufend weiter von der DSK veröffentlicht. Sie sind auf der Homepage des TLfDI zu finden (https://www.tlfdi.de/tlfdi/europa/europaeischeDS-GVO/). Sie können für den öffentlichen Bereich als Orientierung verstanden werden. Der TLfDI wird auf seiner Internetseite dazu ergänzende Hinweise veröffentlichen. Auch auf Landesebene gibt es zahlreiche Fragen zur Umsetzung der DS-GVO im öffentlichen wie auch im nicht-öffentlichen Bereich. Der TLfDI hat auch im Rahmen der Einführung und Umsetzung der DS-GVO verschiedene Pressemitteilungen veröffentlicht und zahlreiche Vorträge gehalten. Diese sind ebenfalls im Anhang zu finden.



Mit der DS-GVO wird das Datenschutzrecht EU-weit vereinheitlicht. Die DS-GVO behält im Wesentlichen die bisherigen datenschutzrechtlichen Grundprinzipien bei und entwickelt sie weiter. Die Grundprinzipien des „Verbots mit Erlaubnisvorbehalt“, der „Datenvermeidung und Datensparsamkeit“, der „Zweckbindung“ und der „Transparenz“ prägen auch die DS-GVO.

Die Verordnung regelt unter anderem die Grundsätze für die Verarbeitung personenbezogener Daten in Artikel 6, die Rechte der Betroffenen in den Artikeln 12 ff. und die Pflichten der Verantwortlichen und Auftragsverarbeiter in Art. 24 ff. Die bereits geltenden Betroffenenrechte, wie z. B. die Transparenz der Informationen, Auskunftsrecht der betroffenen Person, Recht auf die Berichtigung unrichtiger Daten, Datenlöschung, das allgemeine Widerspruchsrecht, werden um neue Rechte ergänzt, z. B. um das Recht auf Datenportabilität in Art. 20 DS-GVO. Es beinhaltet das Recht des Betroffenen, seine personenbezogenen Daten von dem einen Verantwortlichen in einem maschinenlesbaren Format zu erhalten und an einen anderen Verantwortlichen zu übermitteln. Das Recht auf Datenlöschung wird in der DS-GVO als das „Recht auf Vergessenwerden“ bezeichnet.

Als zentrale Norm der DS-GVO regelt Art. 5 die Grundsätze zur Verarbeitung personenbezogener Daten. Diese Grundsätze sind die

Rechtmäßigkeit der Verarbeitung, Verarbeitung nach Treu und Glauben, Transparenz der Verarbeitung, die Zweckbindung, die Datenminimierung, Richtigkeit der Daten, Speicherbegrenzung, Integrität und Vertraulichkeit und die Rechenschaftspflicht.

Personenbezogene Daten dürfen nur auf „rechtmäßige Weise“ verarbeitet werden. Was eine rechtmäßige Verarbeitung nach DS-GVO ist, definiert Art. 6 DS-GVO und legt Bedingungen fest, die erfüllt sein müssen. Die Verarbeitung von Daten ist demnach nur zulässig, wenn eine Einwilligung oder eine andere in der DS-GVO oder im nationalen Recht normierte Rechtsgrundlage (besondere Erforderlichkeit nach Art. 6 Abs. 1 Buchstabe b-f DS-GVO) vorliegt, z. B. wenn sie zur Erfüllung eines Vertrages oder eines vorvertraglichen Schuldverhältnisses mit dem Betroffenen erforderlich ist, Art. 6 Abs. 1 Buchstabe B DS-GVO. Die Voraussetzungen für eine Einwilligung ergeben sich aus der Begriffsbestimmung in Art. 4 Nr. 11 DS-GVO und sind weitestgehend identisch mit den bisherigen Anforderungen (freiwillig, zweckbestimmt und informiert). Allerdings werden die formalen Anforderungen an eine wirksame Einwilligung präzisiert. Nach Erwägungsgrund (EG) 42 muss die Einwilligungserklärung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zur Verfügung gestellt werden. Weitere Bedingungen für die wirksame Erteilung der Einwilligung sind in Art. 7 und 8 DS-GVO geregelt (Nachweis, schriftliche Erklärung, Widerruf).

Personenbezogene Daten müssen zudem nach „Treu und Glauben“ und in einer für den Betroffenen nachvollziehbaren Art und Weise, also transparent, verarbeitet werden. Die Ausgestaltung dieser Transparenz findet in den umfangreichen Informationspflichten (Art. 13 DS-GVO) und Auskunftsansprüchen (Art. 14 DS-GVO) ihren Niederschlag, deren Erfüllung durch den Verantwortlichen ebenfalls umfangreich geregelt ist (Art. 12 DS-GVO). Personenbezogene Daten dürfen nur für festgelegte, eindeutige und rechtmäßige Zwecke erhoben werden, Zweckbindungsgrundsatz Art. 5 Abs. 1 DS-GVO. Die Verarbeitung personenbezogener Daten muss dem Zweck angemessen und sachlich relevant sein. Die Erhebung der Daten muss auf das für den Zweck der Datenverarbeitung notwendige Maß beschränkt sein, Datenminimierungsgrundsatz gem. Art. 5 Abs. 2 Buchstabe c DS-GVO. Das Prinzip der Speicherbegrenzung ergänzt die Datensparsamkeit in zeitlicher Hinsicht. Auch die Gewährleistung von Integrität und Vertraulichkeit, also die Datensi-

cherheit, ist nun gesetzlich verankert, Art. 5 Abs. 1 Buchstabe f und Art. 32 DS-GVO. Das bedeutet, dass Daten in einer Weise verarbeitet werden müssen, die eine angemessene Sicherheit gewährleistet, einschließlich des Schutzes durch geeignete technische und organisatorische Maßnahmen, Art. 24 Abs. 1 DS-GVO.
Die DS-GVO stellt insbesondere die Bedeutung des technischen und organisatorischen Datenschutzes heraus. Art. 25 DS-GVO normiert den Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen, sogenanntes Privacy by Design und Privacy by Default. Das bedeutet, der Verantwortliche muss sicherstellen, dass Standardeinstellungen darauf ausgerichtet sind, nur personenbezogene Daten zu verarbeiten, die für den konkreten Zweck auch erforderlich sind. Das betrifft den Umfang der erhobenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit.
Es finden sich weiterhin auch Regelungen zur Auftragsdatenverarbeitung (neu: Auftragsverarbeitung), Art. 28 DS-GVO; zur Meldung über Datenschutzverletzungen, Art. 33 f. DS-GVO und zum betrieblichen Datenschutzbeauftragten, Art. 37 DS-GVO.
Eine Datenschutz-Folgeabschätzung Art. 35 DS-GVO, ist stets erforderlich, wenn eine Datenverarbeitung, insbesondere bei der Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke, voraussichtlich zu einem hohen Risiko für die Rechte und Freiheiten einer natürlichen Person führt. Dann muss der Verantwortliche vorab eine Abschätzung der Folgen der Verarbeitungsvorgänge vornehmen und bewerten sowie auf ein Mindestmaß durch die Ergreifung geeigneter Maßnahmen reduzieren. Die Datenschutz-Folgenabschätzung tritt an die Stelle der Vorabkontrolle durch den betrieblichen Datenschutzbeauftragten bzw. die Meldepflicht nach BDSG.
Der betriebliche/behördliche Datenschutzbeauftragte wird in Art. 37 DS-GVO geregelt. Nach Art. 37 Abs. 1 DS-GVO müssen in drei Fällen interne Datenschutzbeauftragte bestellt werden:
Öffentliche Stellen haben, sofern sie personenbezogene Daten verarbeiten, stets einen Datenschutzbeauftragten zu bestellen. Nichtöffentliche Stellen haben einen Datenschutzbeauftragten zu bestellen, wenn deren Kerntätigkeit in einer Datenverarbeitung besteht, die aufgrund ihres Zwecks oder ihres Umfangs eine umfangreiche, regelmäßige und systematische Überwachung von betroffenen Personen erfordert oder eine umfangreiche Verarbeitung von Daten, die

nach Art. 9 oder 10 DS-GVO besonders schutzwürdig sind, umfasst (u. a. Gesundheitsdaten). Die DS-GVO erlaubt zudem, dass die Mitgliedstaaten im nationalen Recht für weitere Fälle die Bestellung eines Datenschutzbeauftragten vorschreiben können. Hiervon hat der Bundesgesetzgeber in § 38 Abs. 1 BDSG-neu Gebrauch gemacht. Danach werden nicht-öffentliche Stellen auch künftig einen Datenschutzbeauftragten zu bestellen haben, wenn in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind. Neu ist allerdings, dass künftig nicht mehr der Datenschutzbeauftragte, sondern vielmehr der Verantwortliche selbst sowohl für die Führung des Verzeichnisses über Verarbeitungstätigkeiten nach Art. 30 DS-GVO als auch für die Datenschutz-Folgenabschätzung verantwortlich ist.

Mit dem Grundsatz der Rechenschaftspflicht in Art. 5 Abs. 2 DS-GVO wird der Verantwortliche ebenfalls stärker in die Pflicht genommen. Das bedeutet, dass er die Grundsätze aus Art. 5 DS-GVO nicht nur einhalten muss, er muss ihre Einhaltung auch nachweisen können. Damit tragen die Verantwortlichen beispielsweise die Darlegungs- und Beweislast dafür, dass die Betroffenen in die Datenverarbeitung eingewilligt haben. Die sorgfältige Dokumentation und Protokollierung der Abläufe ist daher für den Verantwortlichen künftig unverzichtbar.

Die DS-GVO gilt auch für Unternehmen, die ihren Sitz zwar außerhalb der Europäischen Union haben, sich mit ihren Angeboten aber an EU-Bürger richten und wenden, das sogenannte Marktortprinzip an. Damit wird der Anwendungsbereich des in Thüringen geltenden Datenschutzrechts erheblich ausgeweitet.

Effektiver Datenschutz erfordert auch die Möglichkeit einer effektiven Durchsetzung. Die DS-GVO sieht im Vergleich zur Datenschutzrichtlinie umfangreichere Befugnisse für die Datenschutzaufsichtsbehörden vor. Zudem werden die Sanktionsmöglichkeiten der Aufsichtsbehörden ausgedehnt. Auch gegenüber dem öffentlichen Bereich bestehen künftig Anordnungsbefugnisse. Die erweiterten Befugnisse werden ebenfalls durch eine spürbare Ausweitung des Bußgeldrahmens flankiert (Art. 83 DS-GVO). Die Geldbuße nach der DS-GVO hat in den Fällen des Art. 83 Abs. 5 und Abs. 6 DS-GVO wirksam, verhältnismäßig und abschreckend zu sein. So sind für bestimmte Rechtsverstöße Bußgelder bis zu 4 Prozent des Jahresumsatzes eines Unternehmens, beziehungsweise 20 Mio. Euro, zulässig.

Die DS-GVO und ihre Umsetzung sind eine datenschutzrechtliche Herausforderung, die alle Bereiche der Gesellschaft in unterschiedlichen Ausprägungen betrifft und fordern wird. Wie genau die Auswirkungen, die auf die öffentliche Verwaltung oder Unternehmen und nicht zuletzt auch auf die Datenschutzbehörden zukommen, aussehen werden, lässt sich derzeit nicht abschließend beurteilen. Mit der DS-GVO wird das Datenschutzrecht in allen Mitgliedstaaten vereinheitlicht und so erstmals eine unmittelbar geltende, gemeinschaftliche und wirksame Grundlage geschaffen. Die Umsetzung der durch die Öffnungsklauseln eingeräumten Befugnisse der Mitgliedstaaten kann zwar Abweichungen in einzelnen Belangen bedeuten, das grundsätzliche Datenschutzniveau bleibt aber erhalten. Der TLfDI wird bei Fragen und Problemen zur Anwendung der DS-GVO den Behörden und Unternehmen sowie den Bürgern als Betroffenen gern beratend zur Seite stehen.

3.2 Das neue BDSG – eine schwere Geburt ...

Am 24. Mai 2016 trat die Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung [DS-GVO]) in Kraft. Die Europäische Union (EU) wollte mit der Verordnung Regelungen für die Verarbeitung von personenbezogenen Daten durch private Unternehmen und öffentliche Stellen EU-weit verbindlich vereinheitlichen. Dadurch sollte einerseits der Schutz von personenbezogenen Daten innerhalb der EU sichergestellt und andererseits der freie Datenverkehr innerhalb des Binnenmarkts gewährleistet werden. Die DS-GVO sieht eine zweijährige Übergangsfrist vor, weshalb sie erst ab dem 25. Mai 2018 anzuwenden ist. Im Gegensatz zur bisher geltenden Datenschutzrichtlinie (95/46/EG), die von den Mitgliedsstaaten zunächst in nationales Recht umgesetzt werden musste, gilt die DS-GVO unmittelbar in allen EU-Mitgliedsstaaten. Die DS-GVO geht dem mitgliedsstaatlichen Recht vor. Sie bringt etliche Neuerungen gegenüber dem in Deutschland geltenden Datenschutzrecht mit sich. Zwar enthält sie zahlreiche Öffnungsklauseln, die dem nationalen Gesetzgeber ermöglichen, bestimmte Sonderregelungen bzw. abweichende Regelungen zu treffen; ein Großteil der Regeln gilt jedoch unmittelbar

und kann auch durch den nationalen Gesetzgeber nicht geändert werden. Eine wesentliche Neuerung der DS-GVO ist beispielsweise die Stärkung der Betroffenenrechte. Die Informationspflichten gegenüber den Betroffenen sind ausgeweitet worden (Artikel 13 und 14 DS-GVO) und es gibt einen Anspruch auf klare und leicht verständliche Informationen (Artikel 12 Abs. 1 DS-GVO). Die Einwilligung in die Datenverarbeitung ist grundsätzlich erst ab 16 Jahren möglich (Artikel 8 DS-GVO) und der Anspruch auf Löschung wurde durch das Recht auf Vergessenwerden (Artikel 17 DS-GVO) gestärkt.
Neu ist das sogenannte Marktortprinzip des Artikel 3 Abs. 2 DS-GVO, das den räumlichen Anwendungsbereich auf Daten verarbeitende Stellen außerhalb der EU ausweitet, soweit sie Waren oder Dienstleistungen auf dem Gebiet der EU anbieten, und zwar auch, wenn dies unentgeltlich geschieht. Die Datenschutzaufsichtsbehörde erhält zahlreiche neue Aufgaben und Befugnisse und es gibt einheitliche Regelungen für den öffentlichen und nicht-öffentlichen Bereich. Allerdings sind im öffentlichen Bereich nach einigen Öffnungsklauseln Ausnahmen möglich.
Wer den Regelungsgehalt der DS-GVO studiert hatte, dem war schnell klar, dass das geltende Datenschutzrecht in Deutschland überarbeitet werden muss. Dies gilt sowohl auf Landesebene für das Thüringer Datenschutzgesetz (vgl. Punkt 3.6) als auch für das Bundesdatenschutzgesetz (BDSG) auf Bundesebene. Bereits früh setzten sich die Datenschutzaufsichtsbehörden des Bundes und der Länder mit der Frage auseinander, wie ein neues BDSG ausgestaltet werden sollte. Im April des Jahres 2016 wies die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) in ihrer Entschließung „Stärkung des Datenschutzes in Europa – nationale Spielräume nutzen“ darauf hin, dass es aus ihrer Sicht wichtig sei, die in der DS-GVO enthaltenen Öffnungs- und Konkretisierungsklauseln zugunsten des Rechts auf informationelle Selbstbestimmung zu nutzen. Wichtig sei insbesondere die Schaffung eines Beschäftigtendatenschutzgesetzes, die Beschränkung für die Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten, die Stärkung der Befugnisse der Aufsichtsbehörden insbesondere durch Schaffung von Klagebefugnissen und effektiven Sanktionen auch gegenüber Behörden, die Begrenzung der Zweckänderung bei Videoüberwachung öffentlich zugänglicher Räume durch Private und die Beibehaltung der Verpflichtung, einen betrieblichen Datenschutzbeauftragten zu bestellen.

Nach dem der Referentenentwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 öffentlich gemacht worden war, wurde der Entwurf unter den Aufsichtsbehörden rege diskutiert. Der Gesetzentwurf, der auch das neue BDSG enthielt, fand nicht nur Zustimmung bei den Aufsichtsbehörden. Die DSK erarbeitete gemeinsam 13 Änderungsanträge, die im Bundesrat in das Gesetzgebungsverfahren eingebracht werden sollten. Diese Anträge übermittelte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) dem Chef der Thüringer Staatskanzlei mit der Bitte, darauf hinzuwirken, dass Thüringen im Bundesrat die vorgeschlagenen Änderungsanträge stellt bzw. ihnen beitritt.
Die Anträge befassten sich mit der Zuständigkeit der federführenden Aufsichtsbehörde sowie der Frage der Vertretung im Europäischen Datenschutzausschuss. Es sollen Regelungen gestrichen werden, die die Betroffenenrechte einschränken, die Kontrolle von Berufsgeheimnisträgern sollte nicht erschwert werden, es sollten spezielle Regelungen zum Beschäftigtendatenschutz getroffen werden. Ein Klagerecht der Aufsichtsbehörde bei Verstößen gegen die DS-GVO wurde ebenso gefordert wie eine Änderung der Regelungen zur Videoüberwachung. Zwar wurde der Gesetzentwurf aufgrund einer Stellungnahme des Bundesrats in einigen Punkten geändert. Andere Vorschläge wurden aber nicht übernommen. Das neue BDSG wurde am 27. April 2017 vom Bundestag verabschiedet und tritt mit Wirksamwerden der DS-GVO am 25. Mai 2018 in Kraft. Nach Auffassung des TLfDI gibt es weiterhin wesentliche Kritikpunkte:
Eine sehr einschneidende Regelung für die Aufgabe der Aufsichtsbehörde ist die Einschränkung der Untersuchungsbefugnisse der Aufsichtsbehörden bei Berufsgeheimnisträgern, nach § 29 Abs. 3 BDSG-neu. Insofern wird auch auf die Pressemitteilung des TLfDI vom 25. November 2016 (https://www.tlfdi.de/mam/tlfdi/presse/kontrollfreie_zonen_besonders_sensible_daten.pdf) verwiesen.



Die Vorschrift zur Videoüberwachung öffentlich zugänglicher Räume (§ 4 BDSG-neu) lässt sich, soweit sie nicht-öffentliche Stellen betrifft, nicht auf den herangezogenen Artikel 6 Abs. 1 Satz 1 Buchstabe e in Verbindung mit Artikel 6 Abs. 3 Satz 1 DS-GVO stützen.

§ 26 BDSG-neu übernimmt leider weitgehend die bisher geltenden Regeln des § 32 BDSG. Diese sind, wie die Praxis erwiesen hat, jedoch unzureichend. Die digitale Arbeitswelt erweitert die Möglichkeit der offenen und versteckten technischen Überwachung von Mitarbeitern erheblich. Hier muss ein angemessener Ausgleich zwischen den Informationsinteressen des Arbeitgebers und dem Schutz der Rechte und Freiheiten des Arbeitnehmers durch eine differenzierte und umfassende gesetzliche Regelung geschaffen werden. Dies sind nur einige wichtige Kritikpunkte an der neuen gesetzlichen Regelung. Die DSK hat sich daher nach der Bundestagswahl mit dem Papier „Grundsatzpositionen und Forderungen für die neue Legislaturperiode“ an den künftigen Gesetzgeber gewandt und dargelegt, welche Änderungen aus ihrer Sicht erforderlich sind, um ein angemessenes und europarechtskonformes Datenschutzrecht in Deutschland zu schaffen (vgl. 0). Wie sich das neue BDSG bewährt, wird die Praxis zeigen müssen. Bei Kollisionen zwischen neuem BDSG und der DS-GVO wird der Anwendungsvorrang des Europarechts zum Zuge kommen, sodass in diesem Falle nationales Recht nicht zur Anwendung gelangt. Insofern kann man schon auf den nächsten Tätigkeitsbericht des TLfDI im nicht-öffentlichen Bereich gespannt sein, wenn erste Anwendungsfälle nach dem BDSG-neu vorliegen.

Die Datenschutz-Grundverordnung schafft ab 28. Mai 2018 in allen Mitgliedstaaten der Europäischen Union in einigen Bereichen völlig neues Datenschutzrecht. Daher müssen die gesetzlichen Regelungen sowohl auf Bundes- als auch auf Landesebene an die neue verbindliche Datenschutz-Grundverordnung angepasst werden. Der TLfDI hat den Gesetzgebungsprozess des Bundes gemeinsam mit den anderen Aufsichtsbehörden des Bundes und der Länder kritisch begleitet. Da die Konferenz der unabhängigen Aufsichtsbehörden des Bundes und der Länder mit einigen getroffenen Regelungen im neuen BDSG nicht zufrieden ist, hat sie in einem Grundsatzpapier Forderungen für die neue Legislaturperiode aufgestellt.

3.3 Umsetzung JI-Richtlinie in nationales Recht

Bis zum 6. Mai 2018 müssen die Mitgliedstaaten die Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbei-

tung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. L 119 vom 4. Mai 2016, S. 89 ff.) (nachfolgend: JI-Richtlinie genannt) in nationales Recht umsetzen. Anders als bei Verordnungen bleibt es den Mitgliedstaaten grundsätzlich überlassen, wie sie Richtlinien umsetzen (Artikel 288 Absatz 3 Vertrag über die Arbeitsweise der Europäischen Union – AEUV). Sie haben bei der Umsetzung einen gewissen Spielraum.

Diese JI-Richtlinie, bei der der Buchstabe J für Justiz und der Buchstabe I für Inneres steht, beabsichtigt die Thüringer Landesregierung in einem neuen Thüringer Datenschutzgesetz umzusetzen. Dieses neue Thüringer Datenschutzgesetz soll auch die am 25. Mai 2018 in Kraft tretende Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4. Mai 2016, S. 1 ff.) berücksichtigen, die dann unmittelbar geltendes Recht in allen Mitgliedstaaten der Europäischen Union sein wird.

Im Rahmen der Ressortabstimmung für ein neues Thüringer Datenschutzgesetz wurde auch der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) um Stellungnahme gebeten, die er auch im Sommer 2017 vor dem Hintergrund der Umsetzung der JI-Richtlinie abgab:

Hinsichtlich des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung hielt sich der Thüringer Gesetzentwurf prinzipiell sehr eng an die Vorgaben der JI-Richtlinie, sodass insoweit vonseiten des TLfDI keine Kritik zu üben war. Hiervon gab es allerdings eine gravierende Ausnahme hinsichtlich der Befugnisse des TLfDI, die im neuen Thüringer Datenschutzgesetz vorgesehen sind.

Einschlägig ist hier § 7 Abs. 5 ThürDSG-Entwurf, der folgenden Wortlaut hatte:

„(5) Stellt der Landesbeauftragte für den Datenschutz bei der Verarbeitung personenbezogener Daten, die nicht im Anwendungsbereich der Verordnung (EU) 2016/679 erfolgt, Verstöße gegen die

Vorschriften des Datenschutzes fest, so beanstandet er dies gegenüber der zuständigen obersten Landesbehörde und fordert diese zur Stellungnahme innerhalb einer von ihm zu bestimmenden Frist auf. Der Landesbeauftragte für den Datenschutz kann von einer Beanstandung absehen oder auf eine Stellungnahme verzichten, insbesondere wenn es sich um unerhebliche oder inzwischen beseitigte Mängel handelt. Die Stellungnahme soll auch eine Darstellung der Maßnahmen enthalten, die aufgrund der Beanstandung getroffen worden sind. Der Landesbeauftragte für den Datenschutz kann den Verantwortlichen auch davor warnen, dass beabsichtigte Verarbeitungsvorgänge voraussichtlich gegen in diesem Gesetz enthaltene und andere auf die jeweilige Datenverarbeitung anzuwendende Vorschriften über den Datenschutz verstoßen."

Im Ergebnis sollte es also beim bisherigen Beanstandungsmodell bleiben.

Demgegenüber sieht die JI-Richtlinie Folgendes vor:

„Art. 47 – Befugnisse

(2) Jeder Mitgliedstaat sieht durch Rechtsvorschriften vor, dass jede Aufsichtsbehörde über wirksame Abhilfebefugnisse wie etwa die beispielhaft genannten folgenden verfügt, die es ihr gestatten, […]

b) den Verantwortlichen oder den Auftragsverarbeiter ***anzuweisen****, Verarbeitungsvorgänge, gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums, mit den nach dieser Richtlinie erlassenen Vorschriften in Einklang zu bringen, insbesondere durch die* ***Anordnung der Berichtigung oder Löschung personenbezogener Daten*** *oder Einschränkung der Verarbeitung gemäß Artikel 16;*

c) eine vorübergehende oder endgültige ***Beschränkung der Verarbeitung****, einschließlich eines* ***Verbots, zu verhängen."***

Die Befugnis, Anordnungen und Verbote zu erlassen, ist eindeutig als ein stärkeres Instrumentarium im Vergleich zur „bloßen" Beanstandungsmöglichkeit zu klassifizieren. In diesem Punkt war die Thüringer Regelung aus der Sicht des TLfDI nicht europarechtskonform und daher überarbeitungsbedürftig.

Auf die Kritik des TLfDI äußerte das Innenministerium, dass zur Umsetzung von Artikel 47 der Richtlinie (EU) 2016/680, Anordnungen und Verbote zu erlassen, eine spezialgesetzliche Regelung in § 45 Polizeiaufgabengesetz (PAG) (Artikel 2 des Thüringer Datenschutz-Anpassungs- und Umsetzungsgesetzes EU – ThürDSAnpUG-EU) erfolgen solle.

Prinzipiell ist nichts dagegen einzuwenden, die Befugnis, Anordnungen und Verbote zu erlassen, spezialgesetzlich in § 45 PAG zu regeln. Der Wortlaut der geplanten neuen Fassung der Vorschrift ist dem TLfDI bisher unbekannt. Es ist aber davon auszugehen, dass dieser nur für die Polizei gilt. Von der EU-Richtlinie werden aber auch weitere Strafverfolgungs- bzw. Justizbehörden erfasst (siehe § 33 ThürDSAnpUG-EU:

„§ 33

Die Vorschriften dieses Abschnitts gelten für die Verarbeitung personenbezogener Daten durch die für die Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Straftaten oder Ordnungswidrigkeiten zuständigen öffentlichen Stellen, soweit sie Daten zum Zweck der Erfüllung dieser Aufgaben verarbeiten. Die öffentlichen Stellen gelten dabei als Verantwortliche. Die Verhütung von Straftaten im Sinne des Satzes 1 umfasst den Schutz vor und die Abwehr von Gefahren für die öffentliche Sicherheit. Die Sätze 1 und 2 finden zudem Anwendung auf diejenigen öffentlichen Stellen, die für die Vollstreckung von Strafen oder Maßnahmen im Sinne des § 11 Abs. 1 Nummer 8 des Strafgesetzbuchs, von Erziehungsmaßregeln oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes und von Geldbußen zuständig sind. Soweit dieser Teil Vorschriften für Auftragsverarbeiter enthält, gilt er auch für diese.“

Die Abhilfe gegenüber der Forderung des TLfDI ist daher nur teilweise vom TMIK umgesetzt worden.

Die Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sieht die Befugnis für die Datenschutzbeauftragten vor, Anordnungen und Verbote zu erlassen. Demgegenüber sieht der bisherige Entwurf eines neuen Thüringer Datenschutzgesetzes für den TLfDI, wie bisher, nur eine Beanstandungsmöglichkeit vor. In diesem Punkt ist die geplante Thüringer Regelung nicht europarechtskonform und daher zu überarbeiten.

3.4 EU-US-Privacy Shield – vom unsicheren Hafen ([un-] Safe Harbor) zum löchrigen Schutzschild!

Bereits in seinem letzten Tätigkeitsbericht informierte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) ausführlich über das Urteil des Europäischen Gerichtshofs vom 6. Oktober 2015 (Az.: C-362/14), das das Safe Harbor-Abkommen (wörtlich: Sicherer-Hafen-Abkommen) für Übermittlungen von Daten aus der EU in die USA für ungültig erklärt hatte (siehe dazu die Nr. 3.1 des 11. Tätigkeitsberichts zum Datenschutz: Öffentlicher Bereich).
Nicht zuletzt aufgrund des massiven Drucks aus den Reihen der US-Wirtschaft war die EU-Kommission deshalb aufgefordert, schnell ein Nachfolge-Abkommen für Safe Harbor vorzulegen, damit Datenübermittlungen aus der EU in die USA weiterhin auf sicherer Rechtsgrundlage erfolgen können. Leider entschied sich die Kommission dabei für Schnelligkeit zulasten der Gründlichkeit. Die Kritik an dem im Februar 2016 vorgelegten EU-US-Datenschutzschild, dem Privacy Shield-Abkommen, fasste unter anderem die Artikel 29-Gruppe in ihren Arbeitspapieren WP 237 und WP 238 prägnant zusammen. Die Artikel 29-Gruppe, in der Datenschutzbeauftragte und/oder Mitarbeiter der europäischen Datenschutzbehörden vertreten sind, bezweifelte unter anderem, dass die Ombudsperson mit hinreichenden Kontrollbefugnissen ausgestattet und in ausreichendem Maße unabhängig sei. Ferner kritisierte die Artikel 29-Gruppe das Fehlen von Begrenzungen der Datenspeicherungsdauer bei Privacy Shield-zertifizierten Unternehmen.
Kritik am geplanten Privacy Shield-Abkommen kam im Frühjahr auch vom Artikel 31-Ausschuss. Dieses Gremium setzt sich aus Vertreterinnen und Vertretern der EU-Mitgliedstaaten zusammen und kommt immer dann zusammen, wenn es um Angemessenheitsentscheidungen zum Datenschutzniveau in Nicht-EU-Ländern geht. Im Fall von Privacy Shield konnte sich der Artikel 31-Ausschuss zunächst nicht auf eine Freigabe einigen. Deshalb führte die EU-Kommission mit der US-Administration Nachverhandlungen und präsentierte dem Artikel 31-Ausschuss einen zweiten Entwurf für das Privacy Shield-Abkommen, den dieser sodann annahm. Die Artikel 29-Gruppe wurde zum zweiten Entwurf hingegen nicht mehr angehört.

Am 12. Juli 2016 stellte dann die EU-Kommission die Angemessenheit des Privacy Shield fest und veröffentlichte die zugrunde liegenden Unterlagen (http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016D1250&from=DE).
Damit stellt sich zwangsläufig die Frage: Was beinhaltet Privacy Shield konkret?



Folgende Kernelemente bzw. Regelungen enthält das Privacy Shield-Abkommen:

- Ebenso wie sein Vorgänger, Safe Harbor, enthält auch das Privacy Shield-Abkommen eine ganze Reihe datenschutzrechtlicher Grundsätze, so z. B. zur Informationspflicht der durch Privacy Shield zertifizierten Unternehmen gegenüber Bürgern, zur Verantwortlichkeit für die Datenweitergabe oder zur Datenintegrität und Zweckbindung sowie zum Auskunftsrecht.
- Als wesentliche Neuerung regelt das Privacy Shield-Abkommen die Errichtung einer Ombudsstelle für den Bereich der nationalen Sicherheit. Dabei handelt es sich um einen leitenden Beamten im US-Außenministerium, der seine Tätigkeit unabhängig von den US-amerikanischen Geheimdiensten ausübt. Betroffene, deren Daten in die USA übermittelt wurden, können sich mit einer Anfrage hinsichtlich des Zugriffs auf diese Daten durch US-amerikanische Geheimdienste über die nationalen Aufsichtsbehörden in Europa an die Ombudsstelle wenden. Für die Einschaltung der Ombudsstelle findet sich auf der Seite des TLfDI das „Formular für die Übermittlung von Anträgen an die US-Ombudsstelle“ https://www.tlfdi.de/mam/tlfdi/datenschutz/safeharbor/ps_formular_ombudsstelle_tlfdi.pdf.



- Weiterhin besteht das Privacy Shield-Abkommen aus einem Konvolut aus Anlagen und Anhängen: Ministerielle Anschreiben mit Erläuterungen zum Rechtssystem in den USA, Verpflichtungserklärungen zur Umsetzung des Privacy Shields fallen hier ebenso darunter wie Erläuterungen zu den Zugriffen durch US-amerikanische Sicherheitsbehörden und Abfragen von Strafverfolgungsbehörden. Ferner enthalten sind Zusicherungen

der US-Administration, die der Absicherung der Betroffenenrechte dienen sollen.

- Schließlich sieht die Angemessenheitsentscheidung der EU-Kommission selbst vor, dass das Privacy Shield-Abkommen jährlich evaluiert werden soll. Vereinbart wurde deshalb von der EU-Kommission mit der US-Seite eine gemeinsame Prüfung, die alle Aspekte der Funktionsweise von Privacy Shield berücksichtigen soll, darunter insbesondere die Handhabung der aus den Gründen der nationalen Sicherheit und Strafverfolgung gewährten Ausnahmen.

Bei dem Stichwort der Ausnahmen aufgrund der Gewährleistung der US-Sicherheit ist man damit erneut bei der nicht verstummenden Kritik am Privacy Shield-Abkommen angelangt. Da die Artikel 29-Gruppe zum zweiten Entwurf des Privacy Shield-Abkommens nicht mehr angehört worden war, stellte sie in ihrem Arbeitspapier WP 238 weitere Kritikpunkte zum „Schutzschild“ in den Fokus: Gerade bei der Frage der sogenannten bulk collection, also der massenhaften und unterschiedslosen Datenerhebung, fehlte es aus der Sicht der Artikel 29-Gruppe an konkreten Zusicherungen, dass solche Mengen an Datenerhebungen von US-Seite nicht erfolgten. Insbesondere ein Schreiben aus dem Büro des – bereits in den Enthüllungen Edward Snowdens zu fragwürdiger Bekanntheit gelangten – Geheimdienstdirektors James Clapper zu den Beschränkungen und Garantien von Zugriffen US-amerikanischer Sicherheitsbehörden schuf hier mehr Fragen als Rechtsklarheit!

Somit bleibt festzuhalten, dass das Privacy Shield-Abkommen in zentralen datenschutzrechtlichen Fragen ebenso löchrig ist wie sein Vorgänger, das Safe Harbor-Abkommen. Insbesondere die wesentliche Kritik des EuGH an Safe Harbor, dass die EU-Kommission nicht ausreichend festgestellt habe, ob die USA aufgrund ihrer innerstaatlichen Regelungen oder internationalen Verpflichtungen ein angemessenes Datenschutzniveau bieten, ist nach den Einschätzungen vieler Datenschutzexperten auch dem Privacy Shield-Abkommen entgegenzuhalten.

Grundsätzliche Informationen zum Privacy Shield-Abkommen bietet der TLfDI unter https://www.tlfdi.de/mam/tlfdi/datenschutz/safeharbor/privacy_shield_website_1_tlfdi.pdf. Ferner hat der TLfDI ebenfalls auf seiner

Homepage ein Formular für die Einreichung von Beschwerden zum EU-US-Privacy Shield veröffentlicht: https://www.tlfdi.de/mam/tlfdi/datenschutz/safeharbor/ps_beschwerdeformular_tlfdi.pdf.



Der Europäische Gerichtshof (EuGH) wird sich in naher Zukunft erneut zu der Frage äußern, unter welchen Voraussetzungen eine Übermittlung personenbezogener Daten aus der EU in die USA zulässig ist: Anfang Oktober 2017 hat der Irische High Court mitgeteilt, dass er dem EuGH unter anderem die Frage zur Entscheidung vorgelegt hat, ob EU-Betroffene bei der Übermittlung ihrer personenbezogenen Daten durch Facebook Irland an Facebook USA unter Verwendung der Standardvertragsklauseln zur Auftragsdatenverarbeitung effektive Rechtsbehelfe im Sinne des Art. 47 EU-Grundrechtecharta haben für den Fall, dass ihre in die USA übermittelten Daten durch US-Behörden für Zwecke der nationalen Sicherheit verarbeitet werden.

Diese Standardvertragsklauseln, die die EU-Kommission zuletzt im Jahr 2010 herausgegeben hat, sollen ein Mindestmaß an Datenschutz gewährleisten. Möglicherweise wird der EuGH zu dieser Rechtsfrage erneut ein obiter dictum sprechen, dass dieses Mal auf jede Datenübermittlung in die USA zu beziehen ist.

Nach dem Safe Harbor-Urteil ist vor dem Privacy Shield-Urteil: Auch wenn sich die EU-Kommission um mehr Datenschutz bei der Übermittlung von personenbezogenen Daten in die USA bemüht und sehr rasch das Privacy Shield-Abkommen aus der Taufe gehoben hat, so bleibt doch zu konstatieren, dass dieser datenschutzrechtliche Schutzschirm extrem löchrig ist. Grund dafür ist wieder einmal die ausufernde Datensammelwut US-amerikanischer Geheimdienste. Daran könnte erneut vor allem der EuGH etwas ändern, wenn er die ihm gegebene Gelegenheit nutzen wird, die Datenübermittlung in die USA erneut unter die Lupe zu nehmen. Es bleibt also spannend…

3.5 Verabschiedung des Fluggastdatengesetzes der Bundesregierung – Privatsphäre von Reisenden adé

Mit Wirkung vom 10. Juni 2017 sind Teile des neuen Fluggastdatengesetzes (FlugDaG) in Kraft getreten. Weitere Teile treten im Mai 2018 in Kraft und dienen der Umsetzung einer EU-Richtlinie zur Verwendung von Fluggastdatensätzen.
Das neue Gesetz ermöglicht die Verwendung von Fluggastdatensätzen (Passenger Name Record Daten -PNR-) zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität. Hierdurch wird der bereits bestehende europaweite Austausch von Erkenntnissen zwischen den Mitgliedstaaten der Europäischen Union durch ein neues Instrument ergänzt. Zukünftig können die Fluggastdaten von den zuständigen Behörden der Mitgliedstaaten überprüft und unter engen Voraussetzungen ausgetauscht werden. Ein einzelner Datensatz umfasst hierbei bis zu sechzig Einzeldaten, z. B. Name, Geburtsdatum, Anschrift, Telefonnummer, E-Mail-Adresse, Angaben über Gepäck, Buchungs- und Flugdaten, Zahlungsinformationen etc.
Kritik über die Ausgestaltung des neuen FlugDaG kam indes u. a. aus den Reihen der Datenschützer. So kritisierte die Bundesbeauftragte für den Datenschutz, *„dass durch das Gesetz zwei grundsätzliche Datenschutzprobleme kombiniert werden. Zum einen schaffe es eine weitere Vorratsdatenspeicherung, bei der jährlich Fluggastdaten zu etwa 170 Millionen Passagieren in Deutschland unterschiedslos abgeglichen und über fünf Jahre gespeichert werden. Zudem werden sämtliche Flugreisende mit abstrakten Gefährderprofilen abgeglichen. Die Daten dienen dem Generieren von Verdächtigen, also dem Aufspüren von Reisenden, die eine Gefahr darstellen könnten und den Sicherheitsbehörden noch nicht bekannt sind. Ob ein solcher Abgleich mit der europäischen Grundrechtecharta vereinbar sei, sei noch nicht geklärt.“*
Der Gerichtshof der Europäischen Union (EuGH) hat sich zwar bis dato noch nicht zum Fluggastdatengesetz geäußert, jedoch stellte er im Juli 2017 in einem Gutachten fest, dass ein inhaltlich ähnliches Abkommen, hier das zwischen Kanada und der Europäischen Union über die Übermittlung von Fluggastdatensätzen, in seiner jetzigen Form nicht geschlossen werden dürfe, weil es unzulässigerweise in die Grundrechte der EU-Bürger eingreife.

Kritikpunkte sind hierbei nicht nur die lange Speicherdauer der Daten über fünf Jahre sowie die Möglichkeit, durch vorliegende Informationen auch Kenntnisse über das Privatleben der Fluggäste zu erlangen, sondern insbesondere auch der Mangel klarer und präziser Regularien für den Umgang mit den zugrundeliegenden Daten.
Des Weiteren steht auch die Frage im Raum, inwiefern sich die Eingriffe in die Grundrechtspositionen der Fluggäste auf das absolut notwendige Maß im Sinne der verfassungsrechtlich verankerten Verhältnismäßigkeit staatlicher Eingriffe beschränken lassen.
Zusammenfassend – so der EuGH – ist festzustellen, dass diverse Bestimmungen des geplanten Abkommens in seiner jetzigen Form nicht mit den Grundrechten vereinbar sind, sodass das Abkommen geändert werden muss, um die Eingriffe besser und genauer einzugrenzen. Bevor dahingehend keine Überarbeitung erfolgt ist, darf die geplante Übereinkunft zwischen Kanada und der EU nicht in Kraft treten.
Da das genannte Abkommen in seiner inhaltlichen Ausgestaltung, insbesondere im Hinblick auf die zu erhebenden und zu verarbeitenden Daten von Fluggästen sowie auf die zugrundeliegende Zweckbestimmung, jener des FlugDaG gleicht, wäre bei einer Prüfung durch den Gerichtshof der Europäischen Union ein ähnliches Ergebnis hinsichtlich der verfassungsrechtlichen Rechtmäßigkeit des FlugDaG zumindest nicht auszuschließen.

Der EuGH hat schon oft die „datenschutzrechtliche Fahne“ hoch gehalten und sowohl dem deutschen als auch dem europäischen Gesetzgeber die „rote Karte“ für die Verletzung datenschutzrechtlicher Mindeststandards gezeigt. Da die gutachterlichen Äußerungen des EuGH zum geplanten Fluggastdatenabkommen zwischen der EU und Kanada deutlich machten, dass der Datenaustausch zu weit gehe, liegt die Vermutung nahe, dass auch das neue Fluggastdatengesetz verfassungsrechtlich höchst bedenklich ist.

3.6 Anpassung des ThürDSG an die DS-GVO – auf dem Weg in den Thüringer Landtag

Die Datenschutz-Grundverordnung (DS-GVO), die ab dem 25. Mai 2018 wesentliche Bereiche des Datenschutzrechtes neu fasst oder ergänzt (siehe Punkt 3.1), machte es erforderlich, dass auch das Thüringer Datenschutzgesetz an dieses europäische Gesetz anzupas-

sen war. Im Sommer 2017 erreichte dazu den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) ein erster Referentenentwurf aus dem Thüringer Ministerium für Inneres und Kommunales (TMIK) für ein Thüringer Datenschutz-Anpassungs- und Umsetzungsgesetz EU (ThürDSAnpUG). Dieser Referentenentwurf war als sogenanntes Artikel-Gesetz konzipiert; das TMIK übersandte dem TLfDI aber lediglich den Inhalt des Artikels 1 – die Neufassung des Thüringer Datenschutzgesetzes (ThürDSG-E). Im Rahmen der ersten Ressortabstimmung machte der TLfDI dazu unter anderem folgende Ergänzungs- oder Verbesserungsvorschläge zum ThürDSG-E:

1. Der TLfDI wies auf die unbefriedigende, weil zu komplizierte Regelung des **§ 2 Abs. 2 Satz 1 und 2 ThürDSG-E** hin. Nach § 2 Abs. 2 ThürDSG-E gelten als öffentliche Stellen auch juristische Personen und sonstige Vereinigungen des privaten Rechts, die Aufgaben der öffentlichen Verwaltung wahrnehmen und an denen eine oder mehrere der in Absatz 2 genannten juristischen Personen des öffentlichen Rechts beteiligt sind. Gleiches gilt, wenn sich eine juristische Person oder sonstige Vereinigung des privaten Rechts, auf die das ThürDSG nach Satz 1 Anwendung findet, an einer weiteren Vereinigung des privaten Rechts beteiligt. Danach ist für diese juristischen Personen und sonstigen Vereinigungen des privaten Rechts grundsätzlich das ThürDSG anwendbar. Da die Regelung des § 2 Abs. 2 Satz 1 und 2 ThürDSG-E keine Angaben im Hinblick auf die Höhe der Beteiligung machen, reicht es für die Zuordnung als öffentliche Stelle aus, wenn die Beteiligung einer juristischen Person nach Abs. 1 nur zu 1 Prozent besteht. Etwas anderes gilt aber nach § 26, soweit diese als öffentliche Stellen geltenden juristischen Personen und sonstige Vereinigungen des privaten Rechts am Wettbewerb teilnehmen. Auf sie, auf ihre Zusammenschlüsse und Verbände sind von den Bestimmungen des ThürDSG nur die §§ 3 bis 12 anzuwenden; im Übrigen finden für sie die Bestimmungen des Teils 2 des Bundesdatenschutzgesetzes Anwendung.

Der TLfDI bewertete diese Regelung als in der Praxis schwierig handhabbar und unterbreitete daher für § 2 Abs. 1 ThürDSG-E folgenden, leichter verständlichen Formulierungsvorschlag:

„(1) Die Bestimmungen dieses Gesetzes gelten für die Verarbeitung und Nutzung personenbezogener Daten durch die Behörden, die

Gerichte und die sonstigen öffentlichen Stellen des Landes, der Gemeinden und Gemeindeverbände und die sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts (öffentliche Stellen). Als öffentliche Stellen im Sinne dieses Gesetzes gelten auch nicht-öffentliche Stellen, soweit sie hoheitliche Aufgaben der öffentlichen Verwaltung wahrnehmen."

Von dem Regelungsbereich dieses neu gefassten § 2 Abs. 1 ThürDSG-E herausnehmen wollte der TLfDI jedoch öffentlich-rechtliche Kreditinstitute und deren Vereinigungen, da diese Stellen zwar traditionell eine öffentlich-rechtliche Rechtsform besitzen, jedoch im Wettbewerb zu privatrechtlich organisierten Unternehmen stehen. Deshalb schlug der TLfDI gegenüber dem TMIK folgende Formulierung für § 2 Abs. 2 ThürDSG-E vor:

„(2) Absatz 1 gilt nicht für öffentlich-rechtliche Kreditinstitute und öffentlich-rechtliche Versicherungsanstalten und deren Vereinigungen. Auf sie finden die Bestimmungen des Bundesdatenschutzgesetzes über nicht-öffentliche Stellen Anwendung."

Schließlich empfahl der TLfDI in diesem Zusammenhang die Streichung des § 26 ThürDSG.

2. Auch die Frage, wer die Einhaltung des Datenschutzes bei Abgeordneten des Thüringer Landtags kontrolliert (siehe dazu den Beitrag 5.4 Zuständig oder nicht zuständig, das ist hier die Frage – Unterschriftenlisten auf dem Abgeordneten-Twitter-Account) thematisierte der TLfDI in seiner Stellungnahme aufgrund der im Rahmen seiner Arbeit aufgekommenen Unklarheiten zu dieser Frage. Angesichts der Tatsache, dass der datenschutzrechtliche Status von Abgeordneten im Rahmen ihrer parlamentarischen Mandatsausübung in der Literatur streitig diskutiert wird (siehe dazu *Dammann*, in: Simitis, BDSG, § 2 Rn. 29.; a. A. Hanloser in: Wolf/Brink, Datenschutzrecht in Bund und Ländern, 1. Auflage 2013, § 2, Rz. 50) empfahl der TLfDI dem TMIK, eine hinreichend klare Neuregelung in **§ 2 Abs. 6 ThürDSG-E** aufzunehmen.
3. Ergänzungsbedarf hatte der TLfDI auch bei **§ 3 Abs. 6 ThürDSG-E,** der unter anderem die Wahl, die Stellvertretung und die Weiterführung der Amtsgeschäfte im Falle des Ausscheidens des TLfDI regelt: Zum einen regte der TLfDI die Aufnahme einer Regelung an, nach der der Landesbeauftragte selbst eine seiner Mitarbeiterinnen / einen seiner Mitarbeiter zum Stellvertreter bestellen kann. Der TLfDI begründete dies

mit dem Gebot der Unabhängigkeit der Aufsichtsbehörde, selbst einen Stellvertreter in eigener Zuständigkeit zu bestellen. Zum anderen sollte die bestellte Stellvertreterin / der bestellte Stellvertreter des Landesbeauftragten die Befähigung zum Richteramt haben müssen. Grund hierfür war und ist die rechtlich komplexe und mit vielen Auslegungsfragen verbundene Materie der DS-GVO, in Verbindung mit dem BDSG und/oder dem ThürDSG.

4. Moniert wurde vom TLfDI auch der Regelungsgehalt des **§ 4 Abs. 7 ThürDSG-E**: Zum einen war hier nicht klar geregelt, wer die Personalstellen des Landesbeauftragten für den Datenschutz besetzt. Der TLfDI regte hier eine Klarstellung im Gesetzentwurf an.

   Zum anderen wies der TLfDI darauf hin, dass nach seinem Verständnis Artikel 52 Abs. 6 DS-GVO zu einer haushälterischen Unabhängigkeit des TLfDI vom Thüringer Landtag führe. Sofern die Bediensteten des TLfDI daher weiterhin Bedienstete bzw. Beamte des Thüringer Landtags sein sollen, müsste sich dies direkt aus dem Gesetz ergeben. Genau an einer solchen Regelung fehle es aber im ThürDSG-E.
5. Verbesserungsbedürftig war für den TLfDI auch die für ihn in **§ 8 Abs. 3 Satz 2 ThürDSG-E** geregelte Unterstützungspflicht gegenüber einer betroffenen Person, die beim TLfDI eine Beschwerde über eine Verarbeitung aus dem Zuständigkeitsbereich einer anderen Datenschutzaufsichtsbehörde der Europäischen Union eingereicht hat. Da dem TLfDI nicht klar war, in welcher Art und Weise er im Rahmen des Anwendungsbereichs der DS-GVO hier eine weitere Unterstützungshandlung – außer der Weiterleitung an die zuständige Behörde – leisten sollte, empfahl er dem TMIK, diese Regelung lediglich auf die Fälle der JI-Richtlinie zu beschränken.
6. Gegenüber dem TMIK sprach der TLfDI sich des Weiteren dafür aus, das bisher in § 11 Abs. 2 ThürDSG geregelte Benachteiligungs- und Maßregelungsverbot der öffentlichen Stellen gegenüber einem Beschwerdeführer in **§ 8 ThürDSG-E** zu übernehmen.
7. Zu **§ 9 ThürDSG-E**, der den Rechtsschutz gegen Anordnungen des TLfDI oder bei dessen Untätigkeit regelt, empfahl der TLfDI, explizit auf die Eröffnung des Verwaltungsrechtsweges hin-

zuweisen. Bislang erfolgte in dieser Regelung nur der Hinweis, dass der Rechtsweg eröffnet sei.

8. Zu der Neuregelung des **§ 11 ThürDSG-E**, der den TLfDI als Aufsichtsbehörde gegenüber nicht-öffentlichen Stellen bestimmt, empfahl der TLfDI, den Wortlaut des § 40 Abs. 1 BDSG auch in § 11 Abs. 1 ThürDSG-E zu verwenden.
9. Als äußerst misslich kritisierte es der TLfDI, dass das TMIK die Chance einer sachgerechten Regelung des Datenschutzes im Beschäftigungskontext nicht mit der Neuregelung in **§ 27 ThürDSG-E** genutzt hat. Wenigstens eine Regelung, die bestimmt, wann unter welchen Voraussetzungen die Einwilligung eines Beschäftigten als DS-GVO-konform anzusehen sei, hätte das TMIK in § 27 ThürDSG-E aufnehmen können.
10. Ebenfalls bemängelte der TLfDI, dass die Regelung zur Videoüberwachung in **§ 30 ThürDSG-E** keinen Bezug zu § 6 Abs. 2 DS-GVO herstelle und auch sonst systematisch wenig geglückt sei. Daher empfahl der TLfDI, sich beim Aufbau der Norm an dem bisherigen § 6b Bundesdatenschutzgesetz zu orientieren.

Das TMIK legte daraufhin im September 2017 einen zweiten Referentenentwurf für ein ThürDSAnpUG vor. Dabei stellte der TLfDI fest, dass in den oben genannten Punkten 1, 3, 4, 5, 9 und 10 keine befriedigende Berücksichtigung seiner Stellungnahme erfolgt ist.
Der TLfDI bleibt dran!

Auch das ThürDSG ist bis zum 25. Mai 2018 für die DS-GVO „fit“ zu machen. Dabei wird es insbesondere darauf ankommen, die Regelungen so einfach und verständlich wie möglich zu formulieren und wesentliche Bereiche des Datenschutzes, wie zum Beispiel des Beschäftigtendatenschutzes oder der Videoüberwachung, noch möglichst datenschutzfreundlich auszugestalten. Fehlende Regelungen, die die Landesregierung hier noch nicht im Sinne des TLfDI in den Gesetzentwurf aufgenommen hat, können die Fraktionen des Thüringer Landtags im parlamentarischen Gesetzgebungsverfahren dann noch ergänzen. Der TLfDI bleibt am Ball.



internet – © Julien Eichinger / Fotolia.com

4. Neue Medien – Rundfunk – Telekommunikation

4.1 Heiße Debatte um den Entwurf einer EU-e-Privacy-Verordnung

Am 25. November 2009 beschlossen das Europäische Parlament und der Rat der Europäischen Union mit der Richtlinie 2009/136/EG unter anderem Änderungen über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation. Diese e-Privacy-Richtlinie, auch unter „Cookie-Richtlinie“ bekannt, regelt im Wesentlichen in Artikel 5 Absatz 3 die Verwendung von Cookies.
Die zusätzliche Richtlinie war damals ein Ergebnis der Überprüfung der Richtlinie 2002/58/EG („e-Datenschutz-Richtlinie“).

Entsprechend dem Erwägungsgrund 173 i. V. m. Artikel 95 der neuen Datenschutz-Grundverordnung (DS-GVO) sollte die Richtlinie 2002/58/EG nochmal einer Überprüfung unterzogen werden, sobald die DS-GVO angenommen wurde, um insbesondere die Kohärenz mit der DS-GVO zu gewährleisten.

Seit dem 10. Januar 2017 liegt nun ein Entwurf einer e-Privacy-Verordnung der Europäischen Kommission vor. Der Begründung zum Entwurf kann man entnehmen, dass seit der letzten Überprüfung der e-Datenschutz-Richtlinie im Jahr 2009 sich wichtige technische und wirtschaftliche Entwicklungen auf dem Markt vollzogen haben. So heißt es: „Anstatt herkömmliche Kommunikationsdienste zu nutzen, verlassen sich Verbraucher und Unternehmen zunehmend auf neue Internetdienste, die eine interpersonelle Kommunikation ermöglichen, z. B. VoIP-Telefonie, Sofortnachrichtenübermittlung (Instant-Messaging) und webgestützte E-Mail-Dienste. Solche Over-the-Top-Kommunikationsdienste („OTT-Dienste“) werden aber im Allgemeinen vom gegenwärtigen Rechtsrahmen der Union für die elektronische Kommunikation, einschließlich der e-Datenschutz-Richtlinie, nicht erfasst. Folglich hat die Richtlinie mit der technischen Entwicklung nicht Schritt gehalten, was zu einem mangelnden Schutz der über solche neuen Dienste abgewickelten Kommunikation führt.“

Weiterhin liefert der Entwurf der Verordnung die Begründung gleich mit, warum es nun eine Verordnung und keine Richtlinie werden soll: „Die Kommission legt einen Vorschlag für eine Verordnung vor, um die Kohärenz mit der Datenschutz-Grundverordnung (DS-GVO) sowie Rechtssicherheit gleichermaßen für Nutzer und Unternehmen dadurch zu gewährleisten, dass eine unterschiedliche Auslegung in den Mitgliedstaaten vermieden wird. Eine Verordnung kann in der gesamten Union ein gleiches Schutzniveau für die Nutzer und niedrige Einhaltungskosten für grenzüberschreitend tätige Unternehmen sicherstellen.“

Geplant ist, dass die Verordnung zum gleichen Zeitpunkt wie die DS-GVO wirksam wird, also zum 25. Mai 2018. Ob der Termin gehalten werden kann, hängt stark davon ab, wie die einzelnen Gremien und betroffenen Wirtschaftsunternehmen Einfluss auf den Entwurf nehmen werden, denn die neuen Regelungen z. B. für das Online- und Direktmarketing haben beträchtliches Diskussionspotenzial. Man erinnere sich daran, wie lange es gedauert hat, bis die DS-GVO verabschiedet wurde.

Auch die Artikel-29-Gruppe der EU-Datenschutzbeauftragten veröffentlichte ihre Kritikpunkte zum Entwurf der EU-Kommission. So dürften beispielsweise Analysen von Metadaten und Inhaltsdaten nur erfolgen, wenn alle Endnutzer ausdrücklich eingewilligt haben. Auch sieht die Artikel-29-Gruppe die allgemeinen Browsereinstellungen als Grundlage einer Einwilligung für Cookies als unzureichend an, da dies nicht der Informationspflicht gemäß Artikel 7 DS-GVO entspricht. Bezüglich des Trackings äußerte die Artikel-29-Gruppe z. B. Änderungswünsche dahingehend, dass Angebote von Websites oder Diensten nur erlaubt seien, wenn diese den Zugang auch ohne Tracking ermöglichen. Zudem ist sie der Meinung, dass bei WiFi- und Bluetooth-Tracking eine Information darüber nicht ausreiche, da die DS-GVO i. d. R. eine Einwilligung verlange.
Man wird abwarten müssen, welche Entwicklung der Entwurf der Verordnung noch nehmen wird.

Entsprechend Erwägungsgrund 173 i. V. m. Artikel 95 der Datenschutz-Grundverordnung sollte, sobald die DS-GVO angenommen wurde, die Richtlinie 2002/58/EG einer Überprüfung unterzogen werden, um insbesondere die Kohärenz mit der DS-GVO zu gewährleisten. Geplant ist, dass die EU-e-Privacy-Verordnung zum gleichen Zeitpunkt wie die DS-GVO wirksam wird, also zum 25. Mai 2018. Wird der Termin nicht gehalten, gelten für die Übergangszeit die DS-GVO und die e-Privacy-Richtlinie 2002/58/EG in Verbindung mit der jeweiligen nationalen Umsetzung.

4.2 Google-Analytics

Im 9. Tätigkeitsbericht (TB) des Thüringer Landesbeauftragten für den Datenschutz wurde auf die Möglichkeit des datenschutzgerechten Einsatzes von Google Analytics hingewiesen. So wurde berichtet, dass die Voraussetzung hierfür die Löschung des letzten Oktetts der IP-Adresse und ein Widerspruch gegen die Erfassung von Nutzungsdaten mittels eines von Google bereitgestellten Deaktivierungs-Add-On durch den Nutzer notwendig ist. Neben diesen umzusetzenden Parametern muss der Webseitenbetreiber, um einen datenschutzgerechten Betrieb von Google Analytics zu ermöglichen, zudem schriftlich einen Vertrag zur Auftragsdatenverarbeitung mit Google Inc. abschließen. Ein Muster dieses Vertrages wird von der Google Inc. selbst auf deren Webseite bereitgestellt (siehe 9. TB, Pkt. 4.1).

Aufgrund der Tatsache, dass das Safe Harbor-Abkommen vom Europäischen Gerichtshof am 6. Oktober 2015 für ungültig erklärt wurde, prüfte der Hamburgische Beauftragte für den Datenschutz und Informationsfreiheit (HmbBfDI) als zuständige Aufsichtsbehörde erneut den Mustervertrag. Nach Aussagen des HmbBfDI hat die Google Inc. die Zertifizierung nach dem aktuellen EU-US-Privacy Shield durchgeführt und somit die rechtlichen Voraussetzungen auch für die Erbringung des Dienstes Google Analytics im Wege der Auftragsdatenverarbeitung geschaffen.

Hinweise zum aktuellen Mustervertrag zur Auftragsdatenverarbeitung sowie aktuelle Hinweise zum datenschutzgerechten Einsatz von Google-Analytics finden Sie auf der Website: https://www.datenschutz-hamburg.de/uploads/media/GoogleAnalytics_Hinweise_fuer_Webseitenbetreiber_in_Hamburg_2017.pdf



Der Einsatz von Google-Analytics ist aus datenschutzrechtlicher Sicht nur unter bestimmten Voraussetzungen erlaubt. Hinweise hierzu finden Sie auf der Webseite der zuständigen Aufsichtsbehörde.

4.3 Pflichten sozialer Netzwerke

Die Datenschutzbeauftragten des Bundes und der Länder beschäftigten sich schon recht früh mit der datenschutzrechtlichen Thematik von sozialen Netzwerken. Durch Facebook aber mit seinen mächtigen Funktionen, die so viel Daten wie möglich sammeln, um dem Nutzer ein „optimales“ Angebot bereitstellen zu können, wurde eine neue Qualität von sozialen Netzwerken geschaffen. Mit der Idee der „optimalen Kundenbetreuung“ ging zwangsweise die Notwendigkeit einer umfassenden Profilbildung der Nutzer einher. Nach dem Motto: Je mehr ich von einem Nutzer weiß, umso besser kann ich durch Algorithmen geschäftsmäßig die Bedürfnisse der Wirtschaft mit dem Kunden verbinden, auch die eigenen.

So stellte im September 2011 die 82. Konferenz der Datenschutzbeauftragten des Bundes und der Länder u. A. klar, dass sich Anbieter solcher Plattformen, die auf den europäischen Markt zielen, auch dann an europäische Datenschutzstandards halten müssen, wenn sie

ihren Sitz außerhalb Europas haben (siehe https://www.tlfdi.de/mam/tlfdi/datenschutz/entschliessungen/80/82_nutzerdaten.pdf).

In den meisten sozialen Netzwerken werden auch Funktionen angeboten, die es ermöglichen, mit anderen Leuten zu diskutieren, Beiträge, Fotos und Videos zu teilen. Somit können Anbieter sozialer Netzwerke durch deren Inhalte und Kommunikationspartner den Nutzer anhand seiner hinterlassenen Daten noch genauer analysieren. Diese Kommunikationsmöglichkeiten haben aber in den letzten Jahren eine besondere Dynamik erlangt. Neben Cybermobbing und anderen strafbaren Inhalten ist zunehmend eine Verbreitung von Hasskriminalität in den sozialen Netzwerken zu verzeichnen. Facebook z. B. verkündete im Mai 2017, dass nun tausende Mitarbeiter eingestellt würden, um dem entgegenzuwirken. Doch wie will man die Millionen Beiträge täglich überprüfen? Was ist zudem strafbar und was ist Kunst oder Meinungsfreiheit? Fast denkt man hier an Goethes Zauberlehrling und die Geister, die man selber rief.

In Deutschland gilt nun seit dem 1. Oktober 2017 das Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Bundesgesetzblatt Nr. 61 vom 7. September 2017).

Durch dieses Netzwerkdurchsetzungsgesetz (NetzDG) sollen die Hasskriminalität und andere strafbare Inhalte in sozialen Netzwerken minimiert werden. So sind Anbieter sozialer Netzwerke nun verpflichtet, bei einem offensichtlich rechtswidrigen Inhalt innerhalb von 24 Stunden nach Eingang der Beschwerde diesen zu entfernen oder den Zugang zu ihm zu sperren. Dies gilt nicht, wenn der Anbieter mit der zuständigen Strafverfolgungsbehörde einen längeren Zeitraum für die Löschung oder Sperrung des offensichtlich rechtswidrigen Inhalts vereinbart hat.

Handelt es sich um einen rechtswidrigen Inhalt, dessen Offensichtlichkeit nicht gleich erkennbar ist, muss der Anbieter trotzdem in der Regel innerhalb von sieben Tagen die Löschung oder Sperrung durchführen. Diese Zeit verlängert sich, falls der Anbieter zwecks Entscheidungsfindung über die Rechtswidrigkeit des Inhalts z. B. dem Nutzer vor der Entscheidung Gelegenheit zur Stellungnahme zu der Beschwerde gibt.

Falls es zu einer Löschung kommt, hat der Anbieter des sozialen Netzwerks den Inhalt für die Dauer von zehn Wochen zu speichern. Weiterhin sind der Beschwerdeführer und der Nutzer über jede Entscheidung unverzüglich zu informieren und die Entscheidung ist zu begründen.
Kritiker sehen hier eine Lücke, da nur eine Informationspflicht vorliegt. Ein Widerspruchsrecht für die Nutzer gibt es nicht.
Hat der Anbieter vom sozialen Netzwerk diesbezüglich mehr als 100 Beschwerden im Kalenderjahr, so ist er berichtspflichtig. Der deutschsprachige Bericht ist auf seiner Homepage und im Bundesanzeiger entsprechend dem NetzDG zu veröffentlichen.
Im Übrigen gelten die Regelungen zu den Beschwerden und zur Berichtspflicht nicht für Anbieter sozialer Netzwerke, wenn das soziale Netzwerk im Inland weniger als zwei Millionen registrierte Nutzer hat.

Anbieter sozialer Netzwerke, die auf den europäischen Markt zielen, müssen sich auch dann an europäische Datenschutzstandards halten, wenn sie ihren Sitz außerhalb Europas haben. Zudem gilt es ab dem 1. Oktober 2017, das Netzwerkdurchsetzungsgesetz (NetzDG) zu beachten.

4.4 Datenweitergabe aus dem Melderegister

Im Berichtszeitraum wandte sich ein Beschwerdeführer mit melderechtlichen Fragen an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI).
Er widersprach in seinem Schreiben an den TLfDI der Weitergabe seiner Daten aus dem Melderegister „an irgendwen“, insbesondere aber an den Beitragsservice der ARD und ZDF. Durch die – seiner Meinung nach – Möglichkeiten einer vollständigen Datenerfassung einschließlich Datenverknüpfung sah er sein allgemeines Persönlichkeitsrecht des Art. 2 Abs. 1 Grundgesetz (GG) in Verbindung mit Art. 1 Abs. 1 GG verletzt. Seiner Meinung nach würde aufgrund dieser Datenweitergabe sein Recht auf informationelle Selbstbestimmung eingeschränkt, da es nicht möglich sei, über die Weitergabe und Verwendung der Daten selbst zu bestimmen.
Der TLfDI hat den Beschwerdeführer über Folgendes informiert:
Dem TLfDI obliegt auch die Kontrolle der Thüringer Meldebehörden nach § 37 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG).

Diese dürfen nur innerhalb des gesetzlich vorgegebenen Rahmens die personenbezogenen Daten der Betroffenen verarbeiten und nutzen.
Die betroffene Person hat allerdings das Recht, dieser Übermittlung der Daten nach § 50 Abs. 1 bis 3 Bundesmeldegesetz (BMG) (s. o.: Auskunft an Parteien, Mandatsträger, Presse, Rundfunk, Adressbuchverlage) gemäß § 50 Abs. 5 BMG zu widersprechen. Der TLfDI hat auf seiner Internetseite ein entsprechendes Formblatt „Widerspruch gegen Datenübermittlung aus Melderegister“ (https://www.tlfdi.de/imperia/md/content/datenschutz/themen/mustervordrucke/anlage_widerspruch_gegen_datenuebermittlung.pdf) zur Verfügung gestellt.
Darüber hinaus gibt es eine Vielzahl von Datenübermittlungen (z. B. Datenübermittlungen an andere öffentliche Stellen gemäß § 34 BMG), denen der Betroffene nicht widersprechen kann.
Auch soweit der betroffene Bürger Kritik an dem Verfahren übte, dass der Beitragsservice ARD und ZDF zwecks Beitragserhebung die Daten der Meldeämter verarbeiten darf, muss der TLfDI auf den Beschluss des Oberverwaltungsgerichts Lüneburg verweisen (Az. 4 ME 204/13). Darin haben die Richter festgestellt, dass der durch den Beitragsservice vorgenommene Abgleich der Melderegisterdaten mit dem beim Beitragsservice vorhandenen Datenbestand auf Grundlage des Rundfunkbeitragsstaatsvertrags erforderlich ist und damit keinen Verstoß gegen das Grundrecht auf informationelle Selbstbestimmung darstellt. Ein Widerspruch gegen diesen Datenabgleich mit dem Beitragsservice (wegen Rundfunk- und Fernsehgebühren) ist in Folge nicht erfolgversprechend.
Der Beschwerdeführer schien mit den Ausführungen des TLfDI zufriedengestellt zu sein, jedenfalls hat er sich nicht erneut an den TLfDI gewandt.

Es ist nicht möglich, jeder Datenübermittlung zu widersprechen. Dies gilt insbesondere für den Abgleich der Melderegisterdaten mit dem beim Beitragsservice vorhandenen Datenbestand zwecks Erhebung von Rundfunkbeiträgen. Die im Bundesmeldegesetz eingeräumten Widerspruchsmöglichkeiten (§ 50 Abs. 5 BMG) sollte man

im Interesse des informationellen Selbstbestimmungsrechtes aber nutzen.

4.5 Die DS-GVO hat auch Auswirkungen auf den Mitteldeutschen Rundfunk (MDR)

Wenn am 25. Mai 2018 die Datenschutz-Grundverordnung (DS-GVO) zur Anwendung kommen wird, hat dies auch Auswirkungen auf die öffentlich-rechtlichen Rundfunkanstalten in Deutschland und damit auch für den Mitteldeutschen Rundfunk. Artikel 85 DS-GVO regelt dazu unter anderem Folgendes:
„Artikel 85 Verarbeitung und Freiheit der Meinungsäußerung und Informationsfreiheit
(1) Die Mitgliedstaaten bringen durch Rechtsvorschriften das Recht auf den Schutz personenbezogener Daten gemäß dieser Verordnung mit dem Recht auf freie Meinungsäußerung und Informationsfreiheit, einschließlich der Verarbeitung zu journalistischen Zwecken und zu wissenschaftlichen, künstlerischen oder literarischen Zwecken, in Einklang.“
Ferner führt Art. 85 Abs. 2 DS-GVO explizit auf, zu welchen Kapiteln der DS-GVO die Mitgliedstaaten Ausnahmen oder Abweichungen für eine Verarbeitung zu journalistischen Zwecken vorsehen können, wenn dies erforderlich ist, um das Recht auf Schutz personenbezogener Daten mit der Freiheit der Meinungsäußerung und der Informationsfreiheit in Einklang zu bringen.
Diesem Auftrag ist die Thüringer Landesregierung nachgekommen: In ihrem Referentenentwurf für ein neues – der DS-GVO angepasstes – Thüringer Datenschutzgesetz regelt sie in einem neuen § 31 ThürDSG-E, welche Artikel der DS-GVO auf eine öffentlich-rechtliche Rundfunkanstalt des Landes Anwendung finden sollen, und welche Artikel der DS-GVO davon ausgenommen sind, weil eine Datenverarbeitung oder -nutzung ausschließlich zu eigenen journalistisch-redaktionellen Zwecken erfolgt.
Ferner regelt § 32 Abs. 1 ThürDSG-E die Bestellung eines Beauftragten für den Datenschutz im Rundfunk. Diese Norm hat folgenden Wortlaut:
„(1) Der Intendant der Rundfunkanstalt beruft mit Zustimmung des Verwaltungsrates einen Beauftragten für den Datenschutz im Rundfunk für die Dauer von sechs Jahren, einmalige Wiederbestellung ist zulässig. Der Beauftragte für den Datenschutz im Rundfunk tritt für

die jeweilige Rundfunkanstalt an Stelle des Thüringer Landesbeauftragten für den Datenschutz als zuständige Aufsichtsbehörde.“
Gem. dem Wortlaut des § 32 Abs. 1 ThürDSG-E („Der Intendant…“) kann sich die hieraus ergebende Verpflichtung nicht auf das MDR-Landesfunkhaus Thüringen beziehen. Denn zum einen hat das Landesfunkhaus Thüringen des MDR keinen Intendanten und zum anderen verfügt es auch über keinen eigenständigen Verwaltungsrat. Somit ist der Beauftragte für den Datenschutz beim MDR an dessen Hauptsitz in Leipzig zu bestellen.
Eine andere Frage, die den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit beschäftigte, war, wer für die datenschutzrechtliche Kontrolle des MDR zuständig ist. Dazu regelt § 14 Abs. 3 des Entwurfs für ein Sächsisches Datenschutzdurchführungsgesetz (SächsDSDG) Folgendes:
„(3) Sofern die Verarbeitung der personenbezogenen Daten zu journalistischen Zwecken erfolgt, bleiben die Vorschriften zu dem Beauftragten für den Datenschutz im Staatsvertrag über den Mitteldeutschen Rundfunk vom 30. Mai 1991 (SächsGVBl. S. 169), in der jeweils geltenden Fassung, unberührt. Im Übrigen ist der Sächsische Datenschutzbeauftrage Aufsichtsbehörde.“
In der Begründung des Gesetzentwurfs zu § 14 Abs. 3 SächsDSDG heißt es dazu:
„Die Regelung stellt klar, dass der Mitteldeutsche Rundfunk im Rahmen der Bereichsausnahme für journalistische Tätigkeit wie bisher vom staatlichen Aufsichtsregime ausgenommen wird. Die Datenschutz-Grundverordnung enthält in Artikel 85 Absatz 2 eine entsprechende Öffnungsklausel. ***Der Begriff des Journalismus ist in diesem Zusammenhang weit auszulegen. Nicht unter den Begriff fallen der Einzug von Rundfunkbeiträgen und die damit verbundene Datenverarbeitung. Diese unterfällt daher der Aufsicht des Sächsischen Datenschutzbeauftragten“***
Daraus ergibt sich eindeutig, dass künftig der Sächsische Datenschutzbeauftragte zuständig sein wird, wenn sich für den Bürger datenschutzrechtliche Beschwerden im Zusammenhang mit dem Einzug von Rundfunkbeiträgen ergeben sollten. Damit wäre dann der Sächsische Datenschutzbeauftragte für alle datenschutzrechtlichen Anfragen aus dem Sendegebiet des MDR, die den Einzug von Rundfunkbeiträgen tangieren, zuständig.

Die öffentlich-rechtlichen Rundfunkanstalten, zu denen auch der MDR gehört, werden auch zukünftig von der Kontrolle durch die Landesdatenschutzbeauftragten „verschont“ werden, soweit sie ihre journalistische Tätigkeit ausüben. Bei nicht journalistischen Angelegenheiten, worunter insbesondere der Einzug von Rundfunkbeiträgen fällt, soll nach § 14 Abs. 3 SächsDSDG-E der Sächsische Datenschutzbeauftragte als Kontrollbehörde für den MDR zuständig sein. Der Gesetzentwurf muss noch vom Sächsischen Landtag beschlossen werden.

4.6 Wenn Kühlschränke eiskalt angreifen

Das ist keine Utopie mehr. Im Herbst 2016 mussten in den USA viele rund zwei Stunden ohne Musik von Spotify und Soundcloud, ohne Twitter, ohne Netflix und ohne ein Dutzend anderer beliebter Onlinedienste auskommen.
Was war geschehen?
Zunehmend halten Haushaltsgeräte im privaten Bereich Einzug, die internetfähig sind. Sie haben neben einer IP-Adresse eine Software, die nicht vom Kunden überschaubar bzw. kontrollierbar ist. Dies betrifft z. B. Kühlschränke, Thermostate, Videogeräte, hausinterne Web-Cams usw.
Oft werden diese Geräte zudem mit Standard-Administrations-Passwörtern ausgeliefert, deren Änderung für den Normal-Verbraucher schon eine Hürde darstellt.
Hacker haben dies bereits erkannt, schalten sich auf solche Geräte auf, programmieren sie so, dass diese zu einem bestimmten Zeitpunkt zeitgleich einen Angriff ausüben. Also zur gleichen Zeit festgelegte Ziel-Server mit Anfragen zuschütten, sodass die Server dann überlastet sind. Im Fachbereich spricht man von einem Botnetz, welches solche Angriffe ausführt.
Nun mag man denken, so etwas wird nicht in Deutschland geschehen. Im November 2016 wurde aber eine größere Anzahl von Routern der Telekom, die unzählige Haushalte vor Angriffen schützen sollten, selbst Opfer eines Hackerangriffes. Nach Angaben des Bundesamtes der Sicherheit in der Informationstechnik (BSI) waren dabei über 900.000 Kundenanschlüsse betroffen. Nach Angaben der Telekom handelte es sich dabei um Telekom-Router von Drittanbietern. Ziel des Angriffs war die Installation einer Schadsoftware auf diese Router, damit diese dann als Teil eines sogenannten Botnetzes

fungierten, also als fernsteuerbare Infrastruktur für weitere Angriffe zur Verfügung stehen. Nach Angaben der Telekom war die Installation der Schadsoftware bei denen, die die Telekom betrieb, nicht erfolgreich. Bei dem Versuch, diese Schadsoftware zu installieren, stürzten diese aber ab. So war für viele Kunden kein Internet und keine IP-Telefonie möglich. Der Angriff auf die Drittanbieter-Router diente der Konstruktion eines Botnetzes zum gleichzeitigen Angriff auf externe Server.

Was ist aber, wenn zukünftige Angriffe nicht nur externen Servern gelten, sondern internetfähige Geräte im Haushalt das Ziel solcher Angriffe sind? Also Router gekapert werden, um Geräte innerhalb des Hauses zu manipulieren, auch um diese für Großangriffe fit zu machen?

Was passiert eigentlich zukünftig, wenn auch hier Hacker Kühlschränke eiskalt manipulieren? Welche Folgen ergeben sich zukünftig für den Bürger daraus? Wird dann der komplette digitalisierte Haushalt von staatlicher Seite abgeschaltet, sämtliche Geräte im Haushalt, einschließlich PC und Smartphone, überprüft? Gibt es dann noch Fernsehen und Strom, da auch diese Geräte mittlerweile vernetzt sind? Welche Rechte und Pflichten wird zukünftig der Bürger in der digitalen Gesellschaft haben?

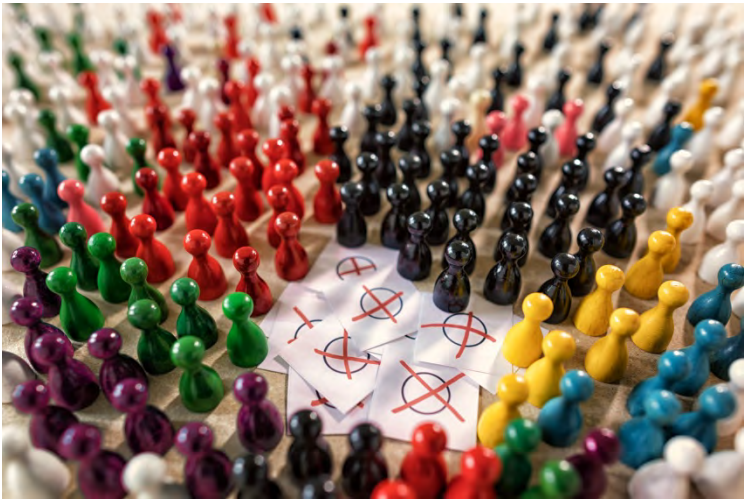
Wenn große Unternehmen sich schon nicht vor Hackerangriffen schützen können, ist es nur eine Frage der Zeit, wann auch in Deutschland beispielsweise Kühlschränke eiskalt angreifen.

Der Einzug in die digitale Gesellschaft kommt und ist auch richtig, nur bedarf es auch einer digitalen und dementsprechenden technischen und rechtlichen Sicherheit für die Bürger, die von den jeweiligen Herstellern solcher Geräte zukünftig sichergestellt werden muss. Die Hersteller von internetfähigen Geräten und auch der Rechtsstaat müssen sich langfristig der Verantwortung bewusst werden, dass die Einführung der digitalen Gesellschaft nicht auf Kosten der Bürger und ihrer Grundrechte gehen darf.

Der TLfDI stellt hierfür seine Erfahrungen und Kenntnisse gern bereit.

Hersteller von internetfähigen Geräten müssen für ihr Produkt haftbar gemacht werden. Geräte sind zudem so zu gestalten, dass neben eindeutigen und verständlichen Hinweisen der Hersteller für Käufer beispielsweise schon beim Erwerb eines solchen Gerätes mit einfa-

chen Mitteln das jeweilige Standard-Passwort vom Eigentümer geändert werden kann.



People going tot he polls - © Ingo Bartussek

5. Landtag

5.1 Erhebung der Personalausweisnummer von Besuchern des Thüringer Landtages zum Zwecke der Einlasskontrolle

Dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) wurde bekannt, dass im Rahmen der Einlasskontrolle der Besucher des Thüringer Landtages diverse personenbezogene Daten, darunter auch die Personalausweisnummer, erhoben und gespeichert werden.
Es wurde u. a. die Frage an den TLfDI herangetragen, inwiefern diese Praxis derer der anderen Landtage der Bundesländer bzw. des Bundestags entspricht und inwiefern die Erhebung und Speicherung insbesondere der Personalausweisnummer datenschutzrechtlich gerechtfertigt ist.
Zunächst war allerdings vom TLfDI zu prüfen, ob überhaupt die Zuständigkeit des TLfDI zu bejahen ist. Nach § 2 Abs. 5 Thüringer Datenschutzgesetz (ThürDSG) gilt das Thüringer Datenschutzgesetz für den Landtag nur, wenn es sich um Verwaltungsangelegenheiten des Landtages handelt. Nach § 2 Abs. 5 Nr. 3 ThürDSG gilt dies insbesondere für die Ausübung des Hausrechts. Einlasskontrollen

dienen der Aufrechterhaltung des Hausrechts, womit die Zuständigkeit des TLfDI zu bejahen war.
Es wurde daraufhin eine Anfrage des TLfDI an die Landesdatenschutzbeauftragten aller Bundesländer sowie den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit mit der Fragestellung gestellt, inwiefern dort im Rahmen der Einlasskontrolle die Personalausweisnummern der Besucher registriert werden.
Es erfolgten zwischenzeitlich Rückmeldungen aus einem Großteil der angefragten Bundesländer. Es war festzustellen, dass ca. die Hälfte der rückmeldenden Datenschutzbehörden einen vergleichbaren zugrunde liegenden Sachverhalt noch nicht geprüft hatte. Die andere Hälfte teilte mit, dass in ihrem Bundesland auf eine Erhebung der Seriennummer des Personalausweises verzichtet werde.
Grundsätzlich besteht für öffentliche Stellen die Möglichkeit, unter Beachtung der rechtlichen Vorgaben, auf Grundlage des Personalausweisgesetzes auch die Personalausweisnummer zu erheben und zu verwenden. Es stellt sich jedoch im Hinblick auf die verfassungsmäßig geforderte Verhältnismäßigkeit staatlicher Eingriffe in die Grundrechtsposition des Einzelnen die Frage, inwiefern die Erhebung und Speicherung der Personalausweisnummer bei Besuchern des Landtags im Einzelfall als erforderlich zu begründen ist.
Welchen Zweck der Thüringer Landtag gerade mit der Erhebung und Verwendung der Personalausweisnummer verfolgt, ist dem TLfDI noch nicht bekannt. Daher kann der TLfDI mangels umfassender Kenntnis des zugrundeliegenden Sachverhalts noch keine abschließende Beurteilung vornehmen.

Der TLfDI wird den Sachverhalt allumfassend prüfen und nach Klärung der noch offenen Fragestellungen eine abschließende Bewertung vornehmen. Zum Ergebnis wird berichtet.

5.2 Auskunftsverpflichtung des Landesamtes für Statistik?

Im Berichtszeitraum wandte sich ein Beschwerdeführer mit der Bitte um Unterstützung und datenschutzrechtliche Prüfung an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Er hatte beim Thüringer Landesamt für Statistik (TLS) um Mitteilung zu Daten ersucht, die nach § 6 Gesetz über die Statistiken der öffentlichen Finanzen und des Personals im öffentlichen Dienst (Finanz- und Personalstatistikgesetz – FPStaG) zum

30. Juni eines jeden Jahres durch die Behörden gemeldet werden müssen.
Auf dieses Verlangen habe das TLS dem Beschwerdeführer aber nicht in Gänze Auskunft erteilt. Das TLS habe mitgeteilt, dass die dargelegten und sehr detaillierten Anfragen nicht beantwortet werden könnten, da die gewünschten Daten entweder dem Landesamt im Rahmen der Personalstandstatistik nicht zur Verfügung stünden bzw. aus Gründen der statistischen Geheimhaltung nicht veröffentlicht werden dürften, da es sich um Einzelangaben handele.
Nach datenschutzrechtlicher Prüfung hat der TLfDI den Beschwerdeführer über Folgendes informiert:
Der TLfDI kontrolliert bei allen öffentlichen Stellen die Einhaltung der Bestimmungen des Thüringer Datenschutzgesetzes (ThürDSG) und anderer Rechtsvorschriften über den Datenschutz. Zweck des ThürDSG ist es dabei, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten durch öffentliche Stellen in seinem Persönlichkeitsrecht beeinträchtigt wird (§ 1 Abs. 1 ThürDSG). Die Daten verarbeitende Stelle hat dem Betroffenen gemäß § 13 Abs. 1 ThürDSG auf Antrag ohne unzumutbare Verzögerung Auskunft zu erteilen über die zu seiner Person verarbeiteten Daten, den Zweck und die Rechtsgrundlage der Verarbeitung sowie die Herkunft der Daten und deren Empfänger oder die Kategorien der Empfänger, soweit diese Angaben gespeichert sind.
Vorliegend handelte es sich aber nicht um personenbezogene Daten des die Auskunft begehrenden Beschwerdeführers. Zudem war auch kein Betroffenenstatus im Sinne des § 13 Abs. 1 ThürDSG erkennbar.
Die Prüfung eines möglichen Auskunftsanspruchs gemäß Thüringer Informationsfreiheitsgesetz (ThürIFG) erzielte folgendes Ergebnis:
Nach § 4 Abs. 1 (ThürIFG) hat jeder nach Maßgabe dieses Gesetzes Anspruch auf Zugang zu amtlichen Informationen, die bei den in § 2 Abs. 1 und 2 ThürIFG genannten Stellen vorhanden sind. Vorliegend müsste es sich aber um amtliche Informationen im Sinne des ThürIFG handeln. Maßgebend für die Feststellung der Amtlichkeit einer Information ist allein ihre Zweckbindung. Amtlichen Zwecken dient eine Aufzeichnung, wenn sie die Behörde betrifft oder in Erfüllung einer amtlichen Tätigkeit angefallen ist oder in anderer Weise im Zusammenhang mit der amtlichen Tätigkeit steht (Schoch, IFG Kommentar, § 2 Rn. 35). Nach Auffassung des TLfDI handelte es sich vorliegend bei den erbetenen Informationen um amtliche Infor-

mationen, da die Erhebung und Verarbeitung dieser Daten im Zusammenhang mit der amtlichen Tätigkeit des TLS steht.
Um Informationen erhalten zu können, ist ein Antrag (des Informationsbegehrenden) auf Informationszugang an das TLS nötig. Der Antrag kann sowohl schriftlich als auch mündlich, zur Niederschrift oder elektronisch gestellt werden. Grundsätzlich bedarf der Antrag auf Informationszugang keiner Begründung. Betrifft der Antrag jedoch – wie vorliegend – Daten Dritter, muss er begründet werden und ggfs. ein rechtliches Interesse (sofern eine Abwägung nach § 9 Abs. 1 Nr. 5 ThürIFG vorgenommen werden muss) geltend gemacht werden. Das Thüringer Informationsfreiheitsgesetz (ThürIFG) sieht dabei zahlreiche Ausschlussgründe vor, bei deren Vorliegen ein Informationszugang verwehrt ist. Diese Ausschlussgründe sind in den §§ 7 bis 9 ThürIFG niedergelegt. Der Antrag ist abzulehnen, wenn beispielsweise bei vertraulich erhobenen oder übermittelten Informationen das Interesse des Dritten an einer vertraulichen Behandlung fortbesteht. Der Anspruch auf Informationszugang nach dem ThürIFG wird zudem nur zu den Informationen gewährt, die bei den in § 2 Abs. 1 und 2 ThürIFG genannten Stellen vorhanden sind. Im Gegensatz zu den meisten anderen gesetzlichen Auskunftsansprüchen, die das Vorhandensein der Informationen als Tatbestandsmerkmal des Informationsanspruches nennen, ist dies beim Informationsfreiheitsgesetz nicht der Fall. Demnach ist das Vorhandensein der Informationen eine denklogische Voraussetzung für den Informationsanspruch des IFG und ist daher als ungeschriebenes Tatbestandsmerkmal mitzulesen. Es gibt keine Anhaltspunkte im Gesetz dafür, dass der Gesetzgeber eine umfangreiche Beschaffungspflicht regeln wollte, die einen neuen zusätzlichen Arbeitsaufwand und auch ein neues Arbeitsfeld schaffen würde. Das IFG sieht eine solche generelle Verpflichtung nicht vor, und zwar auch dann nicht, wenn eine Information bei einer Stelle vorhanden sein müsste, es aber nicht so ist (Berger/Partsch/Roth/Scheel, IFG Kommentar, § 2 Rn. 24). D. h., sofern keine Informationen vorliegen sollten, ist die informationspflichtige Stelle grundsätzlich nicht zur Informationsbeschaffung verpflichtet.
Der TLfDI hat dem Beschwerdeführer abschließend mitgeteilt, dass aus datenschutzrechtlicher Sicht keine Auskunftspflicht des TLS hinsichtlich der begehrten Daten besteht, da es sich vorliegend nicht um personenbezogene Daten des Auskunftsbegehrenden handelt und auch kein Betroffenenstatus im Sinne des § 13 Abs. 1 ThürDSG

erkennbar ist. Eine Auskunftspflicht des TLS gegenüber Betroffenen bestünde lediglich hinsichtlich der zur eigenen Person beim TLS verarbeiteten Daten.
Ein Informationsanspruch nach dem ThürIFG könnte teilweise gegeben sein, nach entsprechendem Antrag und jedenfalls für die Informationen, die tatsächlich beim TLS vorhanden sind und die nach jeweiliger Abwägung gemäß § 9 ThürIFG herauszugeben wären.
Der TLfDI geht davon aus, dass der Beschwerdeführer mit den o. g. Informationen zufrieden war. Er hat sich jedenfalls nicht nochmals an den TLfDI gewandt.

Wer nicht Betroffener im Sinne des ThürDSG ist, kann auch keinen Auskunftsanspruch gemäß § 13 ThürDSG wirksam geltend machen. Ggf. öffnet das ThürIFG den Weg zu den gewünschten Informationen.

5.3 Freier W-LAN-Zugang im Thüringer Landtag doch nicht frei

Eine Landtagsfraktion wandte sich im Berichtszeitraum an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), da sie mit der Erhebung von personenbezogenen Daten im Zusammenhang mit der Nutzung des freien W-LAN-Netzes im Thüringer Landtag nicht einverstanden war.
Grundlage der Beschwerde ist die praktische Verfahrensweise, dass derjenige, der das Angebot des freien W-LAN im Thüringer Landtag nutzen möchte, zunächst im Rahmen der Unterzeichnung eines Formblattes mit zugrundeliegenden Nutzungsbedingungen diverse personenbezogene Daten hinterlegen muss, um ein Passwort und somit einen Zugang zum W-LAN-Netz zu erhalten.
Zu diesen personenbezogenen Daten gehörten neben dem Namen, Vornamen sowie der Adresse auch die Nummer des Personalausweises des Nutzers.
Grundsätzlich besteht für öffentliche Stellen die Möglichkeit, unter Beachtung der rechtlichen Vorgaben, auf Grundlage von §§ 14 und 20 Personalausweisgesetz auch die Personalausweisnummer zu erheben und zu verwenden. Es stellte sich jedoch im Hinblick auf die verfassungsmäßig geforderte Verhältnismäßigkeit staatlicher Eingriffe in die Grundrechtsposition des Einzelnen die Frage, inwiefern die Erhebung und Speicherung der Personalausweisnummer bei Inan-

spruchnahme der Nutzung des freien W-LAN im Einzelfall als erforderlich zu begründen ist.
Nach Auffassung des TLfDI ist eine Erhebung und Speicherung der Personalausweisnummer oder alternativ der Seriennummer des Passdokumentes im vorliegenden Fall als kritisch zu betrachten.
Insbesondere im Hinblick auf die Abschaffung der sogenannten Störerhaftung durch Änderung des Telemediengesetzes sind Diensteanbieter, in diesem Falle der Thüringer Landtag, nicht mehr verpflichtet, die über ihr Netzwerk übermittelten und gespeicherten Inhalte zu überwachen oder nach Umständen zu forschen, die auf rechtswidrige Tätigkeiten im Zusammenhang mit der Nutzung des W-LAN-Netzes hinweisen. Vor diesem Hintergrund stellt sich weiterhin die Frage für den TLfDI, inwiefern überhaupt eine Datenerhebung dahingehend beim Nutzer erfolgen muss bzw. sollte.

Auch wenn die Erhebung einer Personalausweisnummer gem. §§ 14 und 20 Personalausweisgesetz als zulässig angesehen werden könnte, stellt sich die Frage, ob diese Erhebung für einen W-LAN-Zugang als erforderlich anzusehen ist. Zum Ergebnis berichtet der TLfDI im nächsten Tätigkeitsbericht.

5.4 Zuständig oder nicht zuständig, das ist hier die Frage – Unterschriftenlisten auf dem Abgeordneten-Twitter-Account

Im Berichtszeitraum erreichten den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) mehrere Beschwerden, ob das Verhalten von Abgeordneten des Thüringer Landtags den datenschutzrechtlichen Vorgaben entsprach. Unter anderem erlangte der TLfDI Kenntnis davon, dass ein Landtagsabgeordneter Anfang 2017 auf seinem Twitter-Account, den er als Abgeordneter des Thüringer Landtags betrieb, Bilder von einer Unterschriftenliste gegen die in Thüringen geplante Kreisgebietsreform veröffentlicht hatte. Auf den veröffentlichten Bildern waren die personenbezogenen Daten von Personen, die sich auf der Unterschriftenliste bereits eingetragen hatten, klar erkennbar.
Zu der Frage, ob der TLfDI überhaupt rechtlich befugt ist, das Verhalten von Abgeordneten des Thüringer Landtages datenschutzrechtlich zu überprüfen, hatte der TLfDI in der Vergangenheit eine klare Position: § 2 Abs. 5 Satz 3 ThürDSG (im vorliegenden Entwurf für

ein neues Thüringer Datenschutzgesetz wird die Vorschrift inhaltsgleich in § 2 Abs. 7 übernommen) legt fest, dass für die Verarbeitung und Nutzung personenbezogener Daten bei der Wahrnehmung parlamentarischer Aufgaben durch den Landtag einschließlich der Fraktionen die Bestimmungen des ThürDSG unter der Berücksichtigung der verfassungsrechtlichen Stellung des Landtags entsprechende Anwendung finden. § 2 Abs. 5 Satz 4 ThürDSG führt ergänzend aus, dass der Ältestenrat des Thüringer Landtags die Einhaltung des Datenschutzes kontrolliert, soweit der Landtag in Wahrnehmung parlamentarischer Aufgaben personenbezogene Daten verarbeitet. Der Ältestenrat des Thüringer Landtages ist dabei mitnichten ein Gremium, in dem die ältesten oder erfahrensten Parlamentarier zusammenkommen. Der Ältestenrat besteht gem. § 10 Abs. 1 der Geschäftsordnung des Thüringer Landtags aus dem Präsidenten, den Vizepräsidenten und weiteren Abgeordneten der Fraktionen des Thüringer Landtags. Für den TLfDI ergab sich daher aus dem Zusammenspiel der beiden genannten Regelungen des ThürDSG, dass auch die Abgeordneten des Thüringer Landtags, soweit ihr Handeln im direkten Zusammenhang mit ihrer Tätigkeit als Parlamentarier des Thüringer Landtags steht, nicht der Kontrollbefugnis des TLfDI, sondern des Ältestenrats des Thüringer Landtags unterliegen. Diese Rechtsauffassung des TLfDI wird untermauert von der Kommentierung von Hanloser in: Wolf/Brink, Datenschutzrecht in Bund und Ländern, 1. Auflage 2013, § 2 BDSG, Rz. 50., der parlamentarische Gruppen und Abgeordnete als öffentliche-rechtlich organisierte Einrichtungen begreift, wenn sie im Rahmen ihrer Mandatsausübung mit personenbezogenen Daten umgehen.

Zu dieser Rechtsfrage teilte die Direktorin des Thüringer Landtags dem TLfDI im Herbst 2016 jedoch ihre überraschende Auffassung mit, die der Ansicht des TLfDI diametral entgegenstand: Der einzelne Abgeordnete sei grundsätzlich im Hinblick auf seine von Fremdbestimmung und öffentlich-rechtlicher Aufgabenbindung freie Mandatswahrnehmung ungeachtet des von ihm bekleideten besonderen öffentlichen Amtes als nicht-öffentliche Stelle nach § 2 Abs. 4 Satz 1 BDSG anzusehen. Zur Untermauerung ihrer Rechtsauffassung verwies die Direktorin des Thüringer Landtags auf die Literaturansicht von Dammann in: Simitis, BDSG, Kommentar, 8. Auflage, § 2, Rz. 29, der den einzelnen Abgeordneten als nicht-öffentliche Stelle im Sinne des BDSG einstuft. Als nicht-öffentliche Stellen sind allerdings Firmen und sonstige Stellen anzusehen, soweit es sich bei

ihnen nicht um öffentliche Stellen handelt. Seit dieser erstmals von der Landtagsverwaltung vertretenen Rechtsauffassung war der TLfDI bemüht, nunmehr eine **grundsätzliche** Klärung herbeizuführen. In mehreren Schreiben bat der TLfDI die Landtagsverwaltung, ihm grundsätzlich folgende Frage zu beantworten:

„Ist im Falle datenschutzrechtlich relevanten Handelns einzelner Abgeordneter der Ältestenrat des Thüringer Landtags gem. § 2 Abs. 5 Satz 3 und 4 ThürDSG für die Aufklärung und Ahndung möglicher datenschutzrechtlicher Verstöße zuständig oder wird die gegenüber dem TLfDI erklärte Rechtsauffassung weiterhin vertreten, wonach der einzelne Abgeordnete als nicht-öffentliche Stelle nach § 2 Abs. 4 Satz 1 BDSG anzusehen ist?“

Eine Antwort der Landtagsverwaltung zu dieser grundsätzlichen Frage des TLfDI lag leider bis zum Redaktionsschluss am 13. Oktober 2017 nicht vor. Die Landtagsverwaltung hatte sich lediglich in dem eingangs genannten konkreten Einzelfall zu der Rechtsauffassung durchringen können, dass hier der Ältestenrat des Landtags für die datenschutzrechtliche Kontrolle des Verhaltens des Abgeordneten zuständig sei.

Fragt man zwei Juristen, so bekommt man drei unterschiedliche Antworten: Diese Binsenweisheit nützt dem TLfDI nichts, wenn es ihm um die konkrete Aufklärung möglicher datenschutzrechtlicher Verstöße von Abgeordneten des Thüringer Landtags geht. Daher muss zu dieser Frage Klarheit bestehen: Ist für die Kontrolle und Ahndung datenschutzrechtlicher Verfehlungen der Landtagsabgeordneten der Ältestenrat des Landtags gem. § 2 Abs. 5 Satz 4 ThürDSG zuständig? Oder kommt hier § 2 Abs. 4 Satz 1 BDSG zur Anwendung, weil die Tätigkeit des Landtagsabgeordneten als Tätigkeit einer nicht-öffentlichen Stelle zu begreifen ist? Beides zusammen geht nicht!



Rathaus – © DOC RABE Media / Fotolia.com

6. Kommunales

6.1 Reichsbürger – Datenübermittlung an den Verfassungsschutz

In den vergangenen Monaten erhielt der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) vermehrt Anfragen von Kommunen und Landkreisen hinsichtlich der Rechtmäßigkeit der Übermittlung von personenbezogenen Daten sogenannter Reichsbürger an das Amt für Verfassungsschutz (AfV).
Anlass war ein Erlass des Thüringer Ministeriums für Inneres und Kommunales, mit dem die Standesämter, die Staatsangehörigkeitsbehörden, die Meldebehörden und die Pass- und Ausweisbehörden gebeten wurden, die ihnen bekannt gewordenen Informationen an das Amt für Verfassungsschutz (AfV) im Thüringer Ministerium für Inneres und Kommunales zu übermitteln.
Bei den anfragenden Behörden herrschte Unsicherheit über die Rechtsgrundlage für die Datenerhebung, die Zulässigkeit der Datenübermittlung sowie den Übermittlungsinhalt.
Rechtsgrundlage für die Datenerhebung und die Datenspeicherung bei den Kommunen und Landkreisen sind zunächst die jeweiligen Spezialnormen, die bei den Standesämtern, Staatsangehörigkeitsbehörden, Meldebehörden und den Pass- und Ausweisbehörden zur Anwendung kommen, um das jeweilige Anliegen der Bürger (und

auch sogenannter Reichsbürger) rechtskonform bearbeiten zu können. Die betreffenden Personen sprechen mit einem konkreten Anliegen bei den jeweiligen Behörden vor. Dabei ist es regelmäßig der Fall, dass bestimmte Bürgerinnen und Bürger aufgrund ihres Verhaltens, ihrer Argumentation und ihrer Einstellung zur Bundesrepublik Deutschland unweigerlich als sogenannte Reichsbürger zu erkennen sind.

Die Zulässigkeit der Datenübermittlung an das AfV im Freistaat Thüringen ergibt sich aus § 19 Abs. 1 Thüringer Verfassungsschutzgesetz (ThürVerfSchG). Danach haben öffentliche Stellen des Freistaates von sich aus dem AfV die ihnen bei Erfüllung ihrer Aufgaben bekannt gewordenen Informationen zu übermitteln, soweit tatsächliche Anhaltspunkte dafür bestehen, dass die Übermittlung der Informationen für die Erfüllung der Aufgaben des AfV nach § 4 Abs. 1 ThürVerfSchG erforderlich ist.

Darüber hinaus ist auch auf § 20 Abs. 1 ThürVerfSchG hinzuweisen, wonach das AfV von den in § 19 Abs. 1 ThürVerfSchG genannten öffentlichen Stellen die Übermittlung entsprechender Informationen anfordern kann, wenn tatsächliche Anhaltspunkte dafür bestehen, dass die Übermittlung für seine Aufgabenerfüllung erforderlich ist (Informationsübermittlung auf Ersuchen des AfV).

Auf Grundlage des §§ 19 Abs. 1 sowie 20 Abs. 1 ThürVerfSchG sowie nach Rücksprache des TLfDI mit dem AfV ist es angezeigt, dass sowohl Name und Adresse als auch die eingereichten Unterlagen, aus denen sich der durch das AfV zu prüfende Sachverhalt ergibt, in Kopie dem AfV übermittelt werden.

Die in § 22 Abs. 1 ThürVerfSchG geregelte Ausnahme, dass Datenübermittlungen dann unterbleiben, wenn für die übermittelnde Stelle erkennbar ist, dass unter Berücksichtigung der Art der personenbezogenen Daten und ihrer Erhebung die schutzwürdigen Interessen der betroffenen Personen das Allgemeininteresse an der Übermittlung überwiegen oder überwiegende Sicherheitsinteressen dies erfordern, war in den vom TLfDI geprüften Fallkonstellationen nicht einschlägig.

Das Ersuchen des AfV war und ist daher datenschutzrechtlich nicht zu beanstanden; das AfV begründete seine Zuständigkeit mit bestimmten Verhaltensweisen des betroffenen Personenkreises, die es für den TLfDI schlüssig als hinreichende tatsächliche Anhaltspunkte für Bestrebungen gegen die freiheitliche demokratische Grundordnung bewertet (vgl. § 4 Abs. 1 Satz 1 Nr. 1 ThürVerfSchG).

Dessen ungeachtet ist dem TLfDI bekannt, dass die Vorgehensweise hinsichtlich der Meldung von sogenannten Reichsbürgern an das AfV auch in anderen Bundesländern in ähnlicher Weise praktiziert wird.

Der Datenschutz steht einer zielgerichteten Kontrolle von so genannten Reichsbürgern durch das AfV nicht im Wege; eine Datenübermittlung von Gemeinden und Landkreisen an das AfV ist unter den Voraussetzungen von § 19 Abs. 1 und § 20 Abs. 1 ThürVerfSchG zulässig. Die Übermittlung personenbezogener Daten hat nach § 22 Abs. 1 ThürVerfSchG dann zu unterbleiben, wenn für die übermittelnde Stelle erkennbar ist, dass unter Berücksichtigung der Art der personenbezogenen Daten und ihrer Erhebung die schutzwürdigen Interessen der betroffenen Personen das Allgemeininteresse an der Übermittlung überwiegen oder überwiegende Sicherheitsinteressen dies erfordern. Da diese Voraussetzungen nicht vorlagen, war die Datenübermittlung zulässig.

6.2 Live-Streaming von Stadtratssitzungen

Auch im Berichtszeitraum für die vergangenen zwei Jahre erkundigten sich Stadtverwaltungen und Bürger wiederum beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) über die Zulässigkeit von Live-Stream-Übertragungen von Stadtratssitzungen.
Hierzu teilte der TLfDI ihnen seine folgende Rechtsauffassung mit:
Grundsätzlich sind Live-Stream-Übertragungen von Stadtratssitzungen aus datenschutzrechtlichen Gründen unzulässig, da keine geeignete Rechtsgrundlage, insbesondere in der spezialgesetzlich maßgeblichen Thüringer Kommunalordnung, Film-, Bild- und Tonaufzeichnungen erlaubt.
Eine andere rechtliche Beurteilung liegt dann vor, wenn die betreffenden Film-, Bild- und Tonaufzeichnungen nicht durch die Stadtverwaltung oder in ihrem Auftrag, sondern durch bei der Stadtverwaltung akkreditierte Medien in deren eigener Verantwortung gefertigt werden. Insofern liegt eine ähnliche Konstellation wie bei der Stadt Erfurt vor, worüber der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) unter dem Gliederungspunkt 5.27 seines 10. Tätigkeitsberichtes für den Öffentlichen

Bereich berichtet hatte. Sinnvollerweise sollte in diesem Falle in der Geschäftsordnung für den Stadtrat z. B. Folgendes geregelt werden:
Film-, Bild- und Tonaufzeichnungen sind möglich, sofern dem die Mehrheit der Stadtratsmitglieder zu Beginn einer Sitzung nicht widerspricht, wobei auch einzelne Stadtratsmitglieder zu Beginn einer Sitzung den Aufnahmen widersprechen können. In diesem Fall werden Aufnahmen zu dieser Person unkenntlich gemacht.
Vor jeder Ratssitzung ist die Kamera so zu positionieren, dass nur der jeweilige Redner am Rednerpult und das Präsidium hinter dem Rednerpult aufgezeichnet werden.
Bei Verstößen gegen die Persönlichkeitsrechte der Stadtratsmitglieder und anderer anwesender Personen kann die Akkreditierung den beteiligten Medien entzogen werden.
Davon zu unterscheiden ist die Zulässigkeit von Livestreams von Plenarsitzungen des Thüringer Landtages, dessen Auftrag nach Artikel 60 Abs. 1 der Verfassung des Freistaats Thüringen darin besteht, öffentlich zu verhandeln.

Nichts Neues im Kommunalrecht: Nach derzeitiger Rechtslage ist die Veröffentlichung von Live-Mitschnitten von Ratssitzungen sowohl durch die Kommune selbst als auch in deren Auftrag datenschutzrechtlich unzulässig. Jedoch sind in eigener Verantwortung handelnde Medienunternehmen unter der Voraussetzung, dass das Persönlichkeitsrecht der bei der Sitzung anwesenden Personen nicht durch die Berichterstattung beeinträchtigt wird, berechtigt, von Stadtratssitzungen auch im Internet in Bild und Ton zu berichten.

6.3 „Meininger Streetview“

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) hatte im Berichtszeitraum durch einen Medienbericht davon Kenntnis erlangt, dass die Stadt Meiningen ein Unternehmen damit beauftragt hatte, sämtliche Straßen, Wege und Plätze etc. zu fotografieren.
Bereits in seinem 10. Tätigkeitsbericht für den Öffentlichen Bereich führte der TLfDI unter dem Gliederungspunkt 5.22, Seite 87 ff „Erfurter Streetview“ über ein ähnliches Verfahren der Stadt Erfurt unter anderem aus, dass bei der Erstellung von Fotos durch oder im Auftrag von öffentlichen Stellen auch immer personenbezogene Daten erhoben werden. Dies ist nach § 19 Thüringer Datenschutzge-

setz (ThürDSG) in aller Regel nicht zur Aufgabenerfüllung erforderlich und damit unzulässig. Die öffentliche Stelle hat daher Vorkehrungen zu veranlassen, dass solche Eingriffe in das Grundrecht auf informationelle Selbstbestimmung unterbleiben. In diesem Zusammenhang hatte die Stadtverwaltung Erfurt seinerzeit auf Anregung des TLfDI durch Dienstanweisung geregelt, dass die Übermittlung von Bildaufnahmen oder Bildausdrucken an Dritte, d. h. andere Stellen innerhalb der Stadtverwaltung, bzw. die Veröffentlichung nur zulässig ist, wenn die auf den Bildaufnahmen enthaltenen personenbezogenen Daten durch geeignete Maßnahmen unkenntlich gemacht worden sind, z. B. durch das Auspixeln oder „Ausradieren“ der entsprechenden Stellen mit einem Fotobearbeitungsprogramm, und auch innerhalb der Stadtverwaltung die auf den Fotos befindlichen personenbezogenen Daten nicht genutzt werden dürfen. Weiterhin wurden alle Aufnahmen, in denen von einem überwiegenden Interesse der betroffenen Grundstückseigentümer auszugehen war, etwa weil überwiegend kein öffentlicher Verkehrsgrund abgebildet ist, gelöscht. Bei Straßen, deren Verkehrsraumbreite sechs Meter unterschritt, wurden die Seitenkameras deaktiviert und mit einem Magnetschild an beiden Seiten des Messfahrzeugs darauf hingewiesen, dass die Seitenkameras außer Betrieb genommen sind und tatsächlich nicht aufzeichnen. Die betroffenen Grundstückseigentümer wurden im Amtsblatt der Landeshauptstadt Erfurt darüber informiert, dass sie ein Widerspruchsrecht in Bezug auf Fotografien von ihrem Grundstück haben. Im Falle eines Widerspruchs sind die betreffenden Fotos so zu bearbeiten, dass ausschließlich Verkehrsanlagen erkennbar sind.

Der TLfDI forderte die Stadtverwaltung Meiningen auf, ihre Dienstanweisung zur Straßenzustandserfassung entsprechend den Empfehlungen des TLfDI, wie sie in den o. g. Regelungen und Vorgehensweisen der Stadtverwaltung Erfurt ihren Niederschlag gefunden hatten, zu ergänzen und die überarbeitete Fassung der Dienstanweisung sowie eine Stellungnahme zur Veröffentlichung des Vorhabens, zum Widerspruchsrecht der Betroffenen und zur datenschutzkonformen Nachbearbeitung von Fotos vorzulegen.

Die Stadtverwaltung Meiningen kam der Aufforderung des TLfDI nach und legte eine überarbeitete Dienstanweisung vor. Hierzu riet der TLfDI der Stadtverwaltung Meiningen, die Zugriffsberechtigung anderer Fachbereiche auf die angefertigten Bilder restriktiv in der Dienstanweisung zu regeln, da keine Rechtfertigungsgründe gem.

§ 20 Abs. 2 Nr. 1 bis 9 ThürDSG in Verbindung mit § 21 ThürDSG für eine solche Datenübermittlung vorlagen. Auch diesen Rat des TLfDI nahm die Stadtverwaltung Meiningen dankbar an.

Eine beim TLfDI wiederkehrende Problematik: Bei der Erstellung von Fotos von Straßen werden auch immer personenbezogene Daten als „Beifang“ erhoben. Diese Daten sind in der Regel nicht zur Aufgabenerfüllung der verantwortlichen öffentlichen Stelle erforderlich und damit unzulässig. Daher hat die verantwortliche Stelle Vorkehrungen zu treffen, dass solche Eingriffe in das Grundrecht auf informationelle Selbstbestimmung der Betroffenen unterbleiben.

6.4 Problematische Betriebsvereinbarung zu einem GPS-System

In zunehmendem Maße bitten Daten verarbeitende Stellen den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) um Prüfung von Entwürfen zu eigenen datenschutzrelevanten Regelungen. So legte eine Stadtverwaltung dem TLfDI den Entwurf einer Betriebsvereinbarung zur GPS-Nutzung bei den Einsatzfahrzeugen ihres Betriebshofs vor.
Der TLfDI teilte der Stadtverwaltung nach Prüfung des vorgelegten Vereinbarungsentwurfs mit, dass die vorgesehenen Regelungen den datenschutzrechtlichen Belangen nicht hinreichend Rechnung trügen. So entspräche nur der Ausschluss von Verhaltens- und Leistungskontrollen den datenschutzrechtlichen Anforderungen. Konkret gehe aus dem Entwurfstext jedoch nicht hervor, welche Daten eines Fahrzeugs oder Beschäftigten im Einzelnen durch den Einsatz von GPS erhoben werden, wie lange diese Daten gespeichert bleiben sollen und zu welchem konkreten Zweck sie durch wen ausgewertet, also verarbeitet werden dürfen. Auch könne nicht nachvollzogen werden, ob GPS in den Fahrzeugen oder als Trackingsystem über Smartphone geplant sei. Des Weiteren wies der TLfDI darauf hin, dass die technischen und organisatorischen Maßnahmen gemäß § 9 ThürDSG und nicht nach BDSG zu treffen seien. Eine Auflistung lediglich abstrakter datenschutzrechtlicher Kontrollziele reiche hierfür nicht aus. Vielmehr seien die tatsächlichen Verhältnisse vor Ort konkret zu berücksichtigen. Auch gehörten mehrdeutige Formulierungen nicht in die Vereinbarung. So blieb z. B. unklar, was unter „Missbrauchskontrolle“ zu verstehen sei. Hier sei konkret anzugeben, welche

Möglichkeiten des Missbrauchs durch die Mitarbeiter möglich sind (z. B. Privatnutzung von Dienstfahrzeugen, unbefugte Nutzung von Dienstfahrzeugen). Sollte auch gemeint sein, dass jemand unbefugt die über GPS entstandenen und gespeicherten Daten verarbeitet habe, sei dies deutlich zu machen.
Der TLfDI empfahl der Stadtverwaltung, sich die Unterlagen zu dem GPS-System vorlegen zulassen, um die gesamten Möglichkeiten des Systems zur Verarbeitung personenbezogener Daten der Beschäftigten zu prüfen und ggf. einzelne Funktionen, die für den konkreten Zweck des Einsatzes nicht erforderlich sind, deaktivieren zu lassen. Weiterhin sollte die Stadtverwaltung prüfen, ob der Betriebshof selbst die Bewegungsdaten der Mitarbeiter erfassen sollte oder eine Auftragsdatenverarbeitung mit einer externen Firma zu vereinbaren sei. In diesem Falle wäre eine gesonderte Vereinbarung zur Auftragsdatenverarbeitung erforderlich und auf den Umstand der Auftragsdatenverarbeitung in der Betriebsvereinbarung hinzuweisen. Der TLfDI wies auf die besondere Bedeutung der Transparenz des Verfahrens für die Betroffenen hin. Konkret bedeutete dies, dass, wenn ein Fahrzeug mit GPS ausgestattet werde, den jeweils betroffenen Mitarbeitern schriftlich mitgeteilt werden müsse, welche konkreten Daten (Bewegungsdaten) gespeichert werden und zu welchem Zweck eine Auswertung oder Einsicht durch wen erlaubt ist.
Nachfolgend teilte die Stadtverwaltung auf Anfrage des TLfDI mit, dass die Hinweise des TLfDI in die Betriebsvereinbarung aufgenommen werden sollen, die Planungsphase der GPS-Nutzung des Betriebshofs derzeit jedoch noch nicht abgeschlossen sei. Der TLfDI wird das Vorhaben weiterhin begleiten.

Daten verarbeitende Stellen tun gut daran, sich vor Einführung neuer Datenverarbeitungssysteme vom TLfDI beraten zu lassen. Dieses proaktive Vorgehen garantiert, dass die vorgesehenen Investitionen gesetzeskonform sind und erspart ggf. unnötigen Ärger im Zusammenhang mit späteren datenschutzrechtlichen Kontrollen.

6.5 Vom Winde verweht ... – Aufgefundene Dokumente von Stadt und Landkreis im Umfeld eines Papierentsorgungsunternehmens

Ein Bürger setzte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) im Berichtszeitraum

darüber in Kenntnis, dass Schreiben einer Stadtverwaltung an das zuständige Landratsamt, die personenbezogene Daten enthielten, in der Nähe eines Unternehmens, das Papier aus blauen Mülltonnen entsorgt, frei umherfliegen würden, und legte dem TLfDI Fotos solcher dienstlicher Schreiben vor.

Daraufhin kontrollierte der TLfDI postwendend das betreffende Entsorgungsunternehmen. Hierbei wurde u. a. festgestellt, dass außerhalb des Firmengeländes in der Nähe der dortigen Papiersilos Papierreste herumlagen, die beim Verladen offenbar durch starken Wind über das firmeneigene Fangnetz hinweg geweht wurden und dann auf einem betriebsfremden Grundstück liegen blieben. Der TLfDI stellte fest, dass das Papierentsorgungsunternehmen nicht gegen datenschutzrechtliche Vorschriften verstoßen hatte, da es keine Aktenvernichtung betrieb, sondern lediglich die Inhalte der blauen Papiertonnen der verantwortlichen Stelle, hier also der Kommune bzw. des Landkreises, zu entsorgen hatte.

Das datenschutzrechtliche Problem bestand vielmehr darin, dass eine Kommune dienstliches Schriftgut, ohne es zuvor selbst zu schreddern, d. h. in weiterhin lesbarer Form, und damit datenschutzrechtlich unzulässig, in die zur „allgemeinen“ Müllentsorgung bestimmten blauen Papiertonnen gegeben hatte.

Etwa zeitgleich zu o. g. Recherchen setzte der TLfDI die Stadtverwaltung und das Landratsamt von der Angelegenheit in Kenntnis und bat, die in deren Kompetenz liegenden technischen und organisatorischen Maßnahmen zur Herstellung datenschutzkonformer Zustände gemäß § 9 ThürDSG, insbesondere zur Gewährleistung der Vertraulichkeit personenbezogener Daten (§ 9 Abs. 2 Nr. 1 ThürDSG) zu treffen und den TLfDI schnellstmöglich zum Sachverhalt über die getroffenen Maßnahmen zu unterrichten.

Der behördliche Datenschutzbeauftragte der betroffenen Stadtverwaltung teilte dem TLfDI mit, dass er, nachdem er von der Angelegenheit erfahren hatte, mit dem Städtischen Hauptamtsleiter den freizugänglichen Fundort der besagten Schreiben nach weiterem dienstlichem Schriftgut abgesucht habe. Dabei seien Teile eines Haushaltsplanes und ein Anhörungsschreiben zur Kreis- und Schulumlage der Städtischen Kämmerei sichergestellt worden. Die Stadtverwaltung legte ein Sicherstellungsprotokoll vor und informierte den TLfDI darüber, dass sie alle Mitarbeiter sowie die Bürgermeister der Ortsteile anlässlich dieses Vorkommnisses nochmals

auf den sorgfältigen Umgang mit zu entsorgendem Dienstgut hingewiesen habe.

Aus dem Auge, aus dem Sinn? Wenn eine Kommune Papiere mit personenbezogenen Daten in den Papiermüll entsorgt hat, entbindet sie das nicht von ihren datenschutzrechtlichen Verpflichtungen. Sie bleibt als verantwortliche Stelle zuständig für die Einhaltung aller technischen und organisatorischen Maßnahmen gem. § 9 ThürDSG, die erforderlich sind, um die Ausführung der Bestimmungen des ThürDSG zu gewährleisten. In diesem Falle hätte die verantwortliche Stelle dafür sorgen müssen, dass kein lesbares dienstliches Schriftgut mit personenbezogenen Daten in die blaue Tonne gelangt.

6.6 Demokratieverständnis eines Bürgermeisters versus Rechtslage

Eine Beschwerdeführerin, die als Stadträtin gewählt war, setzte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) darüber in Kenntnis, dass ein Bürgermeister alle anderen Stadtratsmitglieder umfassend über die von der Beschwerdeführerin an die Kommunalaufsicht des Landratsamtes zu leistenden Verwaltungsgebühren informiert und ferner den kompletten persönlichen Schriftwechsel der Stadträtin mit dem Landratsamt zur Verfügung gestellt hatte.
Der TLfDI teilte dem Bürgermeister mit, dass es sich bei der Angelegenheit nach seiner vorläufigen Beurteilung um eine unzulässige Übermittlung personenbezogener Daten innerhalb des öffentlichen Bereichs gem. § 21 Thüringer Datenschutzgesetz (ThürDSG) handle. Zugleich forderte der TLfDI den Bürgermeister auf, zu der Angelegenheit Stellung zu nehmen und insbesondere mitzuteilen, auf welcher Rechtsgrundlage die o. g. Datenübermittlung beruhte und welchen Zwecken sie diente.
Nachdem der Bürgermeister dem TLfDI geantwortet hatte, stellte sich der Sachverhalt wie folgt dar:
Die Stadtverwaltung hatte allen Mitgliedern des Stadtrates den Widerspruchsbescheid der Kommunalaufsicht des Landratsamtes zum Widerspruch der Stadträtin gegen eine Entscheidung der Stadtverwaltung Blankenhain zum Verlust ihres Sitzes in einem Stadtratsausschuss einschließlich der personenbezogenen Daten der Stadträtin übermittelt. Davon betroffen waren unter anderem der komplette

persönliche Schriftwechsel der Stadträtin mit dem Landratsamt sowie Informationen über die von ihr zu leistenden Verwaltungsgebühren.
Die Übermittlung des kompletten persönlichen Schriftwechsels der Beschwerdeführerin und Stadträtin mit dem Landratsamt an die übrigen Mitglieder des Stadtrates sah der Bürgermeister als zulässig an, da der Widerspruch der betroffenen Stadträtin das Verfahren zur Bildung von Fraktionen generell in Frage gestellt und es sich daher um eine Grundsatzangelegenheit gehandelt hätte. Obwohl der Bürgermeister einräumte, dass es in dieser Frage keine konkrete Rechtsvorschrift in der Thüringer Kommunalordnung (ThürKO) gebe, gehöre es nach seinem Demokratieverständnis zum kollegialen Umgang, den Schriftwechsel dem Stadtrat zur Kenntnis zu geben.
Der TLfDI bewertete diesen Sachverhalt datenschutzrechtlich folgendermaßen:
Eine Rechtsvorschrift aus der Thüringer Kommunalordnung (ThürKO), die die Übermittlung der personenbezogenen Daten der Stadträtin aus ihrem Schriftwechsel mit der Kommunalaufsicht des Landratsamtes an die anderen Stadträte gestattete, war für den TLfDI nicht ersichtlich. Deshalb kam als Rechtsgrundlage hier nur § 4 Abs. 1 in Verbindung mit § 21 Abs. 1 ThürDSG in Betracht.
Die Voraussetzungen des § 21 Abs. 1 Nr. 1 ThürDSG, dass die Datenübermittlung zwischen zwei öffentlichen Stellen zur Erfüllung der Aufgaben der übermittelnden Stelle oder des Empfängers erforderlich ist, lagen im konkreten Fall aber nicht vor. Das ergab sich bereits daraus, dass der Widerspruchsbescheid einen persönlichen Widerspruch der betroffenen Stadträtin betraf und die Kenntnis seines konkreten Wortlauts nicht zur Erfüllung der in der Zuständigkeit der Stadtverwaltung und des Stadtrates von Blankenhain liegenden Aufgaben erforderlich war. Soweit der Bürgermeister vortrug, dass es zur Rechtsfrage der Bildung von Fraktionen erforderlich gewesen sei, die anderen Stadträte darüber zu informieren, so hätte der Bürgermeister über die (in dem Widerspruchsbescheid enthaltene) Rechtsauffassung der Kommunalaufsicht abstrakt und losgelöst vom Einzelfall und damit ohne die Übermittlung personenbezogener Daten der betroffenen Stadträtin informieren können und müssen.
Zudem widersprach die Übermittlung der personenbezogenen Daten der betroffenen Stadträtin an ihre Kolleginnen und Kollegen im Kommunalparlament dem Grundsatz der Datensparsamkeit. Dieser in § 1 Abs. 2 Satz 1 ThürDSG geregelte Grundsatz besagt, dass sich

unter anderem die Verarbeitung (worunter gem. § 3 Abs. 3 Nr. 4 ThürDSG auch die Übermittlung fällt) und Nutzung personenbezogener Daten an dem Ziel auszurichten haben, so wenig wie möglich personenbezogene Daten zu verarbeiten und zu nutzen. Entgegen der Auffassung des Bürgermeisters hing die Zulässigkeit einer Datenübermittlung nicht von der Verpflichtung der Stadtratsmitglieder zur Verschwiegenheit aus § 12 Abs. 3 Satz 1 in Verbindung mit § 24 ThürKO ab. Auch beim Grundrecht auf informationelle Selbstbestimmung sind Behörden an Recht und Gesetz gebunden. Wie mit personenbezogenen Daten verfahren wird, ist daher weder einer Frage des individuellen Demokratieverständnisses noch der Verschwiegenheitsverpflichtung von verantwortlichen Personen.
Im Ergebnis der datenschutzrechtlichen Prüfung hat der TLfDI die ohne Rechtsgrundlage erfolgte Übermittlung des kompletten persönlichen Schriftwechsels der betroffenen Stadträtin mit dem Landratsamt sowie des Gebührenbescheides der betroffenen Stadträtin an den Stadtrat als Verletzung datenschutzrechtlicher Vorschriften gem. § 39 Abs. 1 ThürDSG beanstandet. Zugleich forderte der TLfDI den Bürgermeister auf, die Angelegenheit in der Stadtverwaltung auszuwerten und ihn über die Art und Weise der Erledigung dieser Forderungen in Kenntnis zu setzen.
Eine Reaktion der Stadtverwaltung auf die datenschutzrechtliche Beanstandung steht derzeit noch aus; der TLfDI wird daher im nächsten Tätigkeitsbericht auf diesen Sachverhalt zurückkommen.

Ein Bürgermeister ist nicht befugt, den persönlichen Schriftwechsel eines Stadtratsmitgliedes anderen Stadträten zur Kenntnis zu geben. Dies stellt mangels einer geeigneten Rechtsgrundlage einen Verstoß gegen datenschutzrechtliche Vorschriften in Form einer unzulässigen Datenübermittlung innerhalb des öffentlichen Bereichs gem. § 21 ThürDSG dar. Auch beim Grundrecht auf informationelle Selbstbestimmung sind Behörden an Recht und Gesetz gebunden. Wie mit personenbezogenen Daten verfahren wird, kann daher auch keine Frage des individuellen Demokratieverständnisses von verantwortlichen Personen oder der Pflicht zur Verschwiegenheit der Stadtratsmitglieder nach § 12 Abs. 3 Satz 1 in Verbindung mit § 24 ThürKO sein. In diesem Falle hat der TLfDI den Datenschutzverstoß aufgrund seiner Schwere gemäß § 39 Abs. 1 ThürDSG beanstandet.

6.7 Sehr beliebt: das Posten von Unterschriftenlisten

Ein Beschwerdeführer teilte dem Thüringer Landesbeauftragten für Datenschutz und Informationsfreiheit (TLfDI) mit, dass der Vorsitzende einer Kommunalverwaltung Fotografien von ausgefüllten Unterschriftenlisten des Thüringer Bürgeraufrufs zum Thema Gebietsreform bei Facebook veröffentlicht und mitgeteilt habe, dass diese Unterschriftenlisten direkt in seiner Verwaltung abgeholt und abgegeben werden können.
Der TLfDI forderte den verantwortlichen Leiter der Kommunalverwaltung auf, zu der Angelegenheit Stellung zu nehmen und insbesondere mitzuteilen, auf welcher Rechtsgrundlage die o. g. Datenübermittlung beruht und zu welchem Zwecke sie erfolgte, da es sich möglicherweise hierbei um eine unzulässige Übermittlung personenbezogener Daten an Stellen die ihren Sitz außerhalb des Geltungsbereichs des Grundgesetzes haben, § 23 Thüringer Datenschutzgesetz (ThürDSG) handle.
In seinem Antwortschreiben setzte der Leiter der Kommunalverwaltung den TLfDI darüber in Kenntnis, dass ihm beim Hochladen des Fotos der Unterschriftenlisten ein Fehler unterlaufen sei, was er bedauere. Da die beabsichtige Unkenntlichmachung des personenbezogenen Inhaltes der Listen nicht funktioniert habe, sei das ursprüngliche Bild gepostet worden. Nachdem er es erst später bemerkte habe, habe er den Beitrag sofort gelöscht. Der „Facebook-Post“ sei über seine privaten Account erfolgt. Er sei als Privatperson Mitglied im Verein Selbstverwaltung für Thüringen e. V. Da viele Menschen dem Aufruf gefolgt seien, wollte er seine Freude mit anderen teilen. Auf Anfrage, wo man die Unterschriften abgeben könne, habe er angegeben, bei ihm zu Hause oder in der Kommunalverwaltung, die ebenfalls ein Mitglied im o. g. Verein sei.
Aufgrund der obigen Darlegungen ging der TLfDI davon aus, dass der Leiter der Kommunalverwaltung in der beschwerdegegenständlichen Angelegenheit als Privatperson und nicht als Leiter einer öffentlichen Stelle gehandelt hatte. Insofern ist ein Verstoß gegen datenschutzrechtliche Vorschriften in Form einer unzulässigen Übermittlung personenbezogener Daten an Stellen außerhalb des Geltungsbereichs des Grundgesetzes, § 23 ThürDSG nicht nachweisbar. Der TLfDI wird das Verhalten des Verwaltungsleiters als Privatperson gesondert überprüfen.

Beim datenschutzrelevanten Publizieren, insbesondere in sozialen Netzwerken, kommt es gelegentlich zu Grenzfällen, bei denen die Aufsichtsbehörde nicht ohne weiteres festzustellen vermag, ob der Leiter einer Behörde als Privatperson oder stellvertretend für seine Behörde gehandelt hat. In diesen Fällen kann der öffentlichen Stelle kein Verstoß gegen datenschutzrechtliche Vorschriften angelastet werden. Dessen ungeachtet darf auch die Privatperson nicht Daten Dritter ohne deren Einwilligung im Internet veröffentlichen.

6.8 Einwohnermeldeamt: Einvernahme von Minderjährigen als Zeugen

Ein Vater wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und beschwerte sich darüber, dass ein Einwohnermeldeamt seine achtjährigen Kinder als Zeugen in einem Streit um die Anmeldung des Wohnsitzes ohne die Zustimmung beider Eltern vernommen habe. Von der Mutter der Kinder sei er getrennt lebend, beide Elternteile hätten aber das gemeinsame Sorgerecht für die Kinder.
Die Mutter der Kinder hatte zuvor einen neuen Wohnsitz gewählt und sich und die Kinder beim zuständigen Einwohnermeldeamt angemeldet. Am Tag nach der Ummeldung begab sich der Vater zu dem für ihn zuständigen Meldeamt und beantragte dort die Anmeldung der Kinder an seinem Wohnsitz. Dies wurde abgelehnt mit der Begründung, dass gerade das andere Meldeamt am Wohnsitz der Mutter die Anmeldung vorgenommen habe. Daraufhin beschwerte der Vater sich bei diesem Meldeamt, wie es die Anmeldung der Kinder vornehmen könne, ohne dass die Einwilligung beider Eltern vorläge. Die Angaben der Mutter seien nicht korrekt; die Kinder würden überwiegend bei ihm wohnen. Dies wiederum nahm das Meldeamt am Wohnsitz der Mutter zum Anlass, die beiden Kinder in der Behörde im Beisein der Mutter ohne Benachrichtigung des Vaters darüber zu vernehmen, bei welchem Elternteil sie sich überwiegend aufhalten würden.
Der Vater sah darin eine unzulässige Datenerhebung und wandte sich an den TLfDI.
Nach § 4 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) ist die Erhebung personenbezogener Daten nur zulässig, wenn das ThürDSG oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder soweit der Betroffene eingewilligt hat.

Die beiden Kinder wurden nach § 26 Abs. 1 Nr. 2 Thüringer Verwaltungsverfahrensgesetz (ThürVwVfG) als Zeugen vernommen.
Da die beiden Kinder minderjährig waren und die Eltern getrennt lebten, wäre eine gemeinsame Einwilligung nach § 1687 Abs. 1 Satz 1 Bürgerliches Gesetzbuch (BGB) in die Vernehmung als Zeugen erforderlich gewesen.
§§ 1687 BGB hat folgenden Wortlaut:
„§ 1687 Ausübung der gemeinsamen Sorge bei Getrenntleben
(1) Leben Eltern, denen die elterliche Sorge gemeinsam zusteht, nicht nur vorübergehend getrennt, so ist bei Entscheidungen in Angelegenheiten, deren Regelung für das Kind von erheblicher Bedeutung ist, ihr gegenseitiges Einvernehmen erforderlich. Der Elternteil, bei dem sich das Kind mit Einwilligung des anderen Elternteils oder auf Grund einer gerichtlichen Entscheidung gewöhnlich aufhält, hat die Befugnis zur alleinigen Entscheidung in Angelegenheiten des täglichen Lebens. Entscheidungen in Angelegenheiten des täglichen Lebens sind in der Regel solche, die häufig vorkommen und die keine schwer abzuändernden Auswirkungen auf die Entwicklung des Kindes haben. Solange sich das Kind mit Einwilligung dieses Elternteils oder auf Grund einer gerichtlichen Entscheidung bei dem anderen Elternteil aufhält, hat dieser die Befugnis zur alleinigen Entscheidung in Angelegenheiten der tatsächlichen Betreuung. § 1629 Abs. 1 Satz 4 und § 1684 Abs. 2 Satz 1 gelten entsprechend.“
Für die Entscheidung zur Durchführung der Zeugenvernehmung war das gegenseitige Einvernehmen der Eltern gem. § 1687 Abs. 1 Satz 1 BGB erforderlich, da es sich um die Entscheidung einer Angelegenheit von erheblicher Bedeutung handelte.
Von erheblicher Bedeutung für das Kind sind alle Angelegenheiten, deren Entscheidung nur schwer oder gar nicht abzuändernde Auswirkungen auf die Entwicklung des Kindes haben (Palandt-Götz, Kommentar zum BGB, § 1687, Rd. 7).
Im Falle der Trennung von Eltern ist es anerkannter Maßstab familienrechtlicher Entscheidungen zu versuchen, Kindern einen Loyalitätskonflikt für oder gegen einen Elternteil zu ersparen. Daher musste der TLfDI im konkreten Fall feststellen, dass die Vernehmung der Kinder geeignet war, in ihnen Schuldgefühle auszulösen, die möglicherweise schwer zu verarbeiten sind. Diese können dem unbeschwerten Verhältnis zu beiden Eltern im Wege stehen und so für die Entwicklung der Kinder eine schwer abzuändernde Auswirkung haben.

Im Übrigen standen auch mildere Mittel zur Klärung des Sachverhaltes zur Verfügung. So hätten Nachbarn, Lehrer oder vielleicht auch schon das zuständige Jugendamt Auskunft über den gewöhnlichen Aufenthalt der Kinder geben können.
§ 1687 Abs. 1 Satz 2 BGB, auf den sich das Meldeamt berief, war vorliegend aus mehreren Gründen nicht anwendbar:
Der Paragraf knüpft als Voraussetzung an die Kenntnis des gewöhnlichen Aufenthaltes des Kindes an. Im vorliegenden Fall war der gewöhnliche Aufenthalt aber gerade streitig. Das melderechtliche Verfahren sollte erst zur Kenntnis des gewöhnlichen Aufenthaltes der Kinder führen; hierzu sollte deren Zeugenbefragung ja gerade dienen. Es wurde also, um die Anwendbarkeit einer Norm zu Beginn des Verwaltungsverfahrens zu begründen, die Kenntnis des Ausgangs des Verwaltungsverfahrens vorausgesetzt. Dies stellte einen logischen Fehler dar.
Des Weiteren setzt § 1687 Abs. 1 Satz 2 BGB voraus, dass sich das Kind mit Einwilligung des anderen Elternteils oder aufgrund einer gerichtlichen Entscheidung gewöhnlich beim anderen Elternteil aufhält. Eine Gerichtsentscheidung bezüglich des Aufenthaltes lag zu dem fraglichen Zeitraum nicht vor. Es war auch keine Einwilligung vorhanden, bei welchem Elternteil sich die Kinder gewöhnlich aufhalten sollten. Vielmehr stritten die Eltern über den gewöhnlichen Aufenthalt.
Schon aus diesen Gründen war § 1687 Abs. 1 Satz 2 BGB nicht anwendbar.
Selbst wenn diese – vorliegend nicht gegebenen – Voraussetzungen des § 1687 Abs. 1 Satz 2 BGB unterstellt würden, wäre immer noch keine Angelegenheit des täglichen Lebens gegeben gewesen. Angelegenheiten des täglichen Lebens sind nach der Legaldefinition des § 1687 Abs. 1 Satz 3 BGB solche, die in der Regel häufig vorkommen und die keine schwer abzuändernden Auswirkungen auf die Entwicklung des Kindes haben.
Wie oben ausgeführt, war durch die Zeugenvernehmung eine schwer abzuändernde Auswirkung auf die Psyche der Kinder zu befürchten. Zusätzlich hätte nach § 1687 Abs. 1 Satz 3 BGB aber auch noch hinzukommen müssen, dass die Entscheidung häufig vorkommt. Das ist bei einer Vernehmung von Kindern als Zeugen augenscheinlich nicht der Fall.
Damit musste der TLfDI abschließend feststellen, dass nach § 4 Abs. 1 ThürDSG eine unzulässige Erhebung personenbezogener

Daten vorlag, da weder § 1687 Abs. 1 Satz 2 BGB noch eine andere Rechtsgrundlage für die Datenerhebung infrage kam. Der TLfDI sprach daher gegenüber der Stadtverwaltung eine Beanstandung nach § 39 Abs. 1 ThürDSG aus.

Die Vernehmung Minderjähriger in einem Verwaltungsverfahren setzt die Einwilligung der Sorgeberechtigten voraus – jedenfalls dann, wenn die Kinder noch relativ jung sind, sie die Konsequenzen ihrer Aussage nicht vollständig abschätzen können oder die Aussage als solche besonders belastend sein kann. Sollte eine Befragung erfolgen, ohne dass eine Einwilligung der Sorgeberechtigten vorliegt, stellt dies nicht nur ein zivilrechtliches Unterlassen, sondern auch einen datenschutzrechtlichen Verstoß dar. § 1687 BGB kommt in solch einem Fall auch nicht als Rechtsgrundlage der Datenerhebung in Frage. Dies führt dazu, dass die Datenerhebung unzulässig ist.

6.9 Videoüberwachung im Internat – Videogaga 1

Der Datenschutzbeauftragte eines Landkreises bat den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) im Berichtszeitraum um Bewertung einer geplanten Videoüberwachung eines Berufsschulinternates in Trägerschaft des betreffenden Landkreises.
Bei einem Beratungs- und Informationsgespräch des TLfDI vor Ort stellte sich heraus, dass insgesamt 17 Kameras, davon sechs für den Außenbereich des Internats und elf im Inneren des Gebäudes, vorgesehen waren. Die Kameraaufnahmen sollten einheitlich 48 Stunden gespeichert werden. Nach Ansicht der Internatsleitung waren sämtliche Kameras zur „Erfüllung und der Wahrnehmung des Hausrechts“ erforderlich. Offensichtlich bezog sich die Internatsleitung dabei auf § 25a Abs. 1 Thüringer Datenschutzgesetz (ThürDSG), der die Videoüberwachung (Videobeobachtung oder -aufzeichnung) mithilfe optisch-elektronischer Einrichtungen für zulässig erklärt, soweit sie zur Wahrnehmung des Hausrechts der verantwortlichen öffentlichen Stelle erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen des Betroffenen überwiegen. Als typische Probleme im Zusammenhang mit der Wahrnehmung des Hausrechts stufte die Internatsleitung übermäßigen Alkoholkonsum, unerlaubtes Rauchen, nächtliche Ruhestörungen, Sachbeschädigung und Vanda-

lismus ein. Jedoch konnten die genannten Vorkommnisse gegenüber dem TLfDI nicht schriftlich nachgewiesen werden.
Zum Kriterium der Erforderlichkeit einer Videoüberwachung nach § 25 Abs. 1 ThürDSG machte die Internatsleitung gegenüber dem TLfDI folgende Angaben: Die Überwachung einer Fensterfront begründete sie damit, dass Internatsbewohner bei sommerlichen Temperaturen die Beine aus den Fenstern ihrer Zimmer baumeln lassen würden. Daher sollten Fensterstürze mittels der Kamerabeobachtung vermieden werden. Die Vertreter des TLfDI bezweifelten bereits die Geeignetheit dieser Überwachungsmaßnahme zum Zwecke der Unfallvermeidung, da zwar etwaige Abstürze gefilmt werden können, jedoch keine Zeit zum Eingreifen bleiben dürfte, einen Absturz zu verhindern. Die Vertreter des TLfDI wiesen auch darauf hin, dass die Zulässigkeit einer Videoüberwachung nur anhand der konkreten Zweckbestimmung sämtlicher Kameras sowie der Dokumentation von früheren sicherheitsrelevanten Vorkommnissen in deren jeweiligen Überwachungsbereichen beurteilt werden könne. Der vor Ort anwesende Vertreter der benachbarten Berufsschule wies darauf hin, dass insbesondere die Lehrkräfte als Benutzer des Fußwegs zur Berufsschule über den Außenbereich des Internates durch eine dort ebenfalls geplante Videoüberwachung in ihren Persönlichkeitsrechten beeinträchtigt würden. Weiterhin informierten die Vertreter des TLfDI über das grundsätzliche Verbot von Videoüberwachungsmaßnahmen im schulischen Umfeld aufgrund einer Verfügung des Thüringer Bildungsministeriums.
Nach vorläufiger Beurteilung aller geplanten Kamerastandorte musste der TLfDI von einer Unzulässigkeit der vorgesehenen Videoüberwachung ausgehen. Nichts anderes gelte für Kameraattrappen. Denn der jeweilige Betroffene im Erfassungsbereich einer Videokameraattrappe weiß ja gerade nicht, dass von ihm keine personenbezogenen Daten erfasst werden, sondern richtet sein Handeln gerade danach aus, dass ihn die Videokamera-Attrappe erfassen kann.
Die Vertreter des TLfDI empfahlen ferner, anstelle von Videoüberwachungsmaßnahmen Mittel, die nicht oder weniger in das Persönlichkeitsrecht der Betroffenen (Bewohner, Mitarbeiter und Besucher des Internates sowie Lehrer der angrenzenden Schule) eingreifen, in Betracht zu ziehen. Dazu zählten z. B. Licht-Bewegungsmelder, um unerlaubtes Rauchen oder unerlaubten Alkoholgenuss gerade in den Nachtzeiten zu verhindern.

Im Nachgang zum o. g. Ortstermin legte das Landratsamt dem TLfDI Auszüge aus dem Dienstbuch des Internates zu dortigen sicherheitsrelevanten Vorkommnissen aus der jüngeren Vergangenheit sowie Erfassungsblätter zu Zweck, Speicherdauer und Betriebsmodus der jeweiligen Kameras vor. Diese Unterlagen beurteilte der TLfDI erneut am Maßstab des § 25a Abs. 1 ThürDSG.
Beurteilungserheblich war dabei insbesondere, ob die dokumentierten Vorkommnisse die Annahmen rechtfertigen, dass eine Überwachung mittels der jeweiligen Kamera zur Wahrnehmung von speziellen, in den kamerabezogenen Erfassungsblättern genannten Zwecken erforderlich ist, wobei keine Anhaltspunkte dafür bestehen dürfen, dass schutzwürdige Interessen der Betroffenen, d. h. der videografierten Personen, überwiegen.
Die Internatsleitung begründete den Einsatz der Videokameras im Außenbereich im Einzelnen mit dem Schutz geparkter PKW vor Vandalismus, der Erkennung einlassbegehrender Personen, der Durchsetzung des Rauchverbotes und dem Schutz des eigenen bzw. der benachbarten Grundstücke vor Verunreinigung bzw. Beschädigung. Jedoch fanden sich im Dienstbuch keine Eintragungen zu entsprechenden Vorkommnissen oder es waren lediglich unerhebliche Einzelereignisse dokumentiert. Dass z. B. laut Dienstbuch der Hausmeister beobachtet hatte, wie eine Person Luft aus den Reifen eines PKW ließ oder auf dem Parkplatz unerlaubterweise geraucht wurde, vermochte eine Videoüberwachung des Parkplatzes im konkreten Fall nicht zu rechtfertigen, da es sich nur um eine unerhebliche einmalige Sachbeschädigung bzw. einen Verstoß gegen das Rauchverbot handelte. Auch war für den TLfDI nicht nachvollziehbar, warum die Aufnahmen einer Kamera zur Erkennung einlassbegehrender Personen gespeichert werden sollen, da es für die Zecke der Zugangskontrolle und Erkennung von einlassbegehrenden Personen ausreicht, die Kamera lediglich als „verlängertes Auge“ im Sinne eines „Monitoring“ (Videobeobachtung) zu nutzen. Deshalb war eine Videoaufzeichnung als eingriffsintensivste Variante der Videoüberwachung nach § 25a ThürDSG hier nicht erforderlich.
Die Erforderlichkeit einer Videoüberwachung des Raucherpavillons zur Durchsetzung des Rauchverbotes konnten die Vertreter der Internatsleitung anhand der Eintragungen im Dienstbuch ebenfalls nicht belegen. In einem Falle wurde laut Dienstbuch eine Scheibe vom Gewächshaus auf dem privaten Nachbargrundstück beschädigt. Da es sich hierbei um ein einmaliges Vorkommnis handelte, dies

aber nicht auf dem Internatsgrundstück (Hausrecht) geschah, rechtfertigte dieser Vorfall eine Videoüberwachung gerade nicht. Ebenso war die Videoüberwachung eines Innenraumes, in dem Internatsgelder verwaltet werden, anhand des Dienstbuchs nicht begründbar, zumal mildere Mittel wie die Nutzung einer abschließbaren Geldkassette bzw. eines Tresors sowie bauliche Maßnahmen, wie der Einbau eines Tresens, denkbare Alternativen darstellten, die gerade nicht in das Grundrecht auf informationelle Selbstbestimmung eingreifen.
Die Erforderlichkeit einer Videoüberwachung der Flure im Internat versuchte deren Leitung mit der Gewährleistung der Sicherheit der anvertrauten Jugendlichen, insbesondere der minderjährigen Schülerinnen und mit der Erkennung von Vandalismus zu begründen. Das Dienstbuch enthielt dazu einige Eintragungen zu Vorkommnissen im Wohnbereich, so u. a. die Entwendung eines Handys, Streit unter alkoholisierten Bewohnern und Belästigungen von Mitbewohnern, unerlaubte Einnahme von Nikotin und Rauschmitteln in den Zimmern, Verunreinigungen von Sanitäranlagen und Türen sowie unangemeldete Aufenthalte fremder Personen. In diesen Fällen stellte sich für den TLfDI die Frage, ob Videoüberwachungen mittels Kameras in den Fluren des Wohnbereichs geeignet wären, um das Hausrecht hinsichtlich o. g. Vorfälle durchzusetzen. Das wäre nur dann der Fall gewesen, wenn eine Videobeobachtung (Monitoring) stattfinden sollte und eine verantwortliche Person erforderlichenfalls unverzüglich eingreifen könnte, um den Verstoß gegen das Hausrecht zu unterbinden. Angesichts der hohen Bedeutung des Rechtes, sein Wohnumfeld unbeobachtet zu nutzen, sind Videoüberwachungsanlagen gem. § 25a Abs. 1 ThürDSG jedoch nur dann zulässig, wenn keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen anderer Personen überwiegen. Daher ging der TLfDI hier davon aus, dass infolge der Überwachung des Wohnumfeldes in den Fluren schutzwürdige Interessen anderer Personen über Gebühr verletzt werden. Deshalb waren die vorgesehenen Videoüberwachungsmaßnahmen für die Durchsetzung der Hausordnung in geschlossen Räumen im Ergebnis unzulässig.
Der TLfDI teilte dem Landratsamt mit, dass der Einsatz sämtlicher vorgesehener Kameras nicht unzulässig sei und eine Installation dieser Kameras zu unterbleiben habe. Der TLfDI empfahl, lediglich eine Kamera zum Zwecke des Erkennens von einlassbegehrenden Personen auf den Betriebsmodus des „verlängerten Auges“ (ohne Speicherung der Videoaufzeichnungen) einzusetzen.

Nachfolgend setzte das Landratsamt den TLfDI darüber in Kenntnis, dass im Ergebnis einer Beratung von einer Installation der vorgesehenen Videoüberwachungskameras abgesehen und der empfohlenen Nutzung einer Kamera ohne Speicherung in Verbindung mit einer Wechselsprechanlage zur Einlasskontrolle gefolgt werde.

Ob eine Videokamera datenschutzrechtlich zulässig ist, richtet sich für öffentliche Stellen (Behörden) nach § 25a Abs. 1 ThürDSG und ist anhand ihrer konkreten Zweckbestimmung sowie von Nachweisen zu früheren sicherheitsrelevanten Vorkommnissen im Überwachungsbereich der Kamera zu beurteilen.
Angesicht der hohen Bedeutung des Rechtes, sein Wohnumfeld unbeobachtet zu nutzen, sind Videoüberwachungsanlagen jedoch nur dann zulässig, wenn keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen anderer Personen überwiegen. Daher sind Videoüberwachungsmaßnahmen für die Durchsetzung der Hausordnung in geschlossenen Räumen eines Internates in öffentlicher Trägerschaft grundsätzlich nicht zulässig.

6.10 Videogaga 2 – Gefilmter Müll

Ein Betroffener beschwerte sich bei dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) darüber, dass vor dem Gebäude einer Feuerwehr eine Anlage zur Videoüberwachung installiert wurde. Nicht etwa, wie man annehmen möchte, zur Überwachung der Sicherheit der Feuerwehr, sondern vielmehr zur Überwachung des Mülltonnenstandplatzes, der sich auf dem öffentlich zugänglichen Gelände vor dem Feuerwehrgebäude befindet.
Der TLfDI fragte aufgrund der Beschwerde bei der Gemeinde nach. Die Gemeinde begründete diese Maßnahme damit, dass in letzter Zeit wiederholt illegal Müll im Bereich des Mülltonnenstandplatzes abgeladen worden sei. Diese Tatsache sowie das Hausrecht rechtfertigten nach Auffassung der Gemeinde den Einsatz der Videotechnik. Die Kamera habe eine derartig abschreckende Wirkung, dass es zu keiner illegalen Müllentsorgung mehr gekommen sei.
Der TLfDI hat der Gemeinde nach Prüfung mitgeteilt, dass der Einsatz von Videotechnik wegen des damit verbundenen Grundrechtseingriffs nur gerechtfertigt sei, wenn tatsächlich dokumentierte Anhaltspunkte vorhanden sind, dass dies zur Wahrung des Hausrechtes

erforderlich ist. Die Auffassung, dass eine Videoüberwachung aufgrund einer damit verbundenen Abschreckung gerechtfertigt sein könnte, verkennt, dass aufgrund des mit einer Videoüberwachung verbundenen Grundrechtseingriffs das Hausrecht eng auszulegen ist und die Abschreckung keinen Gesetzeszweck im Sinne des § 25a Thüringer Datenschutzgesetz (ThürDSG) darstellt.
Die Gemeinde hat daraufhin die Kamera abgebaut.

Videokameras im öffentlichen Raum dürfen von öffentlichen Stellen nur unter den engen Voraussetzungen des § 25a ThürDSG zum Einsatz gelangen. Die Voraussetzung der Erforderlichkeit zur Wahrung des Hausrechts ist eng auszulegen.

6.11 Videoüberwachung durch eine Ampelanlage in Erfurt?

Ein Bürger bat den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) um die datenschutzrechtliche Bewertung einer Kamera an einer Straßenkreuzung in der Nähe seiner Wohnung.
Die Stadtverwaltung Erfurt teilte dem TLfDI auf Anfrage die Stellungnahme ihres zuständigen Tiefbau- und Verkehrsamtes mit, wonach an der betreffenden Kreuzung keine Verkehrsbeobachtungskameras installiert seien. Bei den dortigen Einrichtungen handle es sich vielmehr um sogenannte Videodetektoren, die zur Erfassung der Fahrzeugströme in den Zufahrten der Iderhoffstraße als Grundlage der verkehrsabhängigen Signalsteuerung dienen. Bei diesen Videodetektoren erfolge keine Bildübertragung an das Knotensteuergerät und in die Verkehrsleitzentrale. Vielmehr seien bei der erstmaligen Installation Detektorfelder definiert worden, deren optische Verarbeitung im laufenden Betrieb direkt im Videodetektor erfolge. Zum Knotensteuergerät würden vom Videodetektor lediglich die Ergebnisse (Belegung der Detektorfelder in Form von „Ja/Nein“-Informationen), jedoch keine Abbildungen des detektierten Bereich mit etwaigen personenbezogenen Daten übermittelt.
Der TLfDI vertritt die Auffassung, dass das o. g. Erfassungsszenario datenschutzrechtlich zulässig ist, da nachvollziehbar dargelegt wurde, dass keine personenbeziehbare Beobachtung erfolgt, also weder Kfz-Kennzeichen noch Verkehrsteilnehmer o. ä. identifizierbar sind.
Die datenschutzrechtliche Bewertung, wonach bezüglich der o. g. Verkehrsdatenerfassung eine Personenbeziehbarkeit nicht gegeben

ist und somit kein Verstoß gegen datenschutzrechtliche Vorschriften vorliegt, wurde dem Beschwerdeführer abschließend mitgeteilt.

Aus der Perspektive des Verkehrsteilnehmers bzw. Anwohners ist nicht ohne Weiteres festzustellen, ob es sich bei den kameraähnlichen Vorrichtungen in größeren Städten um Videodetektoren zur Signalsteuerung oder Verkehrsüberwachungskameras mit dem Potential zur personenbeziehbaren Beobachtung handelt. Insofern ist es erforderlich, dass der TLfDI bei der Recherche zum bewertungsrelevanten Sachverhalt auf die Fachkompetenz der zuständigen öffentlichen Stellen zurückgreift.

6.12 Videoüberwachung durch Stadtverwaltung

Ein Bürger wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Er hatte durch die Presse von der Videoüberwachung durch das Ordnungsamt der Stadt erfahren. Er erbat Rechtsauskunft über die Rechtsgrundlagen der Videoüberwachung und die näheren Umstände, die zur Videoüberwachung führten.
Dem Bürger wurde zur Rechtslage Folgendes erläutert:
Die rechtliche Grundlage stellt § 26 Thüringer Ordnungsbehördengesetz da, der eine spezialgesetzliche Regelung zu § 25a „Videoüberwachung“ Thüringer Datenschutzgesetz darstellt. Der maßgebliche Absatz 1 hat folgenden Wortlaut:

§ 26
Geltung des Datenschutzgesetzes

(1) Die Ordnungsbehörden können personenbezogene Daten, auch durch Einsatz technischer Mittel zur Anfertigung von Bild- und Tonaufnahmen oder -aufzeichnungen, bei oder im Zusammenhang mit öffentlichen Veranstaltungen und Ansammlungen, die nicht dem Versammlungsgesetz unterliegen, oder zur Erfüllung ihrer sonstigen Aufgaben nur erheben, soweit tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass Gefahren für die öffentliche Sicherheit oder Ordnung entstehen. Die Unterlagen sind spätestens zwei Monate nach Ablauf des auslösenden Ereignisses zu vernichten, soweit sie nicht zur Verfolgung von Straftaten oder Ordnungswidrigkeiten benötigt werden.

Die maßgeblichen Passagen sind unterstrichen.

Öffentliche Sicherheit wird durch § 54 Ordnungsbehördengesetz definiert als die Unverletzlichkeit der Rechtsordnung, der subjektiven Rechte und Rechtsgüter des Einzelnen sowie des Bestandes, der Einrichtungen und Veranstaltungen des Staates oder sonstiger Träger von Hoheitsgewalt.
Die Recherchen des TLfDI ergaben, dass die Kameras an Orten eingesetzt sind, an denen es bereits zu Sachbeschädigungen bzw. im Fall des Teiches zur Gefahr, dass Kinder ins Eis einbrechen können, kam. Bei dem Brunnen der Stadt ging es auch um hygienische Belange, da dort bereits in der Vergangenheit verbotenerweise Hunde hineingelassen wurden und so tatsächliche Anhaltspunkte dafür vorlagen, dass es zu Wiederholungen kommen kann.
Die öffentliche Sicherheit und Ordnung war damit tangiert.

Videoüberwachung kann neben § 25a Thüringer Datenschutzgesetz auch nach § 26 Ordnungsbehördengesetz erfolgen. Es sind strenge Maßstäbe an die Verhältnismäßigkeit anzulegen.

6.13 Videoüberwachung mittels Webcam?

Zu Beginn des Jahres 2016 erreichte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) die Anfrage einer Stadtverwaltung. Hintergrund war die geplante Anschaffung einer „Info-Stele“, in die eine Webcam installiert werden sollte, die Aufzeichnungen auf einen Monitor überträgt (sogenanntes Monitoring), mit dem Ziel diese später für die Erstellung von persönlichen Postkarten zu nutzen. Dabei sollte eine dauerhafte Aufzeichnung stattfinden. Damit sollte Touristen die Möglichkeit offeriert werden, Fotos von sich zu machen und diese als E-Mail oder auch Postkarte zu versenden.
Im Datenschutzrecht gilt ein sogenanntes Verbot mit Erlaubnisvorbehalt. Das bedeutet, dass eine Videoüberwachung grundsätzlich verboten ist, es sei denn, ein spezieller Erlaubnisvorbehalt greift ein. Die Möglichkeit der Einwilligung der betroffenen Personen scheidet bei dieser Konstellation aus, da die „Info-Stele“ auf einem öffentlichen Platz mit einer hohen Besucherzahl aufgestellt werden sollte und eine informierte Einwilligung, wie sie § 4 Abs. 2 und 3 Thüringer Datenschutzgesetz (ThürDSG) vorschreibt, in diesem Falle nicht gewährleistet werden kann.

Den Einsatz von Videoüberwachung regelt für öffentliche Stellen im Freistaat Thüringen § 25a ThürDSG. Nach dieser Bestimmung ist die Videoüberwachung allein zur Wahrung des Hausrechts der verantwortlichen öffentlichen Stelle zulässig, sofern sie für diesen Zweck erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen (siehe hierzu auch den Bericht in der Zeitung „Thüringer Allgemeine“ vom 14. Februar 2017, S. 3, „Sorgen mehr Kameras für mehr Sicherheit?“).
Der Begriff der Videoüberwachung umfasst sowohl die Videobeobachtung, bei der eine Live-Übertragung der Bilder auf einen Monitor erfolgt, als auch die Videoaufzeichnung, bei der die Aufnahmen gespeichert werden. Eine Videoüberwachung liegt – unabhängig von einer möglichen Speicherung oder Aufzeichnung der Bilder – schon bei bloßer Live-Beobachtung mittels optisch-elektronischer Einrichtungen vor, sodass die Vorgaben des § 25a ThürDSG einzuhalten sind. Der Begriff der Beobachtung erfasst auch die digitale Fotografie, sofern eine gewisse zeitliche Dauer zugrunde liegt. Damit unterfällt beispielsweise das Anfertigen von Fotos in kurzen Zeitintervallen ebenfalls dieser Vorschrift.
Der TLfDI erklärte gegenüber der Stadtverwaltung, dass die Verwendung von Webcams nicht grundsätzlich datenschutzrechtlich unzulässig sei. Solange die Webcam-Bilder Personen nicht erkennen ließen, verletze dies keine datenschutzrechtlichen Belange. Gegebenenfalls müsste eine Zoomfunktion so weit zurückgenommen werden, dass ein Personenbezug nicht herzustellen ist. Dies wäre in diesem Falle jedoch nicht zielführend gewesen, da dies ja gerade die verfolgte Intention war (z. B. Postkarten fertigen) und die „Info-Stele“ auch an einem zentralen Platz aufgestellt werden sollte.
Im Übrigen wies der TLfDI noch darauf hin, dass, auch wenn kein Personenbezug hergestellt werden könne, noch am Aufstellungsort der Kamera ein Schild darauf hinweisen müsste, wer die Kamera betreibt und auf welcher Website die Bilder eingesehen werden können.
Die Stadtverwaltung teilte daraufhin dem TLfDI mit, von dem Vorhaben Abstand genommen zu haben.

Aufzeichnungen mittels einer Webcam durch öffentliche Stellen des Freistaates Thüringen unterliegen § 25a Thüringer Datenschutzgesetz (ThürDSG). Danach ist die Videoüberwachung allein zur Wah-

rung des Hausrechts der verantwortlichen öffentlichen Stelle zulässig, sofern sie für diesen Zweck erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Soweit kein Personenbezug durch Webcams herstellbar ist, werden auch keine datenschutzrechtlichen Belange verletzt.

6.14 Videoüberwachung und -aufzeichnung im Stadtgebiet – per Gesetz auch für die Ordnungsbehörde erlaubt

Ein Bürger wandte sich im Berichtszeitraum an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Er hatte der lokalen Zeitung entnommen, dass an bestimmten Punkten der Stadt eine Videoüberwachung des öffentlichen Raumes durch das Ordnungsamt stattfinden würde. Er bat um Mitteilung, welche rechtlichen Grundlagen für die Videoüberwachung in der Stadt Anwendung fänden und warum die Überwachung nicht von der Polizei durchgeführt würde.
Der TLfDI wies auf § 26 Ordnungsbehördengesetz (OBG) hin, der folgenden Wortlaut hat:

„§ 26
Geltung des Datenschutzgesetzes

Das Thüringer Datenschutzgesetz vom 29. Oktober 1991 (GVBl. S. 516) in der jeweils geltenden Fassung gilt mit folgenden Maßgaben:

1. Die Ordnungsbehörden können personenbezogene Daten, auch durch Einsatz technischer Mittel zur Anfertigung von Bild- und Tonaufnahmen oder -aufzeichnungen, bei oder im Zusammenhang mit öffentlichen Veranstaltungen und Ansammlungen, die nicht dem Versammlungsgesetz unterliegen, oder zur Erfüllung ihrer sonstigen Aufgaben nur erheben, soweit tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass Gefahren für die öffentliche Sicherheit oder Ordnung entstehen. Die Unterlagen sind spätestens zwei Monate nach Ablauf des auslösenden Ereignisses zu vernichten, soweit sie nicht zur Verfolgung von Straftaten oder Ordnungswidrigkeiten benötigt werden. […]“

Die für den geschilderten Sachverhalt maßgeblichen Passagen sind unterstrichen.
Die Aufgabe der Ordnungsbehörde ergibt sich aus § 2 Ordnungsbehördengesetz:

„§ 2
Aufgaben der Ordnungsbehörden
(1) Die Ordnungsbehörden haben die Aufgabe, die öffentliche Sicherheit oder Ordnung durch Abwehr von Gefahren und durch Unterbindung und Beseitigung von Störungen aufrechtzuerhalten."
Den Begriff der öffentlichen Sicherheit definiert § 54 Nr. 1 OBG als die Unverletzlichkeit der Rechtsordnung, der subjektiven Rechte und Rechtsgüter des Einzelnen sowie des Bestandes, der Einrichtungen und Veranstaltungen des Staates oder sonstiger Träger von Hoheitsgewalt.
Die Frage, warum hinsichtlich der Abwehr von konkreten Gefahren für die öffentliche Sicherheit und Ordnung nicht die Polizei auf Grundlage des Polizeiaufgabengesetzes (§ 33 Abs. 2 Nr. 1 Polizeiaufgabengesetz) tätig werden würde, konnte der TLfDI unter Hinweis auf § 3 Abs. 1 OBG beantworten, wonach Maßnahmen der Ordnungsbehörden Vorrang gegenüber Maßnahmen der Polizei haben.

Bei tatsächlichen Anhaltspunkten für Gefahren für die Sicherheit und Ordnung und damit erst recht bei Verstößen hiergegen kann eine Videoüberwachung auch nach § 26 Ordnungsbehördengesetz erfolgen. Zuständige Behörde hierfür ist gem. § 3 Ordnungsbehördengesetz das Ordnungsamt, vorrangig vor der Polizei.

6.15 Abwahl eines Bürgermeisters nach § 28 Absatz 6 ThürKO – Transparenz versus Schutz personenbezogener Daten

Im Berichtszeitraum erreichte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) eine Beschwerde eines Bürgermeisters einer Gemeinde aus dem Landkreis Weimarer Land. Dieser berichtete dem TLfDI Folgendes: Im Herbst 2015 hatten drei Ratsherren einen Antrag gem. § 28 Abs. 6 Satz 4 Thüringer Kommunalordnung (ThürKO) in den Gemeinderat eingebracht, der den Beschlussvorschlag enthielt, den Bürgermeister der Gemeinde abzuwählen. Die drei Ratsherren begründeten ihren Antrag in der öffentlichen Gemeinderatssitzung im Dezember 2015 unter anderem damit, dass der Bürgermeister unentgeltlich Gemeindevermögen an Familienangehörige weitergegeben, vergaberechtliche Grundsätze missachtet und die Abwasserproblematik über Jahre verschleppt habe. Da der Bürgermeister, gegen den sich die genann-

ten und weitere Vorwürfe richteten, in der besagten Gemeinderatsitzung nicht anwesend war, gab ihm der Gemeinderat Gelegenheit, sich zu seinen behaupteten Verfehlungen bis Mitte Januar 2016 zu äußern.
Mit Schreiben vom Mitte Januar 2016 nahm der Bürgermeister Stellung zu den behaupteten Fehlern seiner Amtszeit. Dabei nannte der Bürgermeister auch die Namen eines Landwirts sowie zweier Gemeinderatsmitglieder und machte ferner Ausführungen zu der beruflichen Tätigkeit eines Gemeinderatsmitglieds, der den Abwahlantrag gegen ihn – den Bürgermeister – maßgeblich initiiert hatte.
In seiner öffentlichen Sitzung Anfang Februar 2016 beriet der Gemeinderat den Antrag zur Abwahl des Bürgermeisters gem. § 28 Abs. 6 Satz 4 ThürKO erneut. In der Niederschrift zur Gemeinderatssitzung heißt es dazu: „*Die Stellungnahme des Bürgermeisters wird verlesen. Es folgen einige Anmerkungen der GR-Mitglieder* [Anm: gemeint sind die Mitglieder des Gemeinderates] *zu den einzelnen Darstellungen.*“
In der darauf folgenden Sitzung Mitte Februar 2016 beschloss der Gemeinderat dann ebenfalls in öffentlicher Sitzung mit Mehrheit die Einleitung eines Verfahrens zur Abwahl des Bürgermeisters nach § 28 Abs. 6 Satz 4 ThürKO.
Vom TLfDI zu einer Stellungnahme aufgefordert, warum die streitgegenständlichen Beratungen des Gemeinderats zum Abwahlantrag nicht in nichtöffentlicher Sitzung gem. § 40 Abs. 1 Satz 2 ThürKO erfolgten, teilte die für die Gemeinde zuständige Verwaltungsgemeinschaft (VG) mit, dass es für die Gemeindebürger von grundlegender Bedeutung sei, warum der Antrag zur Abwahl ihres Bürgermeisters gestellt wurde. Zur Begründung ihrer Rechtsauffassung verwies die VG auf die Kommentierung des § 28 ThürKO von Wachsmuth/Oehler. Dort heißt es unter der Gliederungsnummer 6.1.1: „*Über den Antrag ist grundsätzlich in öffentlicher Sitzung zu beraten, auch dann, wenn persönliche Angelegenheiten des Bürgermeisters behandelt werden, die mit seinem Wahlamt in Verbindung stehen. Für die Gemeindebürger, die über die Abwahl zu entscheiden haben, ist von Bedeutung, warum vom Gemeinderat ein solcher Antrag gestellt wird. Bei diesen Angelegenheiten besteht kein berechtigtes Interesse des betroffenen Bürgermeisters, die Öffentlichkeit von der Sitzung auszuschließen. Nur in Einzelfällen, bei privaten Angelegenheiten, die sein Amt als Bürgermeister nicht berühren und die darauf auch keinen Einfluss haben, können ggf. schutzwürdige*

Interessen des Bürgermeisters vorliegen, die den Ausschluss bzw. teilweisen Ausschluss der Öffentlichkeit rechtfertigen."
Daraufhin wies der TLfDI die zuständige VG auf die der Kommentierung von Wachsmuth/Oehler entgegen stehenden Rechtsauffassungen von Uckel/Hauth/Hoffmann, Kommunalrecht in Thüringen, Loseblattsammlung, 58. Lieferung, Stand August 2012, Nr. 10.2 zu § 28 ThürKO sowie Rücker/Dieter/Schmidt, Kommunalverfassungsrecht Thüringen, Band 1, Stand: 30. Nachlieferung, März 2015, § 28, Nr. 21 hin. Danach werde die Beratung über einen Abwahlantrag des Bürgermeisters *„regelmäßig […] unter Ausschluss der Öffentlichkeit (§ 40 Abs. 1 ThürKO) stattfinden, jedenfalls dann, wenn Anlass des Antrags die behaupteten Verfehlungen des Bürgermeisters sind."*
Ferner bat der TLfDI die VG um Stellungnahme zu dem behaupteten Fehlverhalten des Bürgermeisters in rechtlicher und tatsächlicher Hinsicht und forderte die VG auf, die von ihr vorgenommene Abwägung der Rechtspositionen der Bürger und des Bürgermeisters zu begründen.
In ihrem weiteren Schreiben an den TLfDI lehnte die VG die Rechtsauffassung der vom TLfDI genannten Kommentar-Fundstellen, die eine nicht-öffentliche Sitzung für die Beratung des Abwahlantrags gem. § 28 Abs. 6 ThürKO bei behaupteten Verfehlungen des Bürgermeisters präferieren, im Ergebnis als zu kurz greifend ab.
Die Frage, ob bei einer öffentlichen Beratung des Abwahlantrags hier entgegenstehende Interessen Einzelner zu berücksichtigen waren, verneinte die VG gegenüber dem TLfDI unter Hinweis darauf, dass ein Bürgermeister als Organ der Gemeinde keine berechtigten Einzelinteressen im Sinne von § 40 Abs. 1 ThürKO geltend machen könnte. Davon zu unterscheiden seien Fälle, in denen der Bürgermeister entweder als reine Privatperson handeln würde (z. B. Rasenmähen auf seinem privaten Grundstück oder Erledigung des häuslichen Einkaufs) oder als Privatperson im Zusammenhang mit der Ausübung seines Wahlamtes (z. B. Fahrt zu einem gemeindlichen Termin und dabei Missachtung der Straßenverkehrsordnung). Nur in den letztgenannten beiden Fallkonstellationen sei – so die VG – ein Ausschluss der Öffentlichkeit für die Dauer der Beratung des Abwahlantrages gem. § 28 Abs. 6 ThürKO gerechtfertigt.
Andere berechtigte Interessen Einzelner, insbesondere von Dritten, die hier eine Ausnahme von dem Grundsatz der öffentlichen Sitzung gem. § 40 Abs. 1 Satz 1 ThürKO rechtfertigten, prüfte die VG hin-

gegen nicht. Sie vertrat deshalb die Rechtsauffassung, dass die von den Antragstellern des Abwahlantrags ins Feld geführten Vorwürfe gegen den Bürgermeister keine Verfehlungen im Sinne der Kommentierungen von Uckel/Hauth/Hoffmann oder Rücker/Dieter/Schmidt seien und daher die Beratung des Abwahlantrags in öffentlicher Sitzung habe stattfinden können.
Bei der Abwägung der widerstreitenden Interessen seien im Ergebnis die Interessen der Bürger, die über die Abwahl des Bürgermeisters zu entscheiden hätten und daher Kenntnis über die Einleitung des Verfahrens erlangen müssen, höher zu gewichten.
Der TLfDI beanstandete nach intensiver datenschutzrechtlicher Prüfung das Vorgehen der Gemeinde in Form der öffentlichen Beratung des Abwahlantrags gegen ihren Bürgermeister aus folgenden Gründen und am Maßstab von § 40 Abs. 1 Satz 1 und § 28 Abs. 6 ThürKO:
Erstens: Der stellvertretende Bürgermeister als Sitzungsleiter bzw. der Gemeinderat hätten zu Beginn der Beratung des Abwahlantrags nach § 28 Abs. 6 Satz 4 ThürKO im öffentlichen Teil der Gemeinderatssitzung am 2. Februar 2016 zunächst erkennen müssen, dass hier personenbezogene Daten von Dritten tangiert waren. Denn der Bürgermeister der Gemeinde nannte in seinem Schreiben von Mitte Januar 2016 mehrere Namen von dritten Personen. Dabei handelte es sich um personenbezogene Daten im Sinne von § 3 Abs. 1 ThürDSG. Insbesondere zum Vorwurf der unentgeltlichen Weitergabe von Gemeindevermögen an Familienangehörige nannte der Bürgermeister zwei Namen dritter Personen. Zum Vorwurf der Missachtung vergaberechtlicher Grundsätze nannte der Bürgermeister ebenfalls den Namen einer dritten Person. Zum Vorwurf der verschleppten Abwasserproblematik nannte der Bürgermeister in seinem Schreiben von Mitte Januar 2016 die Namen von zwei weiteren dritten Personen.
Zweitens: Gem. § 4 Abs. 1 ThürDSG ist die Verarbeitung personenbezogener Daten (worunter auch die Bekanntgabe als Unterform der Übermittlung – § 3 Abs. 3 Nr. 4 ThürDSG – fällt) nur zulässig, wenn das ThürDSG selbst oder eine andere Rechtsgrundlage sie erlaubt oder soweit der Betroffene eingewilligt hat.
Die Nennung all dieser Namen als personenbezogene Daten hätte im vorliegenden Fall nicht in öffentlicher Sitzung gem. § 40 Abs. 1 Satz 1 ThürKO erfolgen dürfen. Denn die Namen der betroffenen Personen wurden entweder im Zusammenhang mit Grundstücksan-

gelegenheiten oder zwecks Entlastung des Bürgermeisters gegen die ihn betreffenden Vorwürfe und damit im Zusammenhang mit seiner eigenen Personalangelegenheit genannt. Sowohl Grundstücks- als auch Personalangelegenheiten stellen nach einhelliger Literaturansicht **berechtigte Interessen Einzelner** dar, die eine Ausnahme vom Grundsatz der Öffentlichkeit von Ratssitzungen gem. § 40 Abs. 1 Satz 1 ThürKO rechtfertigen (so *Rücker/Dieter/Schmidt,* Kommunalverfassungsrecht Thüringen, Band 1, Stand: 30. Nachlieferung, März 2015, § 40, Nr. 2.4; *Uckel/Hauth/Hoffmann*, Kommunalrecht in Thüringen, Loseblattsammlung, 58. Lieferung, Stand August 2012, Nr. 2 zu § 40 ThürKO).

Insbesondere für den hier vorliegenden Ausnahmegrund der Personalangelegenheit war ferner zu berücksichtigen, dass auch nach dem Vortrag des Bürgermeisters nicht klar war, ob die von ihm schriftlich benannten Personen als „Zeugen" in dem Sinne zu begreifen waren, dass sie den Sachverhalt aus der Sicht des Bürgermeisters gestützt hätten. Da ferner auch nicht klar erkennbar war, ob die vom Bürgermeister benannten Personen in die Nennung ihres Namens durch den Bürgermeister eingewilligt hatten, galt daher umso mehr, dass ihre Namensnennung allenfalls in nicht-öffentlicher Sitzung des Gemeinderates hätte erfolgen dürfen.

Drittens: Entgegen der Rechtsauffassung der zuständigen VG hatte auch der Bürgermeister im konkreten Fall ein berechtigtes Interesse gem. § 40 Abs. 1 Satz 1 ThürKO, dass der genannte Abwahlantrag, der sich gegen ihn direkt als Bürgermeister richtete, im nicht-öffentlichen Teil der Gemeinderatssitzung von Anfang Februar 2016 hätte beraten werden müssen. Das berechtigte Interesse des Bürgermeisters, den gegen ihn gerichteten Abwahlantrag im nichtöffentlichen Teil der Gemeinderatssitzungen beraten zu lassen, ergab sich im vorliegenden Fall daraus, dass die gegen ihn vorgebrachten Verfehlungen allesamt nur behauptet, aber nicht bewiesen waren.

Viertens: Dem berechtigten Interesse des Bürgermeisters, dass der gegen ihn gerichtete Abwahlantrag im nicht-öffentlichen Teil der Gemeinderatssitzung Anfang Februar 2016 hätten beraten werden müssen, stand zum Zeitpunkt der Sitzung des Gemeinderates auch kein höher wiegendes berechtigtes Informationsinteresse der Bürger von der Gemeinde an der Einleitung eines Abwahlverfahrens entgegen.

Diese Rechtsauffassung ergab sich für den TLfDI aus der Auslegung des § 28 Abs. 6 Satz 4 ThürKO nach seinem Sinn und Zweck. Denn

diese Norm wies zum damaligen Zeitpunkt allein dem Gemeinderat die Funktion des „Anstoßgebers“ für ein Abwahlverfahren zu (zur neu geschaffenen Abwahl des Bürgermeisters durch ein Bürgerbegehren siehe § 11 Abs. 2 und § 14 Abs. 3 Thüringer Gesetz über das Verfahren bei Einwohnerantrag, Bürgerbegehren und Bürgerentscheid vom 7. Oktober 2016). Ausschließlich der Gemeinderat konnte somit die Abwahl eines Bürgermeisters einleiten, während die Gemeindebürger damals selbst keine Möglichkeit besaßen, ein solches Verfahren zu initiieren – auch nicht durch Bürgerbegehren und Bürgerentscheid (siehe dazu *Uckel/Hauth/Hoffmann*, a.a.O. zu § 28 ThürKO, Nr. 10.2). Die Mitglieder des Gemeinderats haben dabei gem. § 24 Abs. 1 Satz 1 ThürKO ihr Ehrenamt nach dem Gesetz und ihrer freien, dem Gemeinwohl verpflichteten Überzeugung auszuüben. Demzufolge hatten die Gemeinderatsmitglieder bei der Beratung eines Abwahlantrages alle **ent- und belastenden Argumente**, die gegen oder für die Abwahl eines Bürgermeisters sprechen, zu gewichten und zu würdigen.

Diese Gewichtung der Argumente für und gegen einen Abwahlantrag kann aber nur dann gelingen, wenn die Willensbildung in einer objektiven und unbefangenen Diskussionsatmosphäre möglich ist. In dieser Willensbildungsphase des Gemeinderats sind daher Sympathiebekundungen, Unterstützungshandlungen verbaler oder nonverbaler Natur, Einflussnahmen oder gar Druckmittel von Dritten für die Herbeiführung einer objektiven Entscheidung unzuträglich.

Ferner wissen die Bürger zum Zeitpunkt der Beratung des Gemeinderates über den Abwahlantrag des Bürgermeisters noch gar nicht, ob es überhaupt zu dem weiteren Abwahlverfahren gegen den Bürgermeister kommen wird, da die Entscheidungsfindung ja erst Gegenstand der Beratung des Gemeinderates über den Abwahlantrag ist und ferner die Entscheidung des Gemeinderates über den Abwahlantrag gem. § 28 Abs. 6 Satz 5 ThürKO erst in einer weiteren Sitzung zu treffen ist.

Deshalb war nach Auffassung des TLfDI bei der Beratung des Gemeinderates über den Abwahlantrag gegen den Bürgermeister dann das berechtigte Interesse des Bürgermeisters nach § 40 Abs. 1 Satz 1 ThürKO höher zu gewichten als das Informationsinteresse der Bürger der Gemeinde zu erfahren, ob es zum weiteren Abwahlverfahren gegen den Bürgermeister kommt, wenn konkrete Verfehlungen des Bürgermeisters im Raum stehen bzw. behauptet werden.

Fünftens: Da, wie unter Drittens und Viertens dargestellt, berechtigte Interessen Einzelner gem. § 40 Abs. 1 Satz 1 ThürKO im konkreten Streitfall vorgelegen hatten, hätte der Gemeinderat gem. § 40 Abs. 1 Satz 2 ThürKO über den Ausschluss der Öffentlichkeit in nicht-öffentlicher Sitzung beraten und entscheiden müssen. Diese Obliegenheit zu erkennen und für die erforderlichen Verfahrensschritte zu sorgen, wäre zuallererst Aufgabe des stellvertretenden Bürgermeisters der Gemeinde gewesen (vgl. dazu *Uckel/Hauth/Hoffmann*, a.a.O., Nr. 3 zu § 40 ThürKO), dem laut Niederschrift zur Gemeinderatssitzung Anfang Februar 2016 die Sitzungsleitung oblag.
Da im Ergebnis keine Rechtsgrundlage für die Nennung der personenbezogenen Daten in der öffentlichen Sitzung des Gemeinderates gegeben war, und darüber hinaus auch keine Einwilligungen der Betroffenen zur Übermittlung ihrer personenbezogenen Daten vorlagen, war dieser datenschutzrechtliche Verstoß vom TLfDI gem. § 39 Abs. 1 ThürDSG zu beanstanden.

Ist ein Abwahlantrag gegen einen Bürgermeister gem. § 28 Abs. 6 ThürKO im Rahmen einer öffentlichen Sitzung des Gemeinderats nach § 40 Abs. 1 Satz 1 ThürKO zu beraten oder -sprechen berechtigte Interessen des „angegriffenen“ Bürgermeisters und ggf. dritter Personen für einen Ausschluss der Öffentlichkeit aus der Sitzung des Gemeinderats?
Die systematischen Argumente plädieren für eine saubere Unterscheidung der Kompetenzen und Rechte von Gemeinderat und Gemeindebürgern im Fall eines Abwahlantrages gegen einen Bürgermeister aufgrund mutmaßlicher konkreter Verfehlungen: Im ersten Schritt berät der Gemeinderat in nicht-öffentlicher Sitzung über den Abwahlantrag. Nach der Entscheidung und dem Beschluss des Gemeinderates, ein Abwahlverfahren gegen den Bürgermeister durchzuführen, haben dann die Bürger der Gemeinde die Möglichkeit, im Verfahren gem. § 28 Abs. 6 Satz 1 bis 3 in Verbindung mit § 17 ThürKO die Abwahl des Bürgermeisters herbeizuführen oder nicht. In dieser Phase ist es dann auch nicht nur legitim, sondern für eine demokratische Willensbildung geradezu erforderlich, wenn die Mitglieder des Gemeinderates, die für den Abwahlantrag gestimmt haben, ihre Gründe für die Unterstützung des Antrags im datenschutzrechtlich gebotenen Rahmen in der Öffentlichkeit mitteilen.

6.16 Schwachstelle Internet: Veröffentlichung personenbezogener Daten in Amtsblättern eines Landkreises

Eine Beschwerdeführerin teilte dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) mit, dass ein Landratsamt ihrer Bitte, ihre personenbezogenen Daten, insbesondere im Zusammenhang mit ihrer Kandidatur zur Kommunalwahl im Jahre 2014, auf der Internetseite des Landratsamtes zu entfernen, nur unvollständig nachgekommen sei. Bisher seien lediglich ihre personenbezogenen Daten aus einem im Internet veröffentlichten Amtsblatt entfernt worden. Unerledigt geblieben sei hingen die Datenlöschung zu fünf weiteren Amtsblättern.
Daraufhin teilte der TLfDI dem betreffenden Landratsamt seine rechtliche Bewertung der Angelegenheit wie folgt mit:
Durch die o. g. Internetveröffentlichung besteht die Gefahr, dass die Betroffene in unzulässiger Weise in ihrem Recht auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 Grundgesetz und Art. 6 Abs. 2 Thüringer Verfassung verletzt wird. Das Erheben, Verarbeiten – das auch die Datenübermittlung umfasst – und das Nutzen von personenbezogenen Daten ist nach § 4 Abs. 1 ThürDSG grundsätzlich unzulässig, es sei denn, es gibt eine Erlaubnisnorm in oder außerhalb des Thüringer Datenschutzgesetzes (ThürDSG) oder der Betroffene hat in den Vorgang eingewilligt (sogenanntes Verbot mit Erlaubnisvorbehalt). Bei einer Internetpublikation personenbezogener Daten handelt es sich um eine Datenübermittlung auch an Drittstaaten im Sinne von § 23 Abs. 2 ThürDSG, in denen kein angemessenes Datenschutzniveau gewährleistet ist. Eine solche Datenübermittlung ist nur zulässig, wenn der Betroffene hierin einwilligt und sie zur Aufgabenwahrnehmung der öffentlichen Stelle erforderlich ist (vgl. hierzu den Beitrag 5.2 im 9. Tätigkeitsbericht des TLfDI).
Der TLfDI forderte das Landratsamt auf, die personenbezogenen Daten der Beschwerdeführerin aus den auf seiner Internetseite gespeicherten Amtsblättern vollständig zu entfernen.
Nachfolgend kam das Landratsamt den Forderungen des TLfDI nach und löschte sämtliche personenbezogenen Daten der Beschwerdeführerin auf seiner Internetseite.

Immer wieder gibt es Datenschutzverstöße infolge der Veröffentlichung von personenbezogenen Daten im Internet. Auch dieser Fall

zeigt, dass es weiterhin erheblichen datenschutzrechtlichen Informationsbedarf in der Thüringer Verwaltung gibt.

6.17 Biene Maja oder Captain Chaos? – Anzeige von Namen auf elektronischer Anzeigetafel

Bereits im letzten Tätigkeitsbericht hatte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) unter Gliederungspunkt 5.38 darüber berichtet, dass die elektronische Anzeigetafel im Bürgerservice der Stadt Jena die Namen von Bürgern sichtbar anzeigt. Diese Namen konnten in Folge auch von den anderen im Bürgerservice Wartenden wahrgenommen werden.
Die Stadt Jena hatte den TLfDI dazu auf Nachfrage informiert, dass die elektronische Anzeigetafel nur die Namen der Bürger anzeige, die elektronisch einen Termin vereinbart hätten. Bereits bei der Buchung eines Online-Termins werde der Nutzer mit folgendem Satz auf die Verfahrensweise beim Aufruf über die Anzeigetafel informiert: „Tragen Sie zur Bestätigung Ihren Familiennamen (Achtung: Dieser wird später am Bildschirm der Aufrufanlage des Bürgerservice angezeigt) […] ein.“ Welchen Namen der Nutzer schlussendlich eingebe, bleibe dem Bürger dabei aber selbst überlassen. So sei es nach Angabe der Stadt schon vorgekommen, dass auf der Anzeigetafel im Bürgerservice die vom Bürger selbst gewählten Fantasienamen „Biene Maja“ oder „Captain Chaos“ erschienen seien.
Da es nach Einschätzung durch den TLfDI im Sinne von § 1 Abs. 2 Satz 1 (Datensparsamkeit) Thüringer Datenschutzgesetz (ThürDSG) nicht erforderlich war, den Familiennamen (wie jedoch grundsätzlich vom Bürgerservice gefordert [s. o. im Text}) anzugeben, wurde der Stadt seitens des TLfDI empfohlen, den Hinweistext für die Online-Terminvereinbarenden entsprechend zu ergänzen und auch auf die Dauer der Namensanzeige an der Anzeigetafel hinzuweisen.
Der Empfehlung des TLfDI folgte die Stadt in Gänze. Bei Aufruf der Bürger, die online einen Termin vereinbart haben, erscheint nunmehr auf der Anzeigetafel: „Tragen Sie zur Bestätigung einen NAMEN (Achtung: Dieser wird später am Bildschirm der Aufrufanlage des Bürgerservice angezeigt. Die Anzeigedauer erstreckt sich bis zum Aufruf des zehntnächsten Kunden) und Ihre E-Mail-Adresse ein! Anschließend erhalten Sie eine E-Mail mit dem Aktivierungs-Link.“
Die Angelegenheit ist für den TLfDI damit erledigt.

Gegebenenfalls sehen es eine Vielzahl der Betroffenen als datenschutzrechtlich unbedenklich an, dass der eigene Familienname bei Aufruf an einer Anzeigetafel erscheint.
Die Verarbeitung und Nutzung personenbezogener Daten hat sich gemäß § 1 Abs. 2 Satz 1 (ThürDSG) aber an dem Ziel auszurichten, so wenig wie möglich personenbezogene Daten zu verarbeiten und zu nutzen (Prinzip der Datensparsamkeit). Dem § 1 Abs. 2 ThürDSG wurde hier Genüge getan.

6.18 Fotosafari im Schlafzimmer – Folge 2

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) hatte in seinem 11. Tätigkeitsbericht für den öffentlichen Bereich unter dem Gliederungspunkt 5.44, S. 138 bis 140, zu dieser Beschwerdeangelegenheit u. a. berichtet, ein Mitarbeiter einer Waffenbehörde habe dem Leiter des Hegerings (einer Organisationseinheit der Jägerschaft), dem auch der Beschwerdeführer angehörte, Einzelheiten zu einer Hausdurchsuchung beim Beschwerdeführer mitgeteilt. Zudem sei dem Leiter des Hegerings die Verwaltungsakte des Beschwerdeführers mit bei der Hausdurchsuchung gemachten Fotos gezeigt worden. Nachfolgend stellte der TLfDI einen Strafantrag gegen Unbekannt gemäß § 43 Abs. 3 Thüringer Datenschutzgesetz (ThürDSG). Zum Ende des Berichtszeitraums 2014/2015 war das staatsanwaltliche Ermittlungsverfahren noch nicht abgeschlossen.
Anfang 2017 teilte die ermittelnde Staatsanwaltschaft auf Nachfrage des TLfDI u. a. mit, dass die zunächst gegen Unbekannt geführten Ermittlungen einen Anfangsverdacht gegen eine konkrete Person wegen Verstoßes gegen das ThürDSG erbracht hätten. Das Ermittlungsverfahren sei jedoch zwischenzeitlich gemäß § 154 Abs. 1 Strafprozessordnung (StPO) eingestellt worden Nach § 154 Abs. 1 StPO kann die Staatsanwaltschaft von der Verfolgung einer Tat absehen, wenn die Strafe oder die Maßregel der Besserung und Sicherung, zu der die Verfolgung führen kann, neben einer Strafe oder Maßregel der Besserung und Sicherung, die gegen den Beschuldigten wegen einer anderen Tat rechtskräftig verhängt worden ist oder die er wegen einer anderen Tat zu erwarten hat, nicht beträchtlich ins Gewicht fällt.
Die ermittelnde Staatsanwaltschaft führte u. a. aus, dass im Zuge der Ermittlungen der Verdacht gegen einen oder mehrere Bedienstete

des Landratsamtes nicht erhärtet werden konnte. Jedoch sei ein Polizeibeamter, der der Polizeiinspektion angehörte, die an der Hausdurchsuchung beteiligt war, in den Verdacht geraten, Lichtbilder der Hausdurchsuchung beim Beschwerdeführer auf seinem Mobiltelefon im Bekanntenkreis gezeigt zu haben. Bei zusammenfassender Würdigung der bisherigen Ermittlungen bestanden Anhaltspunkte dafür, dass der Beschuldigte Lichtbilder, die im Zuge der ordnungsbehördlichen Kontrolle beim Beschwerdeführer gefertigt wurden, verfahrensfremden Personen gezeigt hatte. Ein Nachweis dahingehend, dass der o. g. Polizeibeamte in der Absicht gehandelt hatte, einen anderen im Sinne von § 43 Abs. 3 ThürDSG zu schädigen, sei aber nicht zu führen gewesen.
Da gegen den betreffenden Polizeibeamten aber in einem anderen Strafverfahren Anklage erhoben wurde, habe die Staatsanwaltschaft im Ergebnis von einer Verfolgung der Straftat, die der TLfDI beantragt hatte, nach § 154 Abs. 1 StPO abgesehen.
Der TLfDI hat angesichts seiner begrenzten rechtlichen Befugnisse zur Ermittlung des tatsächlichen Geschehens von einer Weiterbearbeitung der Angelegenheit abgesehen.

Zwar erbrachten die Ermittlungen der Staatsanwaltschaft Anhaltspunkte dafür, dass ein Polizist Lichtbilder, die im Zuge einer ordnungsbehördlichen Kontrolle beim Beschwerdeführer gefertigt wurden, verfahrensfremden Personen gezeigt hatte. Ein Nachweis dahingehend, dass der o. g. Polizist in der Absicht gehandelt hatte, einen anderen im Sinne von § 43 Abs. 3 ThürDSG zu schädigen, ist nach Auffassung der ermittelnden Staatsanwaltschaft jedoch nicht zu führen gewesen. Letztendlich stellte die Staatsanwaltschaft das Ermittlungsverfahren ein.

6.19 Was darf die Meldebehörde nach dem Bundesmeldegesetz?

Ein Bürger wandte sich im Berichtszeitraum an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und bat – vorbeugend – um datenschutzrechtliche Einschätzung eines Widerspruchs gegen die Weitergabe von Daten durch die Meldebehörde. Insbesondere wollte er wissen, gegen welche Datenweitergabe kein Widerspruch möglich sei und was es mit dem Widerspruchsrecht gegen die Weitergabe von Daten an die ehemalige

GEZ (Gebühreneinzugszentrale, jetzt Bürgerservice ARD und ZDF) auf sich habe.
Der TLfDI hat dem Anfragenden Folgendes mitgeteilt:
Dem TLfDI obliegt nach § 37 Abs. 1 Thüringer Datenschutzgesetz auch die Kontrolle der Thüringer Meldebehörden. Diese dürfen nur innerhalb des gesetzlich vorgegebenen Rahmens, also des Bundesmeldegesetzes (BMG), die personenbezogenen Daten der Betroffenen verarbeiten und nutzen.
Die Meldebehörde darf zum Beispiel gemäß § 44 Abs. 1 BMG (siehe dazu: https://www.gesetze-im-internet.de/bmg/) einer Person auf Verlangen Auskunft (einfache Melderegisterauskunft) zu einer anderen bestimmten Person hinsichtlich folgender Daten erteilen: Familienname, Vornamen, Doktorgrad und derzeitige Anschriften sowie, sofern die Person verstorben ist, diese Tatsache.



Gemäß § 49 Abs. 2 BMG können seitens der Meldebehörde einfache Melderegisterauskünfte auch durch einen automatisierten Abruf über das Internet erteilt werden. Die Erteilung dieser einfachen Melderegisterauskunft ist nur zulässig, wenn die Identität der Person, über die eine Auskunft begehrt wird, aufgrund der in der Anfrage mitgeteilten Angaben über den Familiennamen, den früheren Namen, die Vornamen, das Geburtsdatum, das Geschlecht oder eine Anschrift eindeutig festgestellt werden kann und die Auskunft verlangende Person oder Stelle erklärt, die Daten nicht für Zwecke der Werbung oder des Adresshandels zu verwenden (§ 44 Abs. 3 BMG). Vom Grundsatz kann die Meldebehörde also jedermann, der über die genannten, zur Identitätsbestimmung der Person erforderlichen Daten verfügt, eine derartige Melderegisterauskunft durch einen automatisierten Abruf über das Internet erteilen.
Gemäß § 50 Abs. 1 BMG (Melderegisterauskünfte in besonderen Fällen) darf die Meldebehörde auch Parteien, Wählergruppen und anderen Trägern von Wahlvorschlägen im Zusammenhang mit Wahlen und Abstimmungen auf staatlicher und kommunaler Ebene in den sechs der Wahl oder Abstimmung vorangehenden Monaten Auskunft aus dem Melderegister über die in § 44 Abs. 1 Satz 1 BMG bezeichneten Daten (Familienname, Vornamen, Doktorgrad und derzeitige Anschriften sowie, sofern die Person verstorben ist, diese Tatsache) von Gruppen von Wahlberechtigten erteilen, soweit für

deren Zusammensetzung das Lebensalter bestimmend ist. Verlangen Mandatsträger, Presse oder Rundfunk Auskunft aus dem Melderegister über Alters- oder Ehejubiläen von Einwohnern, darf die Meldebehörde gemäß § 50 Abs. 2 BMG Auskunft erteilen über Familienname, Vornamen, Doktorgrad, Anschrift sowie Datum und Art des Jubiläums. Altersjubiläen sind in diesem Sinne der 70. Geburtstag, jeder fünfte weitere Geburtstag und ab dem 100. Geburtstag jeder folgende Geburtstag; Ehejubiläen sind das 50. und jedes folgende Ehejubiläum.

Adressbuchverlagen darf gemäß § 50 Abs. 3 BMG zu allen Einwohnern, die das 18. Lebensjahr vollendet haben, Auskunft erteilt werden über deren Familienname, Vornamen, Doktorgrad und derzeitige Anschriften.

Die betroffene Person hat allerdings das Recht, dieser Übermittlung der Daten nach § 50 Abs. 1 bis 3 BMG (siehe oben: Auskunft an Parteien, Mandatsträger, Presse, Rundfunk, Adressbuchverlage) gemäß § 50 Abs. 5 BMG zu widersprechen. Der TLfDI hat auf seiner Internetseite ein entsprechendes Formblatt „Widerspruch gegen Datenübermittlung aus Melderegister“ zur Verfügung gestellt (https://www.tlfdi.de/imperia/md/content/datenschutz/themen/mustervordrucke/anlage_widerspruch_gegen_datenuebermittlung.pdf).

Darüber hinaus gibt es eine Vielzahl von Datenübermittlungen (z. B. Datenübermittlungen an andere öffentliche Stellen gemäß § 34 BMG), denen der Betroffene nicht widersprechen kann. Auch soweit ein betroffener Bürger Kritik an dem Verfahren übt, dass der Beitragsservice ARD und ZDF (früher die GEZ) zwecks Gebührenbeitreibung die Daten der Meldeämter verarbeiten darf, muss der TLfDI auf den Beschluss des Oberverwaltungsgerichts Lüneburg verweisen (Az. 4 ME 204/13). Darin haben die Richter festgestellt, dass der durch den Beitragsservice vorgenommene Abgleich der Melderegisterdaten mit dem beim Beitragsservice vorhandenen Datenbestand auf Grundlage des Rundfunkbeitragsstaatsvertrags erforderlich ist und damit keinen Verstoß gegen das Grundrecht auf informationelle Selbstbestimmung darstellt. Ein Widerspruch gegen diesen Datenabgleich mit dem Beitragsservice (wegen Rundfunk- und Fernsehbeiträgen) ist deshalb nicht erfolgversprechend.

Die Möglichkeiten des Widerspruchs einer Weitergabe von personenbezogenen Daten aus dem Melderegister an verschiedene Empfänger (§ 50 Abs. 5 BMG) sollte man im Interesse des informationellen Selbstbestimmungsrechtes nutzen. Der anfragende und informierte Bürger wird dies nach Einschätzung des TLfDI tun. Dennoch enthält das BMG in den §§ 44 ff. BMG einige Regelungen bereit, die Bürgern, Parteien, Mandatsträgern, Pressevertretern oder Adressbuchverlagen unter bestimmten Voraussetzungen Auskünfte aus dem Melderegister gewähren.

6.20 Keine Auskunft vom Einwohnermeldeamt: ein Missverständnis

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) wurde im Berichtszeitraum von einem Jenaer Bürger um Unterstützung gebeten: Nach seinen Angaben hatte er sich an das Einwohnermeldeamt Jena (Fachdienst Bürger- & Familienservice) und zeitgleich an den Beitragsservice von ARD, ZDF und Deutschlandradio mit der Bitte um Auskunft zu seinen personenbezogenen Daten gewandt, der aber von keiner der genannten Stellen entsprochen worden sei. Sein Auskunftsbegehren hatte der Beschwerdeführer auf § 19 Bundesdatenschutzgesetz (BDSG) gestützt.
Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) kontrolliert gemäß § 37 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) i. V. m. § 2 ThürDSG die öffentlichen Stellen in Thüringen, also auch das Einwohnermeldeamt Jena. Nach § 13 Abs. 1 ThürDSG hat jede Daten verarbeitende Stelle dem Betroffenen auf Antrag ohne zumutbare Verzögerung Auskunft zu erteilen über die zu seiner Person verarbeiteten Daten, den Zweck und die Rechtsgrundlage der Verarbeitung sowie die Herkunft der Daten und deren Empfänger oder die Kategorien der Empfänger, soweit diese Angaben gespeichert sind. Wird dem Betroffenen keine Auskunft erteilt, so ist die Auskunft auf Verlangen des Betroffenen dem Landesbeauftragten für den Datenschutz zu erteilen, soweit nicht das zuständige Landesministerium im Einzelfall feststellt, dass dadurch die Sicherheit des Bundes oder eines Landes gefährdet würde (§ 13 Abs. 7 ThürDSG).
Der TLfDI bat im geschilderten Fall das Einwohnermeldeamt um Stellungnahme zur Angelegenheit, insbesondere um Mitteilung, auf

welcher Rechtgrundlage dem Auskunftsersuchen des Betroffenen nicht entsprochen worden war. Nach Auffassung des TLfDI konnte jedenfalls eine vom Bürger falsch benannte Rechtsgrundlage für sein Auskunftsbegehren nicht zur Verweigerung jedweder Auskunft/Antwort an den Betroffenen führen.
Das Antwortschreiben des Einwohnermeldeamtes erreichte den TLfDI kurzfristig. Nach Angaben der Stadtverwaltung Jena/Fachdienst Bürger- und Familienservice handelte es sich im vorliegenden Fall um ein Versehen der Stadtverwaltung bzw. um ein Missverständnis. Die Stadtverwaltung teilte weiterhin mit, dass der Beschwerdeführer selbstverständlich die Auskunft über seine beim Einwohnermeldeamt gespeicherten Daten und die Empfänger, an die die Daten weitergegeben werden bzw. weitergegeben worden sind, erhalten werde. Diese Auskunft an den Beschwerdeführer befand sich nach Angaben der Stadtverwaltung bereits auf dem Postweg. Der TLfDI hat den Beschwerdeführer über die Antwort der Stadtverwaltung informiert.
Die datenschutzrechtliche Zuständigkeit für die Kontrolle des Beitragsservices von ARD, ZDF und Deutschlandradio liegt allerdings aufgrund von § 28 Abs. 1 Satz 2 ThürDSG nicht beim TLfDI. Der Beitragsservice hat gemäß § 11 Abs. 2 Rundfunkbeitragsstaatsvertrag einen eigenen Datenschutzbeauftragten, der betriebsintern die Einhaltung datenschutzrechtlicher Vorschriften unterstützt. Der TLfDI hat dem Beschwerdeführer die Kontaktdaten der Datenschutzbeauftragten des Beitragsservices übermittelt und gebeten, sich in dieser Angelegenheit unmittelbar an die genannte Institution zu wenden.

Die „Mühlen“ der Behörden „mahlen“ mitunter langsam. Auch Missverständnisse können nicht immer ausgeräumt oder zu 100 % ausgeschlossen werden. Wenn im Ergebnis dem Datenschutz Genüge getan wird, ist der TLfDI aber zufrieden. Er sieht seine Aufgaben unter anderem auch darin, „liegen gebliebene“ datenschutzrechtliche Anfragen an die Verwaltung erneut „anzuschieben“.

6.21 Glückwunschschreiben vom Oberbürgermeister zur Schuleinführung: nicht gewünscht und datenschutzrechtlich unzulässig!

Eine besorgte Mutter teilte dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) mit, dass ihre Tochter am Tag der Schuleinführung eine Glückwunschkarte des Oberbürgermeisters der Stadt Nordhausen erhalten habe. Sowohl auf dem Umschlag der Karte als auch auf der Karte selbst sei die Tochter mit allen drei Vornamen und dem Nachnamen benannt worden. Da die Mutter bei der Anmeldung lediglich den Rufnamen der Tochter angegeben habe, stelle sich ihr die Frage, inwieweit ggf. das Einwohnermeldeamt personenbezogene Daten herausgäbe. Sie bat den TLfDI zu prüfen, ob eine derartige Nutzung personenbezogener Daten von Schulanfängern zulässig sei. Die Mutter sah durch diese mögliche Datenverarbeitung die Persönlichkeitsrechte ihrer Tochter verletzt.
Der TLfDI wandte sich zur datenschutzrechtlichen Klärung der Angelegenheit an den Oberbürgermeister und bat um Mitteilung, wer ihm für die genannten Glückwunschkarten die Daten der Schulanfänger der Grundschule Nordhausen übermittelt, ob er diese ggf. beim Meldeamt der Stadtverwaltung angefordert und auf welcher Rechtsgrundlage er die personenbezogenen Daten der Schulanfänger verarbeitet und genutzt habe.
Der Nordhäuser Oberbürgermeister teilte dem TLfDI mit, dass die Daten der Schulanfänger im Vorjahr jeweils Ende September/Oktober von der Schulverwaltung der Stadt Nordhausen beim Einwohnermeldeamt angefordert und sodann den jeweils zuständigen Schulen übermittelt würden. Nach der erfolgten Schulanmeldung erbitte die Schulverwaltung der Stadt Nordhausen im Auftrag des Oberbürgermeisters von den Schulen zum Zweck der Erstellung der vom Oberbürgermeister zu signierenden Glückwunschkarten die Zusendung der Vor- und Familiennamen der in der jeweiligen Schule angemeldeten Kinder.
Eine Verarbeitung – diese umfasst auch die Erhebung und Übermittlung – und Nutzung personenbezogener Daten ist gemäß § 4 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) nur zulässig, soweit das Thüringer Datenschutzgesetz oder eine andere Rechtsvorschrift sie erlaubt oder anordnet oder soweit der Betroffene eingewilligt hat. Eine Zulässigkeit der Datenübermittlung könnte sich zwar aus § 57

Abs. 1 Thüringer Schulgesetz (ThürSchulG) ergeben. Zur Erfüllung der den Schulträgern und Schulaufsichtsbehörden durch Rechtsvorschriften zugewiesenen Aufgaben sind das Verarbeiten und Nutzen personenbezogener Daten der Schüler demnach zulässig, soweit dies für den jeweils mit den Aufgaben verbundenen Zweck erforderlich ist. Die namentliche Beglückwünschung der Schulanfänger durch den Oberbürgermeister zählt aber nach Auffassung des TLfDI nicht zu den Aufgaben des Oberbürgermeisters. Zwar verkennt der TLfDI durchaus nicht das Ansinnen des Oberbürgermeisters. Als datenschutzfreundliche Lösung könnte aber z. B. die Schule auf Bitte des Oberbürgermeisters bereits bei der Anmeldung die entsprechende Einwilligung der Eltern zur Verarbeitung der Daten (Vor- und Zuname des Kindes) für den Zweck „Beglückwünschung der Schulanfänger durch den Oberbürgermeister“ einholen.
Im Ergebnis hielt der TLfDI die namentliche Beglückwünschung der Schulanfänger durch den Oberbürgermeister ohne Einwilligung der Betroffenen (Eltern) für nicht datenschutzkonform und bat den Oberbürgermeister, umgehend für Abhilfe Sorge zu tragen.
Die Stadt Nordhausen hat den TLfDI daraufhin informiert, dass es in Zukunft keine namentlichen Beglückwünschungen von Schulanfängern geben werde. Sollten die Kinder weiter eine Grußkarte des Oberbürgermeisters zur Einschulung erhalten, so werden diese anonymisiert am ersten Schultag in den Schulen ausgegeben.
Dieses Vorgehen hält der TLfDI im Ergebnis für datenschutzkonform.

Über eine Glückwunschkarte vom Oberbürgermeister zum Schulanfang freuen sich fast alle Grundschüler (und ihre Eltern), aber nur, sofern datenschutzrechtliche Regelungen beachtet werden.

6.22 Nebenkostenschuldner einer Wohnungseigentümergesellschaft wird von der Verwaltungs-GmbH verpetzt

Ein Beschwerdeführer, der Mitglied einer Wohnungseigentümergemeinschaft war, setzte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) darüber in Kenntnis, dass eine GmbH, die für die Verwaltung und Abrechnung der Wohnanlage der Wohnungseigentümergemeinschaft zuständig war, eine Verwaltungskostenabrechnung, aus der die Schulden des Beschwerdeführers hinsichtlich der Instandhaltungsrücklage zu ent-

nehmen waren, erstellt und diese dann allen weiteren Eigentümern der Wohnanlage übermittelt habe.
Zunächst war vom TLfDI zu entscheiden, ob es sich bei der GmbH um eine öffentliche oder nicht-öffentliche Stelle handelte, da die Gesellschaftsanteile sämtlich durch eine Thüringer Kommune gehalten wurden.
Die GmbH bot einen Verwaltungsdienst für private Immobilien an, im konkreten Fall für Sondereigentumsverwaltung (Eigentumswohnungen).
Zu den Aufgaben der öffentlichen Verwaltung gemäß § 1 Abs. 3 Thüringer Kommunalordnung (ThürKO) zählen u. a. die Energie- und Wasserversorgung, die Bereitstellung des örtlichen ÖPNV als Aufgaben des örtlichen Wirkungskreises der Gemeinden (§ 2 Abs. 2 ThürKO). Nicht ausreichend sind hingegen Aufgaben, die lediglich im allgemeinen öffentlichen Interesse liegen (so Abel/Müller-Grune/Dick, Thüringer Datenschutzgesetz, Kommentar, § 2, Nr. 3, Privatrechtliche Rechtsformen [Absatz 2]).
Damit lag keine Aufgabe der öffentlichen Verwaltung vor. Die Verwaltung von Eigentumswohnungen stellt eine rein privatrechtliche Tätigkeit dar.
Damit war hier § 28 Bundesdatenschutzgesetz (BDSG) zugrunde zu legen, der die Datenerhebung und -speicherung für eigene Geschäftszwecke regelt. § 28 BDSG hat folgenden Wortlaut:
„§ 28 Datenerhebung und -speicherung für eigene Geschäftszwecke
(1) Das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke ist zulässig
1. wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist, …
Vorliegend kam die Tatbestandsalternative der *Durchführung* eines rechtsgeschäftlichen Schuldverhältnisses in Betracht.
Die Wohnungseigentümer standen im vorliegenden Fall untereinander zweifellos in einem rechtsgeschäftlichen Schuldverhältnis. Die GmbH verwaltete diese Rechte und Pflichten der Wohnungseigentümer, das heißt, sie trieb unter anderem Forderungen der Gemeinschaft ein und führte Beschlüsse der Wohnungseigentümerversammlung aus.

Fraglich war, ob die Information der Wohnungseigentümergemeinschaft, d. h. jedes Wohnungseigentümers, über den Schuldenstand eines einzelnen erforderlich war.
Grundsätzliche Entscheidungen werden nach § 23 Wohnungseigentumsgesetz (WEG) in der Wohnungseigentümerversammlung getroffen. Nach § 16 Abs. 2 WEG ist jeder Wohnungseigentümer den anderen Wohnungseigentümern gegenüber verpflichtet, die Lasten des gemeinschaftlichen Eigentums sowie die Kosten der Instandhaltung, Instandsetzung, sonstigen Verwaltung und eines gemeinschaftlichen Gebrauchs des gemeinschaftlichen Eigentums nach dem Verhältnis seines Anteils (§ 16 Abs. 1 Satz 2 WEG) zu tragen. Daraus folgt, dass die Wohnungseigentümerversammlung auch in die Lage versetzt werden muss, dieses Recht auf Kostentragung durchzusetzen. Praktisch heißt dies, dass gegebenenfalls der Beschluss gefasst wird, Klage gegen den betreffenden Schuldner einzureichen. Hierzu ist die Kenntnis der Identität des Schuldners erforderlich.
Des Weiteren war für den vorliegenden Sachverhalt die Regelung des § 18 Abs. 2 Nr. 2 WEG relevant, nach der die anderen Wohnungseigentümer von einem Wohnungseigentümer die Veräußerung seines Wohnungseigentums verlangen können, wenn Letzterer sich einer so schweren Verletzung einer gegenüber anderen Wohnungseigentümern obliegenden Verpflichtung schuldig gemacht hat, dass diesen die Fortsetzung der Gemeinschaft mit ihm nicht mehr zugemutet werden kann. Diese Voraussetzungen liegen insbesondere dann vor, wenn der Wohnungseigentümer sich mit der Erfüllung seiner Verpflichtungen zur Lasten- und Kostentragung (§ 16 Abs. 2 WEG) in Höhe eines Betrags, der drei vom Hundert des Einheitswerts seines Wohnungseigentums übersteigt, länger als drei Monate in Verzug befindet.
Auch hier verhält es sich so, dass die Wohnungseigentümerversammlung die Kenntnis erlangen muss, gegen wen ein Verfahren nach § 18 Wohnungseigentumsgesetz einzuleiten ist. Die Kenntnis der Identität des Schuldners ist hierfür erforderlich.
Im Ergebnis war damit die Kenntnis der Identität des Schuldners erforderlich im Sinne des § 28 BDSG. Daher konnte kein Verstoß gegen datenschutzrechtliche Bestimmungen festgestellt werden.

Die Bekanntgabe eines Nebenkostenschuldners gegenüber der Wohnungseigentümergemeinschaft, die dem WEG unterfällt, ist erforderlich, damit Letztere ihre Rechte nach § 16 und § 18 WEG ausüben

kann. Ein Verstoß gegen § 28 Abs. 1 BDSG liegt somit nicht vor, da die personenbezogenen Daten nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG verarbeitet werden durften.

6.23 Ausspionieren eines Facebook-Accounts durch einen Mitarbeiter einer Wohnungsbaufirma?

Eine Mieterin beschwerte sich beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) über einen Mitarbeiter ihres Vermieters, einer Kommunalen Wohnungsbaugesellschaft, der ihren Facebook-Account ausspioniert habe. Die Beschwerdeführerin stützte ihre Beschwerde darauf, dass sie der betreffende Mitarbeiter beschuldigt habe, sie hätte den automatischen Türschließer ihrer Wohnungstür ausgehängt, was auf einem Bild ihres Facebook-Profils zu sehen gewesen sei.
Auf Anforderung des TLfDI, zu der Angelegenheit Stellung zu nehmen und insbesondere mitzuteilen, zu welchem Zwecke ihre Mitarbeiter auf Facebook nach personenbezogenen Daten von Kunden ihres Unternehmens recherchiert haben und auf welcher Rechtsgrundlage eine solche Recherche beruht, teilte die Wohnungsbaugesellschaft mit, dass der Mitarbeiter mitgeteilt habe, dass er sich bei einem Gespräch mit der Mieterin wegen eines Schadensfalles lediglich auf ein durch die Mieterin öffentlich in Facebook eingestelltes Foto berufen habe.
Ein Facebook-Kunde hat zu einer Kenntnisnahme der auf seiner öffentlich zugänglichen Facebook-Seite eingestellten Daten durch Dritte eingewilligt. Er kann sich nicht aussuchen, ob Dritte dann nur die Informationen der Seite entnehmen, die ihm genehm sind. Daher konnte der TLfDI einen diesbezüglichen Verstoß gegen datenschutzrechtliche Vorschriften in diesem Falle nicht feststellen.

Dieses Beispiel zeigt die Eigenverantwortlichkeit der Bürger in der modernen Informationsgesellschaft bei der Nutzung der sozialen Medien und modernen Kommunikationsmittel. Insbesondere beim Umgang mit den sogenannten Sozialen Medien sollte man sich gut überlegen, welche personenbezogenen Daten man veröffentlicht.

6.24 Videokamera in der Gemeinde Piesau – reloaded

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) hatte in seinem 11. Tätigkeitsbericht für den öffentlichen Bereich (Nr. 5.31) darüber berichtet, dass er die Gemeinde Piesau aufgefordert hatte, die am Gemeindeamt Piesau und am Treffpunkt der Gemeindejugend im Bauhof der Gemeinde Piesau befindlichen defekten Videokameras abzubauen bzw. sie mittels einer Schutzfolie erkennbar zu deaktivieren und ihn über den Vollzug dieser Maßnahmen in Kenntnis zu setzen. Der TLfDI begründete diese Forderung seinerzeit damit, dass auch deaktivierte Kameras geeignet sind, bei Passanten den Anschein zu erwecken, dass ihr Verhalten überwacht werde. Dies könne eine negative Beeinflussung des Verhaltens von Bürgern zur Folge haben. Somit seien die o. g. Kameras gem. § 25a Thüringer Datenschutzgesetz zu beurteilen. Im Ergebnis ging der TLfDI von einer datenschutzrechtlichen Unzulässigkeit der Installation der (deaktivierten) Videokameras aus, da Betroffene davon ausgehen konnten, dass sie mit derart platzierten Kameras aufgenommen werden. Nachfolgend informierte die Gemeinde Piesau den TLfDI darüber, dass die o. g. defekten Kameras mit einer Schutzfolie abgedeckt wurden und damit nicht mehr sichtbar seien.

Im aktuellen Berichtszeitraum setzte die Verwaltungsgemeinschaft Lichtetal am Rennsteig den TLfDI darüber in Kenntnis, dass im Gemeinderat Piesau vorgeschlagen worden sei, die o. g. Videokameras am Gemeindeamt sowie im Bauhof/Jugendtreff zu reaktivieren bzw. neu anzubringen und bat um Informationen zum Stand der Angelegenheit.

Daraufhin teilte der TLfDI der Verwaltungsgemeinschaft Lichtetal am Rennsteig, u. a. mit, dass er der Bürgermeisterin von Piesau die Rechtslage zu dem abgeschlossenen Altfall mehrfach mitgeteilt hätte, wonach bei den bislang installierten Videokameras mangels einer geeigneten Rechtsgrundlage, die den mit dem Betrieb der Videoanlage verbundenen Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen rechtfertigen könnte, von einer datenschutzrechtlichen Unzulässigkeit auszugehen sei. Dass die Videokamera am Gemeindehaus mit öffentlichen Mitteln gefördert wurde und Aussteller zum Schutze ihrer Ausstellungsstücke in der Heimatstube des Gemeindehauses eine „vorsorgliche“ Videoüberwachung des Eingangsbereiches eines öffentlichen Gebäudes wün-

schen, rechtfertige nicht den mit der Videoüberwachung verbundenen Grundrechtseingriff. Letztendlich ist die Gemeinde Piesau der Forderung des TLfDI nachgekommen. Dem TLfDI sind keine neuen Tatsachen bekannt, die eine Reaktivierung bzw. Neuinstallation von Videokameras seitens der Gemeinde Piesau rechtfertigen könnten.

Der TLfDI hat seine Rechtsauffassung vom 11. Tätigkeitsbericht zur datenschutzrechtlichen Unzulässigkeit der Piesauer Videokameras auf Anfrage nochmals bestätigt. Dass Videokameras mit öffentlichen Mitteln gefördert wurden, kann kein Rechtfertigungsgrund für den mit der Videoüberwachung verbundenen Grundrechtseingriff sein.

6.25 Speicherung von personenbezogenen Daten bei der Vergabe eines roten Kennzeichens

Ein Landratsamt hatte an einen „Autoservice“ ein „rotes Kennzeichen“ zur dauerhaften Verwendung ausgegeben. Später wurde dessen Rückgabe verlangt, da es aus Sicht des Landratsamtes zu Pflichtverstößen des Kennzeicheninhabers kam. Im Zuge dieses Verwaltungsverfahrens nahm der Betroffene Akteneinsicht und meinte, dass von ihm in unzulässiger Weise persönliche Daten in der Akte gespeichert worden seien. Deshalb wandte er sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Dieser führte eine Vor-Ort-Kontrolle im Landratsamt durch.
Da die Zulässigkeit einer Datenspeicherung von deren Zweck abhängt, war vom TLfDI zunächst zu klären, wie der Bescheid des Landratsamtes zur Zuteilung eines roten Kennzeichens rechtlich einzuordnen war.
Ein Bescheid über die Zuteilung eines roten Kennzeichens stellt einen genehmigenden Verwaltungsakt (VA) mit Widerrufsvorbehalt dar, der dem zuverlässigen Antragsteller die Möglichkeit einräumt, Fahrzeuge mit den roten Zulassungskennzeichen zu versehen und zweckgemäß zu gebrauchen. Es handelt sich dabei um einen Dauerverwaltungsakt, da zwischen den Beteiligten ein langfristiges Rechtsverhältnis begründet oder verändert wird. Im Gegensatz zu einem einmaligen VA wirkt ein VA mit Dauerwirkung nicht nur zu einem bestimmten Zeitpunkt, sondern während der gesamten Dauer des Rechtsverhältnisses fort. Daraus folgt, dass die gesetzlich gefor-

derte „Zuverlässigkeit“ des Kennzeicheninhabers auch dauerhaft gegeben sein muss.
Im Rahmen des Vor-Ort-Termins konnte kein Verstoß gegen das Thüringer Datenschutzgesetz festgestellt werden. In der Akte des Antragstellers befanden sich zwei Auszüge (jeweils eine einzelne Seite) von Fahrtenbüchern aus zwei verschiedenen Jahren. Auf diesen Fahrtenbuchseiten wurden nach Aussage des zuständigen Mitarbeiters der Zulassungsstelle im Rahmen einer Kontrolle Beanstandungen festgestellt, die Rückschlüsse auf die Zuverlässigkeit/Unzuverlässigkeit beinhalteten. Diese beiden Fahrtenbuchseiten wurden im Rahmen einer ordnungsgemäßen Aktenführung dazu benötigt, um das Merkmal der Zuverlässigkeit des Antragstellers zu belegen, was für eine weitergehende Bewilligung unablässig war.
Nach § 20 Thüringer Datenschutzgesetz ist das Speichern personenbezogener Daten zulässig, wenn es zur Erfüllung der in der Zuständigkeit der Daten verarbeitenden Stelle liegenden Aufgaben erforderlich ist. Eine Erforderlichkeit zur Speicherung und Vorhaltung der persönlichen Daten wird aus der Pflicht zur ordnungsgemäßen Aktenführung nach § 29 Thüringer Verwaltungsverfahrensgesetz (VwVfG) abgeleitet (Kopp/Ramsauer, Kommentar zum VwVfG, 10. Auflage, § 29 Rd 11).
Eine ordnungsmäße Aktenführung umfasst die Pflicht der Behörde zur objektiven Dokumentation des wesentlichen sachbezogenen Geschehensablaufs. Die öffentliche Verwaltung ist verpflichtet, Akten zu führen (Gebot der Aktenmäßigkeit), alle wesentlichen Verfahrenshandlungen vollständig und nachvollziehbar abzubilden (Gebot der Vollständigkeit und Nachvollziehbarkeit) und diese wahrheitsgemäß aktenkundig zu machen.
Daher waren Datenverstöße nicht zu erkennen.

Ein Bescheid über die Zuteilung eines roten Kennzeichens stellt einen genehmigenden Verwaltungsakt (VA) mit Widerrufsvorbehalt dar, der dem zuverlässigen Antragsteller die Möglichkeit einräumt, Fahrzeuge mit den roten Zulassungskennzeichen zu versehen und zweckgemäß zu gebrauchen. Es handelt sich dabei um einen Dauerverwaltungsakt. Um die Zuverlässigkeit beurteilen zu können, muss die Zuverlässigkeit auch dauerhaft, ordnungsgemäß aktenmäßig dokumentiert sein.
Eine ordnungsgemäße Aktenführung umfasst die Pflicht der Behörde zur objektiven Dokumentation des wesentlichen sachbezogenen

Geschehensablaufs. Die öffentliche Verwaltung ist verpflichtet, Akten zu führen (Gebot der Aktenmäßigkeit), alle wesentlichen Verfahrenshandlungen vollständig und nachvollziehbar abzubilden (Gebot der Vollständigkeit und Nachvollziehbarkeit). Die Speicherung von personenbezogenen Daten, kann sich aus dieser Pflicht nach § 29 VwVfG ergeben.

6.26 Ein wichtiger Schritt zur Integration: TLfDI hilft

Im Berichtszeitraum erreichte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) eine Anfrage des Landratsamtes Sonneberg.
Hintergrund war die Teilnahme des Landkreises Sonneberg am Bundesprojekt „Bildung integriert“. Ziel war es, Neuzugewanderte im Bereich der Bildung gut zu integrieren und entsprechende Angebote zu schaffen. Aus diesem Grund übersandte das Landratsamt Sonneberg dem TLfDI einen Fragebogen, der Aufschluss über den Bildungsstand der Asylsuchenden geben sollte. Die angedachten Fragen drehten sich beispielsweise um die vorhandenen Sprachkenntnisse, die berufliche Ausbildung respektive Bildung, den Abschluss eines Studiums und dergleichen. Unsicherheit bestand dahingehend, ob diese Daten mittels eines selbst entworfenen Fragebogens erhoben werden dürften.
Gemäß § 4 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) ist die Verarbeitung und Nutzung personenbezogener Daten nur zulässig, wenn sie das ThürDSG oder eine andere Rechtsvorschrift erlaubt oder anordnet oder soweit der Betroffene eingewilligt hat. Der TLfDI hat daher angeregt, vor der Befragung – mittels eines Fragebogens – eine Einwilligungserklärung durch die betroffenen Asylsuchenden einzuholen.
Die Anregung des TLfDI, eine Einwilligungserklärung der Teilnehmer vor der Befragung mittels Fragebogen einzuholen, wurde vom Landratsamt Sonneberg dankend übernommen. Die Erklärung wurde neben den Sprachen Deutsch und Englisch auch ins Arabische und Persische übersetzt, um mögliche Missverständnisse bereits von Beginn an einzudämmen. Die deutsche Ausgabe des Fragebogens wurde auch in die Sprachen Englisch, Arabisch und Persisch übertragen, um mehr Interesse für eine Teilnahme zu wecken und somit jene Personen einzubeziehen, die Deutsch oder Englisch nicht verstehen können.

Ein schönes Beispiel dafür, datenschutzrechtliche Fragestellungen besser vorab vom TLfDI klären zu lassen, als im Nachhinein Probleme mit dem TLfDI zu bekommen.

Gemäß § 4 Abs. 2 und 3 ThürDSG erfolgt die Einwilligung auf freiwilliger Basis und bedarf der Schriftform oder der elektronischen Form mittels qualifizierter Signatur. Außerdem ist der Betroffene auf den Zweck und den Umfang der Verarbeitung oder Nutzung sowie die voraussichtliche Dauer der Speicherung seiner Daten hinzuweisen. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist die Einwilligungserklärung im äußeren Erscheinungsbild der Erklärung hervorzuheben.

6.27 Angst vor waffenbesitzendem Ehemann

Eine Betroffene setzte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) über folgenden Sachverhalt in Kenntnis:
Die Betroffene hatte die Waffenbehörde eines Landratsamtes aus Furcht davor, dass ihr Ehemann mit seinen Waffen andere bedrohen könnte, vertraulich informiert. Wenig später hatte das Landratsamt ihren Ehemann über ihren erfolgten Hinweis ohne ihre Einwilligung telefonisch in Kenntnis gesetzt.
Der TLfDI teilte dem Landratsamt mit, dass er davon ausgehe, dass hier ein Verstoß gegen datenschutzrechtliche Vorschriften in Form einer unzulässigen Übermittlung personenbezogener Daten vorliege und forderte es auf, zu dieser Angelegenheit Stellung zu nehmen und insbesondere mitzuteilen, auf welcher Rechtgrundlage die Information an den Ehemann der Betroffenen beruhte und zu welchem Zwecke sie erfolgte.
In seiner Stellungnahme gegenüber dem TLfDI beschränkte sich das Landratsamt auf die Mitteilung, dass das Landratsamt auf Nachfrage des Ehemannes telefonisch mitgeteilt bzw. bestätigt habe, dass seine Ehefrau den Vorfall der Behörde gemeldet habe. Weiterhin habe die Waffenbehörde den Waffenbesitzer gebeten, die Waffen aus seinem direkten Zugriff zu entfernen; dies stelle, so die Waffenbehörde, „… eine gefahrenmindernde Maßnahme mit Einschränkung von Eigentumsrechten nach dem Ordnungsrecht …“ dar. Eine rechtliche Wertung der unzulässigen Datenübermittlung nahm das Landratsamt nicht vor.

Der TLfDI teilte daraufhin dem Landratsamt mit, dass die telefonische Mitteilung an den Waffenbesitzer, dass sich seine Ehefrau über ihn beschwert habe, datenschutzrelevant sei und daher gesondert beurteilt werden müsse.
Nach Auffassung des TLfDI betrifft diese Auskunft bzw. Bestätigung ein personenbezogenes Datum der betroffenen Ehefrau, § 3 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG). Die Verarbeitung personenbezogener Daten, die nach § 3 Abs. 3 Nr. 4 ThürDSG auch deren Übermittlung betrifft, ist jedoch nur dann zulässig, wenn das ThürDSG oder eine andere Rechtsvorschrift sie erlaubt oder anordnet oder soweit der bzw. die Betroffene eingewilligt hat, § 4 Abs. 1 ThürDSG.
Da diese Zulässigkeitsvoraussetzungen nicht gegeben sind, handelt es sich bei der telefonischen o. g. Bestätigung um einen Verstoß gegen datenschutzrechtliche Vorschriften in Form einer unzulässigen Übermittlung personenbezogener Daten.
Diese Bewertung hat der TLfDI dem Landratsamt mitgeteilt und gefordert, den TLfDI darüber in Kenntnis zu setzen, wie dieses Vorkommnis in der Behörde ausgewertet wurde und welche organisatorischen Maßnahmen künftig veranlasst werden, um eine datenschutzkonforme Reaktion seitens der Behörde in ähnlichen Fällen sicherzustellen.
Das Landratsamt teilte mit, dass im zuständigen Fachreferat aufgrund der Forderungen des TLfDI die datenschutzrechtlichen Bestimmungen ausgewertet wurden. Insbesondere seien die Mitarbeiter hinsichtlich der Zulässigkeitsvoraussetzungen für die Übermittlung personengebundener Daten noch einmal geschult und sensibilisiert worden.

Eine Information an eine Behörde zu einem Fehlverhalten eines Dritten, das zu einem Einschreiten der Waffenbehörde nach § 41 „Waffenverbot für den Einzelfall“ führen kann, ist grundsätzlich vertraulich zu behandeln. Die Weitergabe dieser Daten an den waffenbesitzenden Ehemann der Betroffenen seitens der Waffenbehörde stellt mangels einer geeigneten Rechtsgrundlage einen Verstoß gegen datenschutzrechtliche Vorschriften dar.

6.28 „Offene“ Unterschriftensammlung zur Kreisfreiheit im Einkaufscenter

Ein Bürger legte dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) Fotos von einer „offenen“ Unterschriftensammlung zum Erhalt der Kreisfreiheit der Stadt Weimar in einem Einkaufszentrum in Weimar vor und bat um datenschutzrechtliche Bewertung der Angelegenheit.
Nachdem erste Recherchen die Vermutung bestätigten, dass die Stadt Weimar an der Unterschriftensammlung beteiligt war, forderte der TLfDI die Stadtverwaltung Weimar auf, mitzuteilen, welche personenbezogenen Daten zu welchem Zweck erhoben wurden, auf welcher Rechtsgrundlage die Erhebung und Verarbeitung dieser Daten beruhte, wie die Verarbeitung der erhobenen Daten konkret erfolgen sollte und welche Stellen daran beteiligt waren sowie eine Kopie des verwendeten Fragebogens vorzulegen.
Daraufhin setzte die Stadt Weimar den TLfDI darüber in Kenntnis, dass Listen mit der Überschrift „Ich unterstütze die Petition mit meiner Unterschrift: Weimar muss kreisfrei bleiben!“ sowie Vor- und Zunamen, Anschriften, E-Mail-Adresse und Unterschriften von Weimarer Bürgern zum Zwecke einer Petition dem Präsidenten des Thüringer Landtags und der Thüringer Landesregierung vorgelegt werden sollten, um zu bewirken, dass die Aufgabe der Kreisfreiheit Weimars im Zuge der Gebietsreform nicht in der vorgesehenen Form umgesetzt wird. Weiter teilte die Stadtverwaltung Weimar mit, dass die Unterschriftenlisten von Mitarbeitern der Stadtverwaltung Weimar und unterstützenden Bürgern ausgelegt und nur dem Präsidenten des Thüringer Landtags, der Thüringer Landesregierung und der „openPetition gemeinnützige“ GmbH übermittelt werden sollten.
Wie der TLfDI feststellte, enthielten die Unterstützerlisten eine „Datenschutzerklärung“ mit folgenden Wortlaut: „Ihre Daten werden ausschließlich zum Zweck dieser Petition verwendet. Die Angabe der E-Mail-Adresse ist freiwillig. Wenn Sie oben mit *ja* angekreuzt haben, wird openPetition Sie über den Fortgang dieser und weiterer Petitionen informieren. Ihre Daten werden nicht an Dritte weitergegeben und werden nach Ende dieser Petition oder auf Ihren Wunsch hin auch früher gelöscht.“ Eine gesonderte Einwilligungserklärung wurde jedoch nicht festgestellt.
Der TLfDI bewertete die Angelegenheit gegenüber der Stadt Weimar wie folgt:

Da Mitarbeiter der Stadtverwaltung Weimar an der Durchführung der damit verbundenen Erhebung personenbezogener Daten beteiligt waren und der Oberbürgermeister der Stadt Weimar die Angelegenheit unterstützte, war die Stadt Weimar in diesem Zusammenhang zumindest als mitverantwortliche Stelle im Sinne des § 3 Abs. 5 Thüringer Datenschutzgesetz (ThürDSG) anzusehen.
Die Verarbeitung personenbezogener Daten, zu der nach § 3 Abs. 3 ThürDSG auch deren Erheben zählt, ist gemäß § 4 Abs. 1 ThürDSG nur zulässig, wenn das ThürDSG oder eine andere Rechtsvorschrift sie erlaubt oder anordnet oder soweit der Betroffene eingewilligt hat. Im Falle der Einwilligung ist die Verarbeitung personenbezogener Daten nur zulässig, wenn dies zur Erfüllung anerkannter Zwecke erforderlich ist. Das Erheben personenbezogener Daten ist zulässig, wenn deren Kenntnis nach § 19 Abs. 1 ThürDSG zur Erfüllung der Aufgaben der erhebenden Stelle erforderlich ist.
Eine Rechtsvorschrift im Sinne des § 4 Abs. 1 ThürDSG, die einer Kommunalverwaltung erlaubt oder sie verpflichtet, personenbezogenen Daten zum Zwecke einer Petition zu erheben, ist nicht ersichtlich. Auch dafür, dass die Kenntnis der erhobenen Daten gemäß § 19 Abs. 1 ThürDSG zur Erfüllung der Aufgaben der Stadtverwaltung erforderlich war, gibt es keine Anhaltspunkte.
Ebenso mangelt es an einer datenschutzrechtlichen Einwilligung im Sinne der § 4 Abs. 2 und 3 ThürDSG. Das ergibt sich bereits daraus, dass eine mit der Unterschrift des Betroffenen versehene Einwilligungserklärung in die Verarbeitung und Nutzung seiner personenbezogenen Daten gemäß § 4 Abs. 3 Satz 3 ThürDSG (Schriftformerfordernis) nicht feststellbar war. Insofern war auch die o. g. „Datenschutzerklärung“ auf den Unterschriftenlisten nicht als datenschutzkonforme Einwilligung anzusehen.
Da eine geeignete Rechtgrundlage für die Verarbeitung und Nutzung der o. g. Daten nicht vorlag und die Betroffenen nicht in die Verarbeitung und Nutzung ihrer Daten eingewilligt haben, handelte es sich bei der Erhebung der persönlichen Auffassung der Bürger zur Aufhebung der Kreisfreiheit Weimars im Rahmen einer Petition um einen Verstoß gegen datenschutzrechtliche Vorschriften.
Zu einem ähnlichen Sachverhalt hatte sich der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) bereits in seinem 10. Tätigkeitsbericht unter dem Gliederungspunkt 5.31 kritisch geäußert.

Abschließend bat der TLfDI die Stadt Weimar, die datenschutzrechtlichen Vorschriften in ähnlichen Konstellationen künftig sorgfältiger zu beachten. Da die Unterschriftensammlung inzwischen beendet war, sah der TLfDI den Vorgang als erledigt an.

Leider sind sich einzelne Kommunalverwaltungen noch immer nicht darüber im Klaren, dass auch das Erheben personenbezogener Daten im Zusammenhang mit Umfragen bzw. Unterschriftensammlungen zu kommunalpolitischen Themen nach § 19 Abs. 1 ThürDSG nur dann zulässig ist, wenn die Kenntnis dieser Daten zur Erfüllung der Aufgaben der erhebenden Stelle erforderlich ist.
Die Kommune ist auch dann als verantwortliche Stelle im datenschutzrechtlichen Sinne anzusehen, wenn Dritte, wie z. B. Bürgerinitiativen, eine solche Unterschriftensammlung initiieren, sich die Kommune aber daran beteiligt.

6.29 Information der Gemeinde an das Kreditinstitut wegen beabsichtigter Kontopfändung?

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) hatte in seinem 11. Tätigkeitsbericht für den öffentlichen Bereich zum Gliederungspunkt 5.57, S. 161 bis 163 unter dem Titel „Pfändung nur mit Kenntnis der Bankverbindung zulässig“ über eine die Stadtverwaltung Eisfeld betreffende Beschwerde berichtet und u. a. festgestellt, dass die Vermutung, dass ein Kostenschuldner eines Verwaltungsaktes bei einem Kreditinstitut eine Bankverbindung unterhält, eine Behörde als Gläubiger dieser Forderung nicht berechtigt, das Kreditinstitut über seine Absicht einer Kontopfändung beim Kostenschuldner zu unterrichten. Lediglich bei sicherer Kenntnis der Bankverbindung des Kostenschuldners bei dem betreffenden Kreditinstitut ist die Information über eine Kontenpfändung aus datenschutzrechtlichen Gesichtspunkten gerechtfertigt.
Der TLfDI hatte die Stadtverwaltung Eisfeld noch im Berichtszeitraum 2014/2015 aufgefordert, die betreffenden Verwaltungsabläufe im Sinne der Einhaltung datenschutzrechtlicher Vorschriften zu verändern.
Die Stadtverwaltung Eisfeld teilte dem TLfDI daraufhin mit, dass sie künftig auf Kontopfändungen verzichten werde, da erfahrungsgemäß die Pfändungen ins Leere laufen würden, wenn der Schuldner wegen

einer beabsichtigten Pfändung um Bekanntgabe seiner Bankverbindung gebeten werde. Entweder gebe der Gläubiger die Bankverbindung nicht bekannt oder das Konto werde rechtzeitig geleert.

Eine Weitergabe von personenbezogenen Daten allein aufgrund von Verwaltungserfahrungen oder Vermutungen ist nicht zulässig. Zulässigkeitsvoraussetzung ist auch im Falle einer Information einer Bank seitens einer öffentlichen Stelle über Kontenpfändungen, dass eine Rechtsvorschrift die Übermittlung dieses Datums erlaubt oder anordnet oder der Betroffene in die Verarbeitung oder Nutzung seiner personenbezogenen Daten eingewilligt hat und die Datenübermittlung zur Erfüllung anerkannter Zwecke erforderlich ist, § 4 Abs. 1 Thüringer Datenschutzgesetz.

6.30 „Falsch geschwärzte“ Daten bei der Stadt Jena

Ein Bürger teilte dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) mit, dass die Stadtverwaltung Jena auf ihrer Internetseite ordnungsbehördliche Bescheide aufgrund des Vollzuges des Thüringer Gesetzes über die Aufgaben und Befugnisse der Ordnungsbehörden (Ordnungsbehördengesetz) samt Auflagen veröffentliche. Problematisch daran sei, dass jedermann personenbezogene Daten eines Bescheid-Adressaten zu einer angemeldeten Demonstration, möglicherweise infolge eines „falschen Schwärzens“ des Dokumentes, durch einfaches Markieren und Kopieren lesbar machen könne.
Der TLfDI forderte die Stadt Jena auf, zu der Angelegenheit Stellung zu nehmen. Daraufhin teilte die Stadtverwaltung Jena dem TLfDI mit, dass der beschwerdegegenständliche Auflagenbescheid mit den darin enthaltenen personenbezogenen Daten zwischenzeitlich aus dem Internet entfernt worden sei und derartige Bescheide künftig ohne personenbezogene bzw. personenbeziehbare Daten im Internet veröffentlicht werden sollen.

Bei der Nutzung des Internets als Publikations- bzw. Kommunikationsmedium sind die verantwortlichen Stellen im Rahmen des § 9 Thüringer Datenschutzgesetz (Gewährleistung des Datenschutzes durch technische und organisatorische Maßnahmen) auch verpflichtet, dafür zu sorgen, dass verlässliche technische Verfahren, z. B. der Datenlöschung und Verschlüsselung, genutzt werden, um eine unzu-

lässige Übermittlung personenbezogener bzw. personenbeziehbarer Daten mit Sicherheit auszuschließen.

6.31 Pistole auf die Brust: Vorkaufsrecht gegen Begleichung der Steuerschuld

Ein Beschwerdeführer teilte dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) mit, dass die Stadt Großbreitenbach im Zusammenhang mit einem Grundstückskaufvertrag sowohl den beteiligten Notar als auch den Grundstücksverkäufer über das Bestehen einer konkreten Steuerschuld des Beschwerdeführers in Kenntnis gesetzt habe und ihre Entscheidung zum gesetzlichen Vorkaufsrecht von der Begleichung der Steuerschuld des Beschwerdeführers abhängig mache.
Daraufhin setzte der TLfDI die Stadt Großbreitenbach darüber in Kenntnis, dass es sich bei den o. g. Mitteilungen nach seiner vorläufigen Beurteilung um unzulässige Übermittlungen von personenbezogenen Daten des Beschwerdeführers handle und forderte die Stadt Großbreitenbach auf, zu der Angelegenheit Stellung zu nehmen und insbesondere darzulegen, auf welcher Rechtsgrundlage die o. g. Übermittlungen personenbezogener Daten beruhen und zu welchen Zwecken sie erfolgten.
Die Stadt Großbreitenbach teilte dem TLfDI mit, dass sie „… nach Abwägung aller Interessen …“ entschieden habe, das Tätigwerden im Rahmen einer Bescheinigung zur Ausübung des gesetzlichen Vorkaufsrechts von der Begleichung der Steuerschuld des Beschwerdeführers abhängig zu machen. Die Mitteilung der Stadt Großbreitenbach an den Notar und den Grundstücksverkäufer sei im Innenverhältnis des Grundstückskaufvertrages erfolgt und die Vertragsparteien seien über die ihnen bekannt gewordenen Umstände zur Verschwiegenheit verpflichtet.
Nachfolgend setzte sich der TLfDI mit der o. g. Argumentation der Stadt Großbreitenbach auseinander und legte der Stadtverwaltung Großbreitenbach die bestehende Rechtslage wie folgt dar:
Die o. g. Argumentation der Stadt Großbreitenbach geht am Kern des Problems vorbei. Es geht nicht darum, ob die Empfänger personenbezogener Daten zur Verschwiegenheit verpflichtet sind, sondern ob diese Daten übermittelt werden durften. Nach § 4 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) ist die Verarbeitung – dieser Begriff beinhaltet auch die Datenübermittlung – und Nutzung perso-

nenbezogener Daten nur zulässig, wenn das ThürDSG oder eine andere Rechtsvorschrift sie erlaubt oder anordnet oder soweit der Betroffene eingewilligt hat. Nach § 22 ThürDSG ist eine Übermittlung an Stellen außerhalb des öffentlichen Bereichs nur zulässig, wenn erstens sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgaben erforderlich ist und die Voraussetzungen vorliegen, die eine Nutzung nach § 20 zulassen würde, oder zweitens der Dritte, an den die Daten übermittelt werden, ein berichtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegt und der Betroffene kein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat. Da die Zulässigkeitsvoraussetzungen des § 22 ThürDSG für solche Datenübermittlungen nicht gegeben waren und insbesondere erheblich in das informationelle Selbstbestimmungsrecht des Beschwerdeführers eingegriffen wurde, sind die erfolgten Mitteilungen zu den Steuerschulden des Beschwerdeführers unzulässig. Dies stellt einen Verstoß gegen datenschutzrechtliche Vorschriften dar.
Die Stadt Großbreitenbach teilte dem TLfDI auf Anfrage mit, dass sie die Rechtsvorschriften des ThürDSG künftig beachten werde. Es sei beabsichtigt, die Mitarbeiter der Stadtverwaltung per Dienstanweisung zur Einhaltung der datenschutzrechtlichen Bestimmungen zu verpflichten.

Leider zeigt dieser Fall wieder einmal das mangelnde Verständnis grundlegender datenschutzrechtlicher Normen in manchen Kommunen. Es kommt nicht darauf an, ob die Empfänger personenbezogener Daten zur Verschwiegenheit verpflichtet sind. Die datenschutzrechtliche Schlüsselfrage ist vielmehr, ob die betreffende Verarbeitung und Nutzung der personenbezogenen Daten nach § 4 Abs. 1 Thüringer Datenschutzgesetz erlaubt ist. Somit ist festzustellen, dass der Informationsbedarf in Sachen Datenschutz noch lange nicht gedeckt ist.

6.32 KoWo kooperativ!

Ein Journalist teilte dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) mit, dass er recherchiert habe, dass eine Kommunale Wohnungsgesellschaft (KoWo) in Thüringen unverschlüsselte Webformulare anbiete, in denen sensible Daten abgefragt würden.

Wie Nachforschungen des TLfDI ergaben, handelte es sich dabei um Webformulare zur Kontaktaufnahme mit der KoWo, zur Anmeldung von Reparaturen und zum Wohnungsgesuch. Tatsächlich war keines der Webformulare mit einer Transportverschlüsselung mittels eines entsprechenden Transportprotokolls abgesichert. Entsprechend den Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI) ist dabei das Transportprotokoll TLS in der aktuellen Version zu verwenden. Zudem wurden im Webformular zum Wohnungsgesuch hochsensible Daten der Mietinteressenten, u. a. zu deren monatlichen Einkommen, Angaben zum Beschäftigungsverhältnis oder zum Bezug von Sozialleistungen, abgefragt.
Der TLfDI teilte daraufhin der KoWo mit, dass damit zu rechnen sei, dass Mietinteressenten die ausgefüllten Webformulare unverschlüsselt an die KoWo zurücksenden. Somit sei nicht auszuschließen, dass auf diesem unsicheren Übertragungsweg personenbezogene Daten der Mietinteressenten von unberechtigten Dritten mitgelesen werden. Dies stelle einen Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen dar. Zugleich forderte der TLfDI die KoWo auf, mitzuteilen, welches Verschlüsselungsverfahren beim Transport der Daten wann und wie zum Einsatz kommt, aus welchen Gründen die KoWo nicht https-basierte Webformulare anbietet und wie sie die Authentifizierung des beteiligten Webservers gegenüber dem Client sicherstellt.
Zur rechtlichen Beurteilung der ähnlichen Thematik der Kommunikation mittels unverschlüsselter E-Mail hatte der TLfDI unter dem Beitrag 5.22 seines 11. Tätigkeitsberichts für den öffentlichen Bereich empfohlen, an Stelle unverschlüsselter E-Mail den sicheren Postweg für die Übermittlung personenbezogener Daten zu nutzen.
Neben der technischen Sicherheit hatte der TLfDI die im Webformular zum Wohnungsgesuch verwendeten Fragen zudem auf datenschutzrechtliche Zulässigkeit geprüft. Im Ergebnis dieser Prüfung stellte der TLfDI fest, dass jegliche Datenerhebung nach § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG) grundsätzlich einer wirksamen Einwilligung der betroffenen potenziellen Mieter oder einer gesetzlichen Grundlage bedarf. Da der Mietinteressent typischerweise meinen könnte, dass er nur dann eine Chance auf die begehrte Wohnung hat, wenn er die geforderten Daten liefert, kann jedoch nicht von einer wirksamen freiwilligen Einwilligung des Betroffenen im Sinne von § 4a Abs. 1 Satz 1 BDSG ausgegangen werden. In der Realität entfällt oftmals die scheinbare Wahlfreiheit und es entsteht eine

Drucksituation, in welcher eine freiwillige Einwilligung nicht möglich ist.
Da eine Einwilligung in derartigen Fällen in der Regel unwirksam ist, ist die Zulässigkeit für eine Erhebung einer Selbstauskunft im Besichtigungstermin und davor regelmäßig nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG zu beurteilen. Spätestens nach der Erklärung des Mietinteressenten, eine Wohnung anmieten zu wollen, entsteht dann ein vorvertragliches Schuldverhältnis zum künftigen Vermieter, sodass § 28 Abs. 1 Satz 1 Nr. 1 BDSG maßgebend ist. Hiernach ist das Erheben personenbezogener Daten als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist. Im Rahmen der dann vorzunehmenden Prüfung der Erforderlichkeit kommt es darauf an, ob von Seiten des Mietinteressenten Offenbarungspflichten bestehen bzw. ob der Vermieter zulässige Fragen stellt. Maßgebend für die Beurteilung des Fragerechts des Vermieters ist, inwieweit die begehrten Angaben in einem objektiven Zusammenhang zum Mietverhältnis stehen und ob schutzwürdige Interessen des Mietanwärters am Ausschluss der Datenerhebung bestehen. Dabei geht es nicht nur um eine datenschutzrechtliche, sondern auch um eine grundrechtliche Problematik der richtigen Abwägung zwischen Mieter- und Vermieterinteressen und damit um die Frage nach der Zulässigkeit oder Unzulässigkeit bestimmter Fragen. Die formularmäßigen Abfragen sollten zudem auf das erforderliche und datenschutzrechtlich zulässige Maß beschränkt werden.
Bezüglich der Datenerhebung ist entsprechend der von den obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis, 27. Januar 2014) beschlossenen Orientierungshilfe zur „Einholung von Selbstauskünften bei Mietinteressenten“, (vgl. Anlage 10 des 2. Tätigkeitsberichts des TLfDI für den nicht-öffentlichen Bereich S. 480 bis 488), dabei zwischen drei Zeitpunkten zu differenzieren, nämlich:

a) dem Besichtigungstermin,
b) der vorvertraglichen Phase, in welcher der Mietinteressent dem künftigen Vermieter mitteilt, eine konkrete Wohnung anmieten zu wollen und
c) der Entscheidung des künftigen Vermieters für einen bestimmten Mietinteressenten.

Deshalb ist ein dreiphasiges Verfahren zur formularmäßigen Abfrage von Mieterdaten empfehlenswert. Eine Unterscheidung nach o. g. Zeitpunkten (ggf. auch in gesonderten Formularen) ist bei der Art der Fragestellung notwendig, um die Mieterselbstauskunft datenschutzrechtlich zulässig anwenden zu dürfen. Bei einer formularmäßigen Mieterselbstauskunft muss dem potentiellen Mieter ersichtlich sein, dass er zum Besichtigungstermin nur die folgenden Daten angeben muss:

- Daten zur Identifikation des Mietinteressenten, hierzu zählen dessen Vorname und Nachname sowie die Adresse (ggf. Telefonnummer zu weiteren Terminabsprachen) und
- Angaben zur Haltung von größeren Tieren (unzulässig ist die pauschale Frage nach Haustieren jeglicher Art, also auch Kleintieren).

Die zweite Phase, die vorvertragliche Phase, tritt ein, wenn der Mietinteressent dem künftigen Vermieter mitteilt, das konkrete Mietobjekt anmieten zu wollen. Dann sind ggf. weitere Fragen zulässig. In der dritten Phase, der Entscheidung des künftigen Vermieters für einen bestimmten Mietinteressenten, möchte der künftige Vermieter nun mit einem Mietinteressenten für eine konkrete Wohnung einen Mietvertrag abschließen. Haben sich zwei oder mehrere Mietinteressenten für eine konkrete Wohnung entschieden, so trifft der künftige Vermieter die Entscheidung für einen bestimmten Mietinteressenten (Erstplatzierter). Nach dieser Entscheidung kann die Einholung weiterer Informationen beim Erstplatzierten erforderlich sein.

Zu den Fragen, die in der zweiten und dritten Phase zulässig sind, finden sich Hinweise in den Beiträgen 2.28 und 2.29 und Anlage 10 des zweiten Tätigkeitsberichts des TLfDI für den nicht-öffentlichen Bereich.

Konkret enthielt das Webformular der KoWo, das die Wohnungssuche, d. h. die o. g. erste Phase betraf, folgende Datenarten, die der TLfDI wie folgt bewertete:

- „E-Mail“ (Kategorie Erreichbarkeit)

Da eine unverschlüsselte Übermittlung personenbezogener Daten mittels des unsicheren Übertragungsweges E-Mail datenschutzrechtlichen Bedenken begegnet, sollte die Erhebung von E-Mail-Adressen entfallen, es sei denn, eine sichere E-Mail-Verschlüsselung steht den Kommunikationspartnern zur Verfügung, wovon im Regelfall nicht auszugehen ist.

- „Geburtsdatum“ (Kategorien „Persönliche Angaben“ und „Weitere Mietvertragspartner“)

Da eine Erforderlichkeit für die Erhebung von Geburtsdaten zur Aufgabenerfüllung des Vermieters nicht ersichtlich ist, sollten keine Geburtsdaten erhoben werden.

- „Einkommensart“ (Kategorien „Persönliche Angaben“ und „Weitere Mietvertragspartner“) für bis zu vier Personen

Unter „Einkommensart“ haben die Betroffenen die Wahl unter diversen konkreten Möglichkeiten, die Rückschlüsse auf ihren sozialen Status ermöglichen. Da eine Erhebung solch sensibler personenbezogener Daten unzulässig ist, sind die entsprechenden Fragen aus dem Formular zu entfernen.

- „Haustiere“ (Kategorie „Freiwillige Angaben“)

Die Erhebung von Tieren ist zum Zeitpunkt der Wohnungssuche unzulässig. Zum Zeitpunkt des Besichtigungstermins ist die Erhebung auf größere und gefährliche Tiere zu beschränken. Unzulässig ist die Frage nach kleinen Haustieren; im Formular sollte darauf hingewiesen werden.

- „Sonstiges“ (Kategorie „Freiwillige Angaben“)

Das Webformular Wohnungssuche betrifft einen Zeitpunkt, zudem noch nicht klar ist, ob es zu einem Besichtigungstermin kommen wird. Insofern sind zu diesem Zeitpunkt ausschließlich die Daten zur Identifikation des Mietinteressenten, hierzu zählen dessen Vorname und Nachname sowie die Adresse (ggf. Telefonnummer zu Terminabsprachen) erforderlich. Alle weiteren Daten sind als unzulässig anzusehen.

Der TLfDI teilte der KoWo seine o. g. Bewertung mit und forderte die KoWo auf, das Webformular zum Wohnungsgesuch entsprechend seiner Hinweise zu überarbeiteten, d. h. die Erhebung auf die Datenarten Vorname, Nachname, Adresse und Telefonnummer zu beschränken.

Wie der TLfDI feststellte, betrafen obige Feststellungen zum Webformular zum Wohnungsgesuch auch den Kundenerfassungsbogen der KoWo in Papierform.

Anlässlich eines Beratungsgesprächs zur inhaltlichen Gestaltung des Webformulars zum Wohnungsgesuch und des Kundenerfassungsbo-

gens kamen die KoWo und der TLfDI überein, dass die KoWo die o. g. Erhebungsformulare derart umgestaltet, dass der Interessent sich entscheiden kann, ob er eine Kontaktaufnahme per E-Mail oder auf dem Postweg wünscht und diese Kommunikationsalternativen in den Formularen deutlich zum Ausdruck bringt. Die Vertreter der KoWo sagten zu, die Einwilligungserklärung entsprechend den datenschutzrechtlichen Vorgaben nach dem Muster der „Orientierungshilfe zur datenschutzrechtlichen Einwilligungserklärung in Formularen“ zu überarbeiten. Der TLfDI regte an, die KoWo möge deutlicher zum Ausdruck bringen, dass sich die Überschrift „Achtung! Wichtiger Hinweis für den Mietinteressenten!“ auf dem Kundenerfassungsbogen und die Überschrift „Bestätigung der Richtigkeit der Daten“ auf dem Webformular zum Wohnungsgesuch auf die Einwilligung bezieht.

Nachfolgend wies die KoWo nach, dass die Erhebungsformulare entsprechend der o. g. Hinweise des TLfDI überarbeitet wurden. Der TLfDI stellte fest, dass nunmehr ausschließlich die Daten zur Identifikation des Mietinteressenten, hierzu zählen dessen Vor- und Nachname, die Adresse und ggf. die Telefonnummer zu Terminabsprachen erhoben werden und der Mietinteressent auf die alternativen Kommunikationsformen Postweg, E-Mail und Telefon hingewiesen wird. Die Überschrift auf dem Kundenerfassungsbogen wurde, wie vereinbart, von „Achtung! Wichtiger Hinweis für den Mietinteressenten!“ auf „Bestätigung der Richtigkeit der Daten / Einwilligungserklärung des Mietinteressenten“ geändert; diese geänderte Überschrift befindet sich nunmehr auch auf dem Webformular zum Mietgesuch. Laut der Datenschutzerklärung der Erhebungsformulare löscht die KoWo die Angaben zum Mietinteressenten bei Nichtzustandekommen eines Mietvertrages zu dessen „Gültigkeitsende“, jedoch spätestens nach zwei Jahren.

Allerdings hielt die KoWo die Erhebung des Geburtsdatums weiterhin für erforderlich, um auszuschließen, dass Mietinteressenten keine früheren Mietschulden mehr bei der KoWo besitzen. Nach nochmaliger Prüfung schlug der TLfDI hierzu folgende künftige Verfahrensweise vor:

Im Kundenerfassungsbogen sollte auf die Erhebung des Geburtsdatums verzichtet werden. Nach Vorliegen der Daten der Interessenten können deren Namen intern mit einer Datei zu früheren Mietschuldnern abgeglichen werden. Hat ein Interessent den gleichen Namen wie ein Mietschuldner, könnte er um eine Erklärung, dass er keine

Mietschulden bei der KoWo hat oder alternativ um sein Geburtsdatum gebeten werden. Aus Gründen der datenschutzrechtlich gebotenen Transparenz sollte dem Interessanten ein nachvollziehbarer Grund für diese zusätzliche Datenerhebung genannt werden. Das o. g. Verfahren hätte den Vorteil, dass die Erhebung des Geburtsdatums ausschließlich in den wenigen Fälle nötig wäre, in denen noch Mietschulden bei der KoWo bestehen könnten. Der TLfDI bat die KoWo, dem TLfDI den entsprechend dem o. g. Hinweis zum Geburtsdatum geänderten Kundenerfassungsbogen vorzulegen und mitzuteilen, ob auch im Webformular zum Wohnungsgesuch das Geburtsdatum entfernt wurde. Daraufhin teilte die KoWo dem TLfDI mit, dass sie das Geburtsdatum aus dem Kundenerfassungsbogen sowie dem Webformular zum Wohnungsgesuch entfernt habe und legte entsprechende Nachweise vor.

Der Prüfungs- und Beratungsprozess zum Thema hochsensible personenbezogene Daten auf einem unsicheren Webformular einer Kommunalen Wohnungsgesellschaft (KoWo) zum Mietgesuch war überaus komplex, da einerseits die datenschutzgerechte Formulargestaltung, insbesondere die rechtliche Zulässigkeit der Formularfragen, als auch vielschichtige Fragen zur Datensicherheit zu klären waren. Im Ergebnis ist die KoWo den Hinweisen des TLfDI gefolgt, sodass nunmehr ausschließlich die Daten zur Identifikation des Mietinteressenten (Vorname, Nachname und Adresse des Mietinteressenten und ggf. Telefonnummer zu Terminabsprachen) erfasst werden und der Mietinteressent auf die alternativen Kommunikationsformen Postweg, E-Mail und Telefon hingewiesen wird. Webformulare sind durch ein verschlüsseltes Transportprotokoll dem Stand der Technik entsprechend abzusichern.

6.33 Anfrage zur geplanten Identifikationskarte für Geflüchtete

Im Zusammenhang mit der bundesweiten Debatte um die Einführung einer Identifikationskarte für Geflüchtete wandte sich ein Abgeordneter des Thüringer Landtags mit der Frage an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), ob bereits eine datenschutzrechtliche Prüfung einer solchen Karte durch den TLfDI erfolgt ist. Mit der von privaten Anbietern angebotenen Identifikationskarte sollen ankommende und bereits hier lebende Flüchtlinge besser erfasst und z. B. die Essenausgabe,

der Zugang zu den Unterkünften, die Beantragung von Leistungen geregelt werden. Dem TLfDI war die Verwendung solcher Karten in den Thüringer Kommunen nicht bekannt. Diese Problematik ergab sich lediglich in wenigen anderen Bundesländern.
Allerdings gab es zu diesem Zeitpunkt erste Überlegungen zur Einführung einer elektronischen Gesundheitskarte für Asylbewerber in Thüringen. Nach dem bis dahin üblichen Verfahren mussten Asylbewerber vor einer medizinischen Behandlung einen Behandlungsschein bei der zuständigen Sozialbehörde beantragen. Die Behörde entschied dann darüber, ob z. B. ein Arztbesuch gerechtfertigt war und übernahm anschließend die Kosten für die erbrachte medizinische Leistung. Mit der Änderung des § 264 Sozialgesetzbuch (SGB) Fünftes Buch (V) hat der Gesetzgeber entschieden, dass die Krankenkassen zur Übernahme der Krankenbehandlung für Empfänger von Gesundheitsleistungen nach §§ 4 und 6 Asylbewerberleistungsgesetz (AsylbLG) verpflichtet werden können. Die Landkreise und kreisfreien Städte mussten hierfür eine Vereinbarung schließen. Dabei ist die Ausgabe der elektronischen Gesundheitskarte (eGK) durch die Krankenkassen möglich.
Der TLfDI bat das Thüringer Ministerium für Migration, Justiz und Verbraucherschutz (TMMJV) um Stellungnahme zum Stand der Einführung und zu den Funktionalitäten einer eGK. Das TMMJV erläuterte in seiner Antwort, dass die eGK im Auftrag der jeweiligen Krankenkasse hergestellt und ausgeben werden, bislang aber noch keine eGK in Thüringen für Leistungsberechtigte nach den §§ 4 und 6 AsylbLG zum Einsatz gekommen war. Dies erfolgte erst Anfang des Jahres 2017. Dann sollte auch die „Rahmenvereinbarung zur Übernahme der Krankenbehandlung für nicht Versicherungspflichtige gegen Kostenerstattung nach § 264 Abs. 1 SGB V i. V. m. den §§ 1, 1a sowie 4 und 6 AsylbLG im Freistaat Thüringen“ in Kraft getreten sein, der alle Landkreise und kreisfreien Städte der Rahmenvereinbarung beitreten sollen. Das TMMJV bat den TLfDI, die Rahmenvereinbarung auf datenschutzrechtliche Bedenken zu prüfen.
Nach Prüfung der Rahmenvereinbarung erklärte der TLfDI, dass keine datenschutzrechtlichen Einwände bestehen, sofern das in § 5 Abs. 3 Buchstabe a der Rahmenvereinbarung erwähnte separate Institutionskennzeichen, das den Betroffenen als Asylbewerber ausweist, nur der Krankenkasse zu Abrechnungszwecken und nicht Dritten gegenüber erkennbar ist. Zudem wies der TLfDI das

TMMJV auf § 67a Abs. 3 SGB Zehntes Buch (X) hin. Danach ist der Betroffene über die Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung und die Identität der verantwortlichen Stelle zu unterrichten. Werden die Sozialdaten beim Betroffenen aufgrund einer Rechtsvorschrift erhoben, die zur Auskunft verpflichtet, oder ist die Erteilung der Auskunft Voraussetzung für die Gewährung von Rechtsvorteilen, ist der Betroffene hierauf sowie auf die Rechtsvorschrift, die zur Auskunft verpflichtet und die Folgen der Verweigerung von Angaben hinzuweisen. Der TLfDI empfahl dringend die Erstellung eines Hinweisblattes, das den Asylbewerber über die entsprechende Vorschrift informiert.
Das TMMJV antwortete darauf, dass bei Vereinbarungen nach § 264 Abs. 1 S. 1 SGB V die elektronische Gesundheitskarte die Angabe zu enthalten hat, dass es sich um einen Empfänger von Gesundheitsleistungen nach den §§ 4 und 6 AsylbLG handelt. Diese Regelung in Verbindung mit der Vereinbarung der Übernahme der Krankenbehandlung nach § 264 Abs. 1 SGB V soll gewährleisten, dass der besondere Schutzstatus des benannten Personenkreises auf der eGK hinterlegt ist. Damit soll für den Arzt und nicht für Dritte erkennbar sein, dass bei dem betreffenden Patienten ein eingeschränkter Leistungsanspruch zu beachten ist.
Das TMMJV übersandte zudem das Hinweisschreiben, mit dem die betroffenen Personen auf die Erhebung, Verarbeitung und Nutzung von Daten im Zusammenhang mit der Gesundheitsversorgung nach dem AsylbLG sowie der Ausgabe der elektronischen Gesundheitskarte aufmerksam gemacht werden sollen. Es wurde beabsichtigt, das Hinweisblatt an die in den Landkreisen und kreisfreien Städten bereits untergebrachten Leistungsberechtigten zu übermitteln. Die Ausführungen in diesem Hinweisschreiben wurden kurz und klar gefasst, um die Verständlichkeit der Informationen bei den Betreffenden zu gewährleisten. Insoweit ist auf eine umfassende Erläuterung von Rechtsvorschriften bzw. von Bestimmungen der Rahmenvereinbarung zur Einführung der eGK verzichtet worden. Dies wurde mit der Beauftragten für Integration, Migration und Flüchtlinge beim TMMJV abgestimmt. Der TLfDI hatte gegen die Gestaltung des Hinweisblattes in der beschriebenen Form keine durchgreifenden datenschutzrechtlichen Bedenken.

Eine elektronische Identifikationskarte für Asylbewerber kommt in Thüringen nicht zum Einsatz. Gegen die eingeführte elektronische

Gesundheitskarte für Leistungsberechtigte nach den §§ 4 und 6 AsylbLG bestehen nunmehr keine datenschutzrechtlichen Bedenken. Ein separates Institutionskennzeichen, das den Betroffenen als Asylbewerber ausweist, darf nur der Krankenkasse zu Abrechnungszwecken und nicht Dritten, beispielsweise dem behandelnden Arzt, erkennbar sein.

6.34 Wenn das Jugendamt Erkundigungen einzieht

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) wurde im Berichtszeitraum von einer Pflegemutter, die ihren Beruf als Ärztin vorübergehend nicht ausübte, wegen eines datenschutzrechtlichen Problems mit dem Jugendamt kontaktiert. Sie wurde von der Landesärztekammer angeschrieben, die mitteilte, dass das Jugendamt Erkundigungen über sie eingezogen hatte. Der TLfDI wandte sich an das Jugendamt und bat um Stellungnahme zum Sachverhalt, denn nach § 67a Abs. 2 Satz 1 Sozialgesetzbuch (SGB) Zehntes Buch (X) sind Sozialdaten ebenso wie nach den allgemeinen Bestimmungen des § 19 Abs. 2 Thüringer Datenschutzgesetz (ThürDSG) grundsätzlich beim Betroffenen zu erheben. Ohne seine Mitwirkung dürfen sie nur in den gesetzlich genannten Ausnahmefällen erhoben werden.
Das Jugendamt legte dar, dass im Rahmen der Erteilung der Pflegeerlaubnis nach § 44 Abs. 1 Sozialgesetzbuch (SGB) Achtes Buch (VIII) als maßgeblich angesehen worden war, dass die Beschwerdeführerin nicht mehr als Ärztin praktiziere. Daran habe man nunmehr Zweifel gehabt, nachdem sie sich jüngst gegenüber der Lokalpresse auf ihre berufliche Qualifikation als Fachärztin berufen hatte, um zu belegen, dass sie einschätzen könne, was das Kind benötige. Aufgrund des Artikels in der Lokalzeitung habe man der Frage nachgehen müssen, ob die Beschwerdeführerin als Ärztin praktiziere und vielleicht auch ihr Pflegekind unerlaubt therapiere.
Rechtsgrundlage für die Anfrage der Mitgliedschaft der Beschwerdeführerin bei der Landesärztekammer sei der § 67a Abs. 2 Satz 2 Nr. 2b) Buchstabe a) SGB X. Demnach dürfen Sozialdaten bei anderen Stellen ohne die Mitwirkung des Betroffenen (nur) erhoben werden, wenn die Aufgaben ihrer Art nach eine Erhebung bei anderen Stellen erforderlich machen. Die Erforderlichkeit der Datenerhebung habe sich aus § 44 Abs. 3 Satz 2 SGB VIII ergeben. Danach ist die Pflegerlaubnis für eine Pflegeperson durch das Jugendamt zurückzu-

nehmen oder zu widerrufen, wenn das Wohl des Kindes in der Pflegestelle gefährdet ist und die Pflegeperson nicht bereit ist, die Gefährdung abzuwenden. Bei der Durchführung einer ärztlichen Therapie am Kind, ohne dass der Arzt die berufsrechtlichen Voraussetzungen erfüllt, bestehe die Möglichkeit, dass das Persönlichkeitsrecht des Kindes und seine körperliche Integrität verletzt werden.
Der TLfDI sah jedoch eine Aufgabe, die ihrer Art nach eine Erhebung bei anderen Personen oder Stellen erforderlich macht, noch nicht. Selbst wenn die Beschwerdeführerin als Ärztin tätig gewesen wäre, konnte aus der Sicht des TLfDI daraus nicht zwingend abgeleitet werden, dass sie als Ärztin ihre Pflegetochter behandle. Nach der Einschätzung des TLfDI bestand die Option einer Erhebung bei der Betroffenen. Erst wenn nach einer entsprechenden Befragung für das Jugendamt noch Zweifel bestanden hätten oder konkrete Angaben zu überprüfen gewesen wären, wäre eine Abfrage bei der Landesärztekammer infrage gekommen. Allerdings hätte man dann auch die Geeignetheit der Abfrage überprüfen müssen. Allein die Mitgliedschaft bei der Landesärztekammer kann nicht belegen, dass die Beschwerdeführerin unerlaubterweise eine ärztliche Behandlung an ihrer Pflegetochter durchführt.
Um die Sache endgültig aufzuklären, hielt der TLfDI einen Termin vor Ort, verbunden mit der Einsicht in die Pflegeakte beim Jugendamt, für erforderlich. Rechtsgrundlage hierfür ist § 37 ThürDSG.
Die Akteneinsicht ergab, dass das Landratsamt per E-Mail bei der Thüringer Landesärztekammer nachfragte, ob die Beschwerdeführerin Mitglied der Landesärztekammer sei. Dies bestätigte die Landesärztekammer unter Hinweis auf § 2 Abs. 1 Thüringer Heilberufsgesetz. Dass diese Anfrage letztendlich inhaltlich nicht zur Erhellung beitragen konnte und keinen Beitrag zur Frage leistete, ob die Pflegschaft widerrufen werden kann oder muss, und damit weder erforderlich noch zulässig war, bestätigte die Auffassung des TLfDI.
Im Hinblick darauf, dass beim Versand von personenbezogenen Daten per E-Mail bekanntermaßen die Vertraulichkeit nicht sichergestellt ist, wenn – wie vorliegend – keine geeignete Verschlüsselungstechnik zur Verfügung steht, wurde die Vorgehensweise nach § 39 i. V. m. § 9 Abs. 2 Nr. 1 ThürDSG mangels Sicherstellung der Vertraulichkeit beanstandet. Zur Behebung des beanstandeten Mangels wies das Landratsamt in einer Dienstanweisung die Mitarbeiterinnen und Mitarbeiter des Hauses an, dass personenbezogene oder sonstige schützenswerte Daten aus Datenschutzgründen nicht per E-

Mail übermittelt werden dürfen, da die Vertraulichkeit bei der Übermittlung nicht gewährleistet ist.

Nach § 67a Abs. 2 Satz 1 SGB X sind Sozialdaten grundsätzlich beim Betroffenen zu erheben; ohne seine Mitwirkung dürfen sie nur in den gesetzlich genannten Ausnahmefällen erhoben werden. Zur Gewährleistung der Vertraulichkeit der Daten sind nach § 9 Abs. 2 Nr. 1 ThürDSG die erforderlichen und geeigneten Maßnahmen zu treffen, die eine unbefugte Kenntnis ausschließen.

6.35 Persönliche Daten vor Gericht

Ein Bürger beschwerte sich beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) darüber, dass ein öffentliches Energieversorgungsunternehmen vor einem Thüringer Gericht in einem Klageverfahren seine persönlichen Energieverbrauchswerte vorgetragen habe, wobei nach Auffassung des Beschwerdeführers davon auszugehen sei, dass es sich dabei um einen Verstoß gegen datenschutzrechtliche Vorschriften handle, da die o. g. Daten nur zum Zwecke der Abrechnung verwendet werden dürften.
Der TLfDI teilte dem Beschwerdeführer mit, dass das Energieversorgungsunternehmen die ihn betreffenden Daten entweder auf prozessrechtliche Anordnung des Gerichts oder in freier Beweisführung vorgetragen habe, um die Rechte der Gegenpartei zu vertreten. Insoweit sei § 2 Absatz 6 Thüringer Datenschutzgesetz (ThürDSG) maßgeblich. Danach gelten für Gerichte wegen der verfassungsrechtlich vorgegebenen richterlichen Unabhängigkeit die §§ 10 und 11 sowie der fünfte Abschnitt des ThürDSG nur, soweit sie in eigenen Verwaltungsangelegenheiten, nicht jedoch, wie in diesem Falle, in einer prozessualen Angelegenheit tätig werden.
Die Folge sei, dass das Recht des Beschwerdeführers, den TLfDI gem. § 11 ThürDSG anzurufen, hier im Ergebnis nicht greife. Das bedeutet, dass dem Beschwerdeführer zwar niemand verwehren könne, den TLfDI anzurufen, jedoch darf der TLfDI wegen der o. g. gesetzlichen Gründe in dieser Angelegenheit nicht tätig werden. Ansonsten würde der TLfDI gegen das ThürDSG verstoßen und die richterliche Unabhängigkeit verletzen. Damit sei der TLfDI im Ergebnis in diesem konkreten Beschwerdefalle nicht zur Überprüfung befugt.

Das ThürDSG erlaubt dem TLfDI die Kontrolle der Gerichte nur, soweit sie in eigenen Verwaltungsangelegenheiten tätig werden, § 2 Abs. 6 ThürDSG. Insoweit ist der TLfDI nicht befugt, die Verarbeitung personenbezogener Daten im Rahmen der Rechtsprechung zu überprüfen.

6.36 Herausgabe der Liste von Gewerbesteuerzahlern an den Bürgermeister – datenschutzrechtlich zulässig?

Ein Stadtkämmerer wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und teilte mit, dass er Bedenken hätte, dem Wunsch seines Bürgermeisters nachzukommen und diesem eine Liste mit den 10 bis 15 besten Gewerbesteuerzahlern auszuhändigen. Diese Liste benötigte der Bürgermeister für Gespräche über die künftige Gewerbesteuerentwicklung, in denen er erfragen wollte, welche Unterstützung die Stadt geben könne.
Der Kämmerer äußerte gegenüber dem TLfDI Bedenken hinsichtlich § 30 Abgabenordnung (AO). In diesem Paragrafen wird das Steuergeheimnis allgemein geregelt, insbesondere für die Finanzämter, aber auch für alle anderen Behörden, die Steuergesetze anwenden. Laut Kommentierung zu dieser Regelung könne eine unbefugte Offenbarung auch gegeben sein, wenn der für die Besteuerung zuständige Finanzbeamte Verhältnisse eines Steuerpflichtigen ohne steuerlichen Anlass einem Kollegen bekannt gäbe.
Diese Bedenken wurden vom TLfDI nicht geteilt.
Gemäß § 29 Abs. 3 Thüringer Kommunalordnung (ThürKO) ist der Bürgermeister oberste Dienstbehörde der Beamten der Gemeinde. Er ist Vorgesetzter und Dienstvorgesetzter der Gemeindebediensteten. Gemäß § 28 ThürKO ist der Bürgermeister selbst Beamter der Gemeinde.
In der Kommentierung zur AO (Kommentar von Klein, AO-Kommentar, 7. Auflage, § 30, Rdn. 60) wird die Auffassung vertreten, dass die Weitergabe von Daten innerhalb der Verwaltung an die zuständige Stelle der Finanzbehörde (einschließlich der Aufsichtsbehörde) zwecks ordnungsgemäßer Erledigung des Verfahrens schon begrifflich nicht als Offenbaren steuerlicher Verhältnisse angesehen werden könne.

Als Dienstvorgesetzter kann der Bürgermeister Weisungen erteilen, wie die Besteuerung zu erfolgen hat (§ 35 Beamtenstatusgesetz [BeamtStG], wogegen Beamte, falls die Weisungen rechtswidrig sein sollten, nach § 36 Abs. 2 BeamtStG vorgehen könnten). Insofern muss ein Bürgermeister, um diese Funktion ausüben zu können, auch in der Lage sein, die entsprechenden Akten einzusehen. Außerdem erhielt der Bürgermeister, da er die Posteingänge zur Kenntnis nahm, insoweit auch Kenntnis der eingehenden Messbetragsbescheide des Finanzamtes. Ein „Offenbaren" im Sinne des § 30 AO scheidet aber aus, wenn die Verhältnisse dem Betreffenden schon bekannt sind (BGH, NJW 63, 2120). Der Bürgermeister ist als Beamter der Stadt selbstverständlich auch an das Steuergeheimnis gebunden. Die Abfrage der Daten zum Zwecke der Beurteilung der künftigen Gewerbesteuerentwicklung fällt schließlich auch in den Zuständigkeitsbereich des Bürgermeisters, da dieser für die Finanzplanung der Gemeinde nach § 62 ThürKO zuständig ist. Die Kenntnis der Steuerdaten war auch deshalb für den Bürgermeister erforderlich.

Das Steuergeheimnis gilt nicht gegenüber Dienstvorgesetzten einer Behörde. Dienstvorgesetzte in die Kenntnis der Vorgänge „ihrer Behörde" zu versetzen, stehen regelmäßig keine datenschutzrechtlichen Hindernisse entgegen. Ein Bürgermeister hat das Recht, von seinem Kämmerer die Gewerbesteuerdaten, einschließlich der Namen der Steuerpflichtigen, zu erfahren.

6.37 Manipulationen am USB-Stick einer Kindergartenmitarbeiterin?

Eine Beschwerdeführerin setzte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) darüber in Kenntnis, dass der Hauptamtsleiter einer Gemeinde auf ihrem privaten USB-Stick einen Ordner mit ihren personenbezogenen Daten sowie einen zweiten Ordner mit personenbezogenen Daten einer weiteren Person ohne ihre Einwilligung angelegt habe. Der o. g. USB-Stick habe sich während einer Unterredung zwischen der Beschwerdeführerin und dem Hauptamtsleiter in der Kindertagesstätte auf dem Dienst-Laptop des Trägers der Kindertagesstätte befunden. Die o. g. Manipulation sei erfolgt, nachdem die Beschwerdeführerin die Besprechung überstürzt verlassen habe. In dieser Zeit könne nur der Hauptamtsleiter Zugriff auf den Dienst-Laptop mit dem o. g.

USB-Stick gehabt haben. Die Beschwerdeführerin habe die Veränderung erst bemerkt, nachdem sie ihren persönlichen USB-Stick, den sie aus Versehen in der Kindertagesstätte zurückgelassen hatte, wieder an sich genommen hatte.
Da es sich bei dem geschilderten Sachverhalt ggf. um einen Verstoß gegen datenschutzrechtliche Bestimmungen in Form einer unzulässigen Datenverarbeitung handeln konnte, forderte der TLfDI die beteiligte Gemeinde auf, zu der Angelegenheit, insbesondere zum beabsichtigten Zweck der o. g. Datenverarbeitung und zur Rechtsgrundlage, auf der der Zugriff auf den USB-Stick und die damit verbundene Datenverarbeitung beruhte, im Einzelnen Stellung zu nehmen.
Der Bürgermeister der beteiligten Gemeinde widersprach der Sachverhaltsdarstellung der Beschwerdeführerin und führte aus, dass der Hauptamtsleiter keine personenbezogenen Daten vom Dienst-Laptop des Trägers der Kindertagesstätte gezogen habe.
Der TLfDI teile daraufhin der Beschwerdeführerin mit, dass in diesem Falle, in dem zwei plausible, sich jedoch widersprechende, Sachverhalte vorgetragen wurden und auch weitere Recherchen keine Aussicht auf Erfolg boten, es mit den Mitteln, die dem TLfDI zu Gebote stehen, so gut wie ausgeschlossen sei, den wirklichen Sachverhalt zweifelsfrei festzustellen, da dem TLfDI keine vergleichbaren gesetzlichen Befugnisse zur exakten Klärung des realen Sachverhalts, wie etwa der Staatsanwaltschaft, zur Verfügung stehen. Insofern sah der TLfDI die Beschwerdeangelegenheit als erledigt an.

Manchmal kann das Ergebnis einer Beschwerdeangelegenheit den TLfDI nicht befriedigen. Etwa dann, wenn plausible, sich jedoch widersprechende Sachverhalte vorgetragen wurden und dem TLfDI keine weiteren erfolgversprechenden Recherchemöglichkeiten zur Verfügung stehen, um einen datenschutzrechtlichen Sachverhalt voll und ganz sowie zur Zufriedenheit aller Beteiligten aufzuklären.

6.38 Keine Daten bei Hundebiss?

Die Datenschutzbeauftragte einer Kommune wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) mit der Frage, ob einer Antragstellerin, die vortrug, durch einen Hund geschädigt worden zu sein, Auskunft darüber gegeben werden könne, wer der Hundehalter sei.

Diese Frage konnte der TLfDI im Sinne der geschädigten Antragstellerin beantworten. Prinzipiell unterliegen Steuerdaten dem Steuergeheimnis. Allerdings macht das Thüringer Kommunalabgabengesetz (ThürKAG) in § 15 Abs. 1, Nr. 1, Buchstabe c), bb) ThürKAG die Ausnahme, dass bei der Hundesteuer in Schadensfällen Auskunft über Namen und Anschrift des Hundehalters an Behörden und Schadensbeteiligte gegeben werden darf. Daher durfte aus diesem Grunde der Antragstellerin die Auskunft gegeben werden.

Im Schadensfall dürfen die Kommunalbehörden Hundehalterdaten nach § 15 Abs.1, Nr. 1, c), bb) ThürKAG an Dritte übermitteln.

6.39 Nichtlöschbarkeit personenbezogener Daten im Internet

Eine Beschwerdeführerin teilte dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) mit, dass sie im Herbst 2015 mittels einer Eingabemaske auf der Homepage der Stadt Eisenach zu einer Stellenausschreibung angefragt habe, wobei sie ihren Namen, ihre E-Mail-Adresse und andere personenbezogene Daten angegeben habe. Ende 2015 habe sie festgestellt, dass die o. g. Maske mit ihren personenbezogenen Daten im Internet angezeigt werde, wenn dort ihr Name gesucht wird. Nachfolgend habe die EDV-Abteilung der Stadt Eisenach die o. g. Daten auf Bitten der Beschwerdeführerin entfernt. Jedoch sei im Sommer 2016 erneut ein solcher Datenabruf möglich gewesen. Auch ihre nachfolgende zweite Beschwerde bei der Stadt Eisenach habe zu keinem bleibenden Erfolg geführt, da o. g. Daten nunmehr seit Mitte März 2017 wieder abrufbar seien.
Der TLfDI teilte der Stadtverwaltung Eisenach mit, dass es sich nach seiner vorläufigen Beurteilung bei der o. g. Angelegenheit um einen Verstoß gegen datenschutzrechtliche Vorschriften handle und bat um Mitteilung, wie es zu einer solchen Offenbarung von personenbezogenen Daten im Internet kommen konnte, was die Stadtverwaltung konkret veranlasst habe bzw. beabsichtige zu tun, um eine Löschung der o. g. personenbezogenen Daten zu bewirken bzw. die Abrufbarkeit dieser Daten im Internet nunmehr dauerhaft auszuschließen und ob der Stadtverwaltung weitere Vorfälle dieser Art bekannt seien.
Daraufhin teilte die Stadtverwaltung Eisenach dem TLfDI mit, dass sie inzwischen eine neue Website ins Internet gestellt habe, die die Gewähr dafür biete, dass personenbezogene Daten im Internet nicht

mehr sichtbar seien. Daher seien auch die beschwerdegegenständlichen personenbezogenen Daten nunmehr nicht mehr abrufbar. Wie es zu den o. g. Vorfällen kam, könne jedoch nicht mehr nachvollzogen werden. Auch seien Vorfälle dieser Art der Stadtverwaltung nicht bekannt.

Das Beispiel zeigt, wie langwierig unter Umständen die Durchsetzung des informationellen Selbstbestimmungsrechts von Bürgern im Einzelfalle sein kann. Schließlich konnte der TLfDI letztendlich eine nachhaltige Löschung der personenbezogenen Daten im Internet bewirken, nachdem sich die Beschwerdeführerin zunächst mehrfach vergeblich an die verantwortliche Stelle gewandt hatte.

6.40 Weiterleitung einer Beschwerde-E-Mail von Behörde zu Behörde

Ein Bürger setzte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) darüber in Kenntnis, dass die Stadtverwaltung Artern seine E-Mail, die einen verschmutzten Radweg zum Gegenstand hatte, komplett an eine andere Behörde übermittelt hatte.
Daraufhin teilte der TLfDI der Stadtverwaltung Artern seine vorläufige Beurteilung der Angelegenheit mit, wonach es sich bei der Weiterleitung der Beschwerde-E-Mail um eine unzulässige Übermittlung personenbezogener Daten, hier in Form der Übermittlung der E-Mail-Adresse des Beschwerdeführers, handelte. Diese Wertung beruhe darauf, dass dieses konkrete Datum für die Bearbeitung der Beschwerde nicht erforderlich und eine geeignete Rechtsgrundlage für die Datenübermittlung an die andere Behörde nicht ersichtlich sei.
Zugleich bat der TLfDI die Stadtverwaltung Artern mitzuteilen, zu welchem Zweck die E-Mail komplett übermittelt wurde und auf welcher Rechtsgrundlage diese Übermittlung personenbezogener Daten erfolgte. Des Weiteren sollte die Stadtverwaltung Artern darauf hinwirken, dass die andere Behörde die E-Mail mit den personenbezogenen Daten der Beschwerdeführers löscht und dem TLfDI mitteilen, wie der Vorfall in der Stadtverwaltung Artern ausgewertet wurde, um Verstöße gegen datenschutzrechtliche Vorschriften in ähnlichen Fällen künftig auszuschließen.

Daraufhin teilte die Stadtverwaltung Artern mit, dass sie die Rechtsauffassung des TLfDI teile und ihre Mitarbeiter angewiesen habe, den Datenschutz umfassend einzuhalten. Auch habe die beteiligte Behörde die beschwerdegegenständliche E-Mail zwischenzeitlich auf Bitten der Stadtverwaltung Artern vollständig gelöscht.

Rechtssicherheit und Datenschutz gehen vor Schnelligkeit! Dieser Fall zeigt wieder einmal, dass jede Verarbeitung personenbezogener Daten nur dann zulässig ist, wenn das Thüringer Datenschutzgesetz (ThürDSG) oder ein anderes Gesetz dies erlaubt oder anordnet oder soweit der Betroffene hierin eingewilligt hat, § 4 Abs. 1 ThürDSG. Das gilt auch für die Übermittlung einer privaten E-Mail-Adresse als personenbezogenes Datum.

6.41 Datenübermittlung gem. § 9 ThürUIG – TLfDI nicht zuständig

Im Mai 2017 wandte sich ein Bürger und Firmeninhaber an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und bat um Überprüfung und Mitteilung, ob bzw. inwiefern das Landratsamt (LRA) Schmalkalden-Meiningen personenbezogene Daten des Firmeninhabers nach § 3 Thüringer Umweltinformationsgesetz (ThürUIG) an eine dritte Person übermitteln darf, wenn diese um die Daten gebeten hat. Gegenüber dem LRA hatte der Firmeninhaber im Zuge der Anhörung nach § 9 ThürUIG der Herausgabe dieser Daten widersprochen.
Der TLfDI teilte dem Beschwerdeführer mit, dass das Landratsamt (LRA) gemäß § 9 ThürUIG generell prüfen muss, ob durch die Bekanntgabe der Informationen personenbezogene Daten offenbart und dadurch schutzwürdige Interessen der Betroffenen beeinträchtigt werden. In einem solchen Falle müsste das LRA den Antrag auf Übermittlung der Daten ablehnen.
Allerdings war der TLfDI nicht für das ThürUIG und dessen Ausführung im konkreten Fall zuständig, sodass die Angelegenheit vom TLfDI rechtlich nicht kontrolliert werden konnte.

Sofern mit der Bekanntgabe von Informationen personenbezogene Daten offenbart und dadurch schutzwürdige Interessen der Betroffenen beeinträchtigt werden, darf eine Behörde diese Informationen nicht an Dritte weitergeben, auch nicht auf der Grundlage von § 9

ThürUIG. Der TLfDI ist aber nicht zuständig, mögliche Verstöße gegen das ThürUIG zu kontrollieren.

6.42 Ordnungswidrigkeitsverfahren gegen Stadtratsmitglieder

Ein Rechtsanwalt setzte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) darüber in Kenntnis, dass eine Person in ihrer Funktion als Stadtratsmitglied eine Ordnungswidrigkeit nach § 43 Thüringer Datenschutzgesetz begangen habe.
Das Thüringer Innenministerium (TIM) steht unter Berufung auf § 8 Abs. 1 und 2 der „Thüringer Verordnung zur Bestimmung von Zuständigkeiten im Geschäftsbereich des Innenministeriums vom 15. April 2008“, wonach die Verwaltungsbehörde für die Verfolgung und Ahndung von Ordnungswidrigkeiten zuständig ist, der der Vollzug derjenigen Rechtsvorschriften obliegt, gegen die sich der Verstoß richtet, auf dem Standpunkt, dass, soweit Personen als Amtsträger handeln, die Kommune selbst für die Ahndung von Ordnungswidrigkeiten zuständig ist. Dies stellt eine problematische Rechtslage da, da die Kommune in der Regel in einen Interessenkonflikt bei dem Vorgehen gegen Ratsmitglieder kommt.
Der TLfDI teilte dem Beschwerdeführer mit, dass er in der o. g. Beschwerdeangelegenheit aufgrund der geltenden Rechtslage für die Verfolgung der mutmaßlichen Ordnungswidrigkeit unzuständig sei.
In der Sache selbst prüfte der TLfDI, ob ein datenschutzrechtlicher Verstoß vorlag. Inhaltlich ging es um die mutmaßliche Weitergabe von Daten aus einem Vorlagepapier für eine Stadtratssitzung. Diese Weitergabe konnte nicht belegt werden, sodass eine Beanstandung durch den TLfDI nicht erfolgte.

Die Zuständigkeit zur Verfolgung von Ordnungswidrigkeiten sollte von den Kommunen dem TLfDI zur Vermeidung von Interessenkonflikten übertragen werden.

6.43 Was weiß die Stadtverwaltung?

Ein Bürger hatte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) gewandt, weil er sich in seinem Persönlichkeitsrecht beeinträchtigt sah. Konkret teilte er mit, dass er von der betreffenden Stadtverwaltung ein Schreiben

zu einer Ordnungswidrigkeit („Falschparken“) erhalten habe. Dieses Schreiben habe im Briefkopf neben seinem Namen auch die Angabe seines Geburtsdatums, -namens und -orts enthalten. Darüber hinaus wollte er wissen, auf welche seiner personenbezogenen Daten die Stadtverwaltung überhaupt Zugriff hat.
Auf Nachfrage des TLfDI teilte die Stadtverwaltung mit, dass der Geburtstag, -name und der Geburtsort des Betroffen auf dem Anschreiben im Rahmen der ersten Halteranhörung im Ordnungswidrigkeitsverfahren angegeben werden, um eine zweifelsfreie Identifikation des Betroffenen zu ermöglichen und somit Verwechslungen, die Verfolgung Unbeteiligter und eine unzulässige Datenübermittlung an Dritte auszuschließen. Diese Daten erhalte die Stadtverwaltung auf entsprechende Kennzeichenanfrage beim Kraftfahrbundesamt nach § 35 Abs. 1 Nr. 3 Straßenverkehrsgesetz (StVG) zur Verfolgung von Ordnungswidrigkeiten. Insofern werden o. g. Daten (Geburtstag, -name und -ort) zur Identifikation und damit im Rahmen der Zweckbindung des § 43 Abs. 2 StVG genutzt.
Nachfolgend setzte der TLfDI den Beschwerdeführer darüber in Kenntnis, dass die betreffende Stadtverwaltung gemäß § 2 Abs. 1 der Thüringer Verordnung über Zuständigkeiten für die Verfolgung und Ahndung von Verkehrsordnungswidrigkeiten vom 21. April 1998 nach § 24 StVG für die Verfolgung geringfügiger Ordnungswidrigkeiten, die im ruhenden Verkehr festgestellt werden, zuständig ist. Weitere Zugriffe im Zusammenhang mit der Erfüllung der Aufgabe der Verfolgung von geringfügigen Ordnungswidrigkeiten im ruhenden Verkehr habe die Stadtverwaltung auch auf die Daten des Melderegisters, sofern dies im Rahmen der Ermittlung des Verantwortlichen im Ordnungswidrigkeitenverfahren notwendig ist. Dies ist z. B. im Falle lückenhafter bzw. widersprüchlicher Halterangaben zum verantwortlichen Fahrzeugführer der Fall. Die Ermächtigungsgrundlage hierfür ergibt sich aus § 37 Abs. 1 Bundesmeldegesetz (BMG).
Weiterhin teilte der TLfDI dem Beschwerdeführer mit, dass die Antwort auf die Frage, auf welche personenbezogenen Daten zu seiner Person die Stadtverwaltung Zugriff hat, davon abhängt, in welchem seiner Lebensbereiche die Stadtverwaltung Dienstleistungen für den Beschwerdeführer erbringt bzw. die Erfüllung gesetzlicher Pflichten von ihm fordere. Dies wiederum setze die Kenntnis einer Vielzahl seiner verwaltungsrelevanten konkreten Lebensumstände voraus, über die ggf. nur nahestehende Personen verfügen. Auch sei im Thüringer Datenschutzgesetz (ThürDSG) eine solche

pauschale Auskunft zu allen über eine Person bei einer öffentlichen Stelle gespeicherten Daten grundsätzlich nicht vorgesehen. Im Ergebnis stellte der TLfDI keinen Verstoß gegen datenschutzrechtliche Bestimmungen fest.

Stadtverwaltungen können im Rahmen der Verfolgung geringfügiger Ordnungswidrigkeiten im ruhenden Verkehr Daten des Fahrzeughalters, die beim Kraftfahrtbundesamt und im Melderegister gespeichert werden, verarbeiten. Der zuständigen Behörde ist es in diesem Zusammenhang erlaubt, im Anschreiben neben Name und Anschrift auch die Daten Geburtstag, -name und Geburtsort zur Identifikation des Betroffenen zu verwenden.
Eine pauschale Auskunft zu allen über eine Person bei einer öffentlichen Stelle gespeicherten Daten sieht das Thüringer Datenschutzgesetz nicht vor.

6.44 Anfrage zur etwaigen Anonymität von Zeugen

Ein Bürger erkundigte sich beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), ob die Anonymität eines Zeugen im Falle einer Anzeige einer Ordnungswidrigkeit gewahrt werden könne. Hintergrund der Anfrage war die Befürchtung, dass sich ein gewaltbereiter Täter im Nachhinein an dem Zeugen rächen könnte.
Der TLfDI teilte dem Bürger mit, dass ohne Kenntnis seines Einzelfalls keine rechtlich zuverlässige Antwort zu der aufgeworfenen Frage, ob und unter welchen Voraussetzungen die Anonymität eines Informanten gewahrt werden muss, möglich ist und wies auf den Beitrag 5.26 „Bleibt der Informant anonym?“ im 10. Tätigkeitsbericht des TLfDI im öffentlichen Bereich, S. 92 bis 95 auf der Internetseite des TLfDI hin. Darin äußerte sich der TLfDI zu der Kernfrage des Bürgers u. a. wie folgt:
„Im Ordnungswidrigkeitenverfahren ist das Recht auf Akteneinsicht des Betroffenen in § 49 Abs. 1 Ordnungswidrigkeitengesetz (OWiG) speziell geregelt. Danach kann die Verwaltungsbehörde dem Betroffenen Einsicht in die Akten unter Aufsicht gewähren, soweit nicht überwiegende schutzwürdige Interessen Dritter entgegenstehen. Dies ist von Amts wegen zu prüfen. Die Verfolgungsbehörde hat einen Ermessensspielraum, ob sie den Namen und die Anschrift des Zeugen bzw. Anzeigenden in Ordnungswidrigkeitenverfahren

angibt oder dies unterlässt. Hierbei hat sie das Datenschutzinteresse des Zeugen gegen das Informationsinteresse des Betroffenen abzuwägen. Hier gelten die gleichen Grundsätze wie zu § 29 Thüringer Verwaltungsverfahrensgesetz. Ein zu erwartendes Bußgeld setzt in aller Regel die Kenntnis der Zeugen voraus. Im Bußgeldverfahren ist es deshalb erforderlich, dass im Anhörungsschreiben der Name und der Wohnort des Zeugen benannt werden. Auf die Angabe der vollständigen Anschrift des Zeugen kann allerdings verzichtet werden. Auf Anfrage oder durch Akteneinsichtnahme steht sie jedoch dem Betroffenen zur Verfügung. Die Abwägung zwischen den datenschutzrechtlichen Interessen der Zeugen und dem Informationsinteresse der Betroffenen führt in diesem Fall zur Zurückstellung der Zeugenbelange.
Zeugen müssen hinnehmen, dass der angezeigten Person ihre Identifikationsdaten (Name und Wohnort) sowie der Gegenstand der Zeugenaussage bekannt werden. Ausnahmen hiervon sind nur bei besonderer Schutzbedürftigkeit der Zeugen zu machen. Wenn Anhaltspunkte dafür vorliegen, dass der Beschuldigte gewaltsam reagieren könnte oder bei besonderer Schutzbedürftigkeit des Zeugen ist das Recht auf Akteneinsicht zu verwehren und von der damit verbundenen Offenbarung personenbezogener Daten des Anzeigenerstatters bzw. Zeugen abzusehen."
Nach § 46 Abs. 1 OWiG gelten für Bußgeldverfahren, soweit das OWiG nichts anderes bestimmt, sinngemäß die Vorschriften der allgemeinen Gesetze über das Strafverfahren, namentlich der Strafprozessordnung (StPO), des Gerichtsverfassungsgesetzes und des Jugendgerichtsgesetzes. Nach Göhler, Kurzkommentar Ordnungswidrigkeitengesetz, 17. Auflage Randnummer 1, S. 364 finden sich die im OWiG anzuwendenden Bestimmungen der StPO, darunter § 68 StPO, im Anhang A 2 des OWiG. Infolgedessen sind folgende Regelungen des § 68 Abs. 2 bis 5 StPO zur Anonymität bzw. zum Schutz von Zeugen sinngemäß auch auf Bußgeldverfahren vor Amtsgerichten anzuwenden:
„(2) Einem Zeugen soll zudem gestattet werden, statt des Wohnortes seinen Geschäfts- oder Dienstort oder eine andere ladungsfähige Anschrift anzugeben, wenn ein begründeter Anlass zu der Besorgnis besteht, dass durch die Angabe des Wohnortes Rechtsgüter des Zeugen oder einer anderen Person gefährdet werden oder dass auf Zeugen oder eine andere Person in unlauterer Weise eingewirkt werden wird. In der Hauptverhandlung soll der Vorsitzende dem Zeugen bei

Vorliegen der Voraussetzungen des Satzes 1 gestatten, seinen Wohnort nicht anzugeben.
(3) Besteht ein begründeter Anlass zu der Besorgnis, dass durch die Offenbarung der Identität oder des Wohn- oder Aufenthaltsortes des Zeugen Leben, Leib oder Freiheit des Zeugen oder einer anderen Person gefährdet wird, so kann ihm gestattet werden, Angaben zur Person nicht oder nur über eine frühere Identität zu machen. Er hat jedoch in der Hauptverhandlung auf Befragen anzugeben, in welcher Eigenschaft ihm die Tatsachen, die er bekundet, bekannt geworden sind.
(4) Liegen Anhaltspunkte dafür vor, dass die Voraussetzungen der Absätze 2 oder 3 vorliegen, ist der Zeuge auf die dort vorgesehenen Befugnisse hinzuweisen. Im Fall des Absatzes 2 soll der Zeuge bei der Benennung einer ladungsfähigen Anschrift unterstützt werden. Die Unterlagen, die die Feststellung des Wohnortes oder der Identität des Zeugen gewährleisten, werden bei der Staatsanwaltschaft verwahrt. Zu den Akten sind sie erst zu nehmen, wenn die Besorgnis der Gefährdung entfällt.
(5) Die Absätze 2 bis 4 gelten auch nach Abschluss der Zeugenvernehmung. Soweit dem Zeugen gestattet wurde, Daten nicht anzugeben, ist bei Auskünften aus und Einsichtnahmen in Akten sicherzustellen, dass diese Daten anderen Personen nicht bekannt werden, es sei denn, dass eine Gefährdung im Sinne der Absätze 2 und 3 ausgeschlossen erscheint.“

Von einer Offenbarung personenbezogener Daten eines Anzeigenerstatters bzw. Zeugen ist abzusehen, wenn Anhaltspunkte dafür sprechen, dass der Beschuldigte gewaltsam reagieren könnte oder bei besonderer Schutzbedürftigkeit des Zeugen.

6.45 Foto von der Teilnehmerliste einer Bürgerversammlung: Was macht der Bürgermeister?

Im Februar 2017 erreichte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) die Beschwerde einer Bürgerin, dass in ihrer Gemeinde der Datenschutz massiv verletzt worden sei. In einer vom Bürgermeister einberufenen Bürgerversammlung im November 2016 habe der ebenfalls eingeladene, jedoch nicht in der Gemeinde wohnende Geschäftsführer eines vor Ort ansässigen Unternehmens mit seinem Handy die vollständig

ausgefüllte Teilnehmerliste der Bürgerversammlung mit den handschriftlichen Namenszügen abfotografiert. Der Bürgermeister als Versammlungsleiter hatte dies offensichtlich nicht bemerkt, da von ihm keine Reaktion erfolgte. Die Bürgerin fragte beim TLfDI nach, ob es sich bei der Teilnehmerliste um ein amtliches Dokument handele, das dem Datenschutz unterliege und nicht in fremde Hände gelangen dürfe. Entgegen dem Willen der Bürgerin verfügte jetzt der Geschäftsführer über den Namenszug mit ihrer Unterschrift, ohne dass sie wüsste, was er damit tun werde.
Der TLfDI bat den Bürgermeister der Gemeinde um eine Stellungnahme zu dem vorgebrachten Sachverhalt. Der Bürgermeister teilte mit, dass sich jeder Teilnehmer der Einwohnerversammlung freiwillig in die ausgelegte Anwesenheitsliste habe eintragen können. Die Beschwerdeführerin hatte sich bereits auch bei ihm schriftlich darüber beschwert, dass eine Person die Anwesenheitsliste abfotografiert habe. Der Bürgermeister hatte der Beschwerdeführerin bereits mitgeteilt, dass er diese Handlung nicht bemerkt habe. Er legte dar, dass er es versäumt habe, zu der benannten Bürgerversammlung die technischen und organisatorischen Maßnahmen zum Schutz der personenbezogenen Daten zu sichern. Der Bürgermeister sicherte zu, dass dies in Zukunft nicht mehr vorkommen werde. Er werde zu den künftigen Einwohnerversammlungen keine Anwesenheitslisten mehr auslegen, sondern die Teilnehmer selbst notieren und die Liste zu den Akten heften. Dies hatte der Bürgermeister nach eigenen Angaben der Beschwerdeführerin bereits mitgeteilt. Der TLfDI begrüßte die künftige datenschutzrechtliche Absicherung von Einwohnerversammlungen durch den Bürgermeister.

Bei der Durchführung von Bürger- bzw. Einwohnerversammlungen muss der Bürgermeister dafür Sorge tragen, dass durch entsprechende technische und organisatorische Maßnahmen gem. § 9 Thüringer Datenschutzgesetz der Schutz von personenbezogenen Daten gewährleistet ist. Die betrifft insbesondere personenbezogene Daten der Versammlungsteilnehmer.

6.46 Beschwerde über die Übermittlung eines Wertgutachtens

Ein Bürger beschwerte sich beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) darüber, dass das Thüringer Landesverwaltungsamt (TLVwA) ein Wertgutachten

zu einem von seiner Familie bewohnten Grundstück mit den darin enthaltenen personenbezogenen Daten der Familienangehörigen an ein Landratsamt übermittelt habe.
Daraufhin forderte der TLfDI das TLVwA auf mitzuteilen, auf welcher Rechtsgrundlage die o. g. Datenübermittlung beruhte, zu welchem Zweck sie erfolgte und warum das Wertgutachten einschließlich der personenbezogenen Daten übermittelt wurde.
Im Ergebnis seiner Recherche fand der TLfDI heraus, dass die beschwerdegegenständliche Datenübermittlung des TLVwA an das Landratsamt der sozialrechtlichen Prüfung des Antrags des Beschwerdeführers auf Übernahme der Kosten der Unterkunft diente.
Im Einzelnen wurde festgestellt, dass der das Wertgutachten empfangende Landkreis als kommunaler Träger nach § 6a Sozialgesetzbuch II (SGB II) Leistungen nach dem SGB II erbringt. Das TLVwA hat die kommunalen Träger gem. § 2 Abs. 1 Satz 2, Abs. 2 Satz 1 des Thüringer Ausführungsgesetzes des SGB II (ThürAGSGB II) als Aufsichtsbehörde zu beraten und ihnen Informationen zur Festlegung von Sozialleistungen zu übermitteln.
Im Zusammenhang mit der Bearbeitung einer Petition des Beschwerdeführers zur Erbringung von Leistungen für Unterkunft und Heizung erfuhr das TLVwA, dass der Beschwerdeführer von seinem Neffen eine Wohnung gemietet hatte. Nach dem SGB II sind Mietverhältnisse auch zwischen Verwandten nicht ausgeschlossen. Da die vereinbarte Miethöhe jedoch in nicht unbedeutendem Umfang den Rahmen des Ortsüblichen überstieg, hatten die Sozialbehörden zu prüfen, ob die vertragliche Miethöhe gerechtfertigt war. Ansonsten wären dem Landkreis Kosten in Rechnung gestellt worden, die gar nicht entstanden waren und so den Antragsteller begünstigten. Bekannt wurde den Sozialbehörden in diesem Zusammenhang, dass der Neffe des Beschwerdeführers das betreffende Mietwohngrundstück per Zwangsversteigerung erworben hatte, wofür die Gerichte regelmäßig Wertgutachten erstellen lassen. Das TLVwA hat die Übersendung des betreffenden Wertgutachtens beim für die Zwangsversteigerung zuständigen Amtsgericht unter Darlegung der hierfür relevanten Gründe erbeten. Bei der Weiterleitung des Wertgutachtens vom Amtsgericht an das TLVwA handelte es sich um eine zulässige Datenübermittlung innerhalb des öffentlichen Bereichs gem. § 21 Thüringer Datenschutzgesetz (ThürDSG) in Verbindung mit § 20 Abs. 2 Nr. 4 ThürDSG zur Überprüfung von Angaben des Betroffenen, da die ortsunüblich hohe Miete einen Anhaltspunkt für eine

Unrichtigkeit der Angaben des Betroffenen darstellte. Das Wertgutachten enthielt u. a. Informationen über den Substanzwert des Gebäudes (z. B. in Bezug auf Wärmeschutz), die Aufschlüsse über die Angemessenheit von Heizkosten geben und zur Aufteilung und Größe des genutzten Wohnraums zur Beurteilung der gerechtfertigten Miethöhe.
Im Ergebnis stellte der TLfDI fest, dass das Wertgutachten mit den darin enthaltenen personenbezogenen bzw. -beziehbaren Daten für die Prüfung der angemessenen Miethöhe im Zusammenhang mit einem Antrag des Beschwerdeführers auf Übernahme der Kosten der Unterkunft und Heizung sowohl für das TLVwA – zur Bearbeitung der Petition des Beschwerdeführers – als auch für das betreffende Landratsamt – dort zur Bearbeitung beantragter Sozialleistungen des Beschwerdeführers – erforderlich war. Daher durfte das TLVwA auch im Rahmen seiner Beratungspflicht dem Landkreis das o. g. Wertgutachten zum Zwecke der Aufgabenwahrnehmung zur Verfügung stellen. Bei der Übermittlung des Wertgutachtens vom TLVwA an das Landratsamt handelte es sich um eine zulässige Datenübermittlung innerhalb des öffentlichen Bereichs gem. § 21 ThürDSG in Verbindung mit § 20 Abs. 2 Nr. 4 ThürDSG zur Überprüfung von Angaben des Betroffenen, da die ortsunüblich hohe Miete einen Anhaltspunkt für eine Unrichtigkeit der Angaben des Betroffenen darstellte.
Im Ergebnis teilte der TLfDI dem Beschwerdeführer mit, dass in dieser Beschwerdeangelegenheit keine Verstöße gegen datenschutzrechtliche Vorschriften festzustellen sind.

Im Rahmen seiner Beratungspflicht darf das Thüringer Landesverwaltungsamt kommunalen Trägern auch eigene Informationen für deren Aufgabenwahrnehmung übermitteln. Dies beinhaltet ggf. auch die Weiterleitung vollständiger Wertgutachten mit den darin enthaltenen personenbezogenen Daten zur Beurteilung von Mietverträgen im Zusammenhang mit der Ermittlung der Kosten der Unterkunft.

6.47 Betreibermodell für das Handyparken

Der Datenschutzbeauftragte einer Kommune begehrte vom Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) die Rechtsauskunft, ob es sich beim sogenannten

Mehrbetreibermodell des „Handyparkens“ um Auftragsdatenverarbeitung nach § 8 Thüringer Datenschutzgesetz (ThürDSG) handelt.
Das Modell kann wie folgt beschrieben werden:
Parker können ihre Parkgebühren anstelle der Bezahlung via Münzen am Parkscheinautomaten auch bargeldlos per Mobiltelefon zahlen. Das Mehrbetreibermodell ermöglicht das gleichzeitige Anbieten dieses Services durch mehrere Betreiber. Der Handyparker muss sich mithilfe einer Vignette – auf der rechten Seite der Windschutzscheibe angebracht – als ein solcher kennzeichnen. Der Parker kann sich frei für einen der Betreiber entscheiden und nach dem Abstellen des Fahrzeugs auf einem gebührenpflichtigen öffentlichen Stellplatz den Parkvorgang mit seinem Mobiltelefon per App, Anruf oder SMS bei seinem Betreiber starten. Er löst also einen digitalen Parkschein ganz ohne Bargeld. In puncto Parkzeit muss er sich dann nicht mehr, wie bisher am Parkscheinautomaten, im Vorfeld festlegen, sondern kann ganz nach Bedarf den Parkvorgang mit seinem Mobiltelefon stoppen oder verlängern.
Bei der Registrierung und zur Durchführung der Abrechnung werden seitens des Betreibers regelmäßig folgende Daten von den Nutzern erhoben: Name, Anschrift, Kontaktdaten, Kfz-Kennzeichen, Mobilfunknummer sowie je nach gewünschter Zahlungsweise Bankverbindung oder Kreditkartendaten, Login Daten, Beginn, Ende und Dauer eines Parkvorgangs, gewählte Parkzonen, abgerechnete Parkgebühr sowie Zahlungsverhalten.
Zu Kontrollzwecken können Kfz-Kennzeichen, Datum und Zeitraum des Parkvorgangs, Parkzone und abgerechnete Parkgebühr an die Gemeinde übermittelt werden.
Der gesamte Vorgang wird durch die vertragliche Einwilligung des Parkers abgedeckt.
Der Betreiber zahlt die bei ihm gebuchten Parkgebühren ohne Zuordnung zu einem bestimmten Nutzer monatlich an die Gemeinde, rechtlich liegt ein Vertrag (des Handyparker-Anbieters) zugunsten Dritter (der Gemeinde) nach § 328 Bürgerliches Gesetzbuch vor.
Eine Auftragsdatenverarbeitung im Sinne des § 8 ThürDSG kommt schon deshalb nicht in Betracht, weil der Betreiber die beim Nutzer erhobenen Daten verarbeitet, um seiner eigenen vertraglichen Verpflichtung gegenüber den Nutzern nachzukommen. Primärer Zweck der Datenverarbeitung ist die Erfüllung der vertraglichen Verpflichtungen. Die Zurverfügungstellung der Nutzerdaten zum Abruf durch die Gemeinde erfolgt in erster Linie in Erfüllung des Vertrages mit

dem Nutzer. Eine Auftragsdatenverarbeitung liegt nur vor, wenn der Auftraggeber nicht nur rechtlich, sondern zumindest prinzipiell auch tatsächlich in der Lage ist, dem Auftragnehmer jeden Arbeitsschritt vorzuschreiben und letztlich auch die korrekte Durchführung des Datenumgangs zu kontrollieren (Petri in: Simitis, Kommentar zum Bundesdatenschutzgesetz, 8. Auflage, § 11, Rd. 20). Die Gemeinde hat keine rechtliche Vereinbarung mit dem Betreiber. Demzufolge kann sie ihm auch keine Vorgaben rechtlicher oder tatsächlicher Art machen hinsichtlich des Datenumgangs. Der Betreiber hat ausschließlich ein Eigeninteresse an der Datenverarbeitung.
Die Kommune verarbeitet die Daten nach der Straßenverkehrsordnung (StVO) als Ordnungswidrigkeitenbehörde. Praktisch läuft es so ab, dass ein Mitarbeiter des Ordnungsamtes den entsprechenden Parkplatz auf das Bezahlen der Parkgebühren kontrolliert. Bei herkömmlichen Gebührenzahlern wird kontrolliert, ob ein Parkschein hinter der Windschutzscheibe hinterlegt ist und die Parkzeit noch nicht abgelaufen ist. Bei Teilnehmern am Handy-Parken gibt der Mitarbeiter die Kontrollnummer des Fahrzeuges ein und erhält so vom Betreiber die Auskunft, ob die Parkzeit beim Betreiber angemeldet wurde. Gegebenenfalls stellt der Mitarbeiter dann einen Verstoß gegen die Straßenverkehrsordnung fest und leitet ein Ordnungswidrigkeitsverfahren nach § 49 Abs. 1 Nr. 13 StVO ein.

Eine Auftragsdatenverarbeitung läge im Fall des Betreibermodells für das Handyparken nur vor, wenn der Auftraggeber nicht nur rechtlich, sondern zumindest prinzipiell auch tatsächlich in der Lage wäre, dem Auftragnehmer jeden Arbeitsschritt vorzuschreiben und letztlich auch die korrekte Durchführung des Datenumgangs kontrollieren zu können. Das war hier aber nicht der Fall. Daher liegt keine Auftragsdatenverarbeitung zwischen dem Handyparken-Betreiber und der Kommune vor. Die Kommune wird nur als Ordnungswidrigkeitenbehörde zur Kontrolle der StVO tätig.

6.48 Wasser- und Abwasserzweckverband will es wissen

Ein Kostenschuldner wandte sich an den Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und beschwerte sich darüber, dass der Zweckverband Wasser und Abwasser ihn aufforderte anzugeben, wie groß die Grundstücke und die bebauten Flächen seien, welche Dachform die Gebäude haben würden, ob und

in welchem Ausmaß eine Grundstücksversiegelung vorliege und welche Mengen Regenwasser aufgefangen und genutzt würden.
Nach § 19 Thüringer Datenschutzgesetz ist die Erhebung personenbezogener Daten zulässig, wenn ihre Kenntnis zur Erfüllung der Aufgaben der erhebenden Stellen erforderlich ist. Neben dieser allgemeinen datenschutzrechtlichen Ermächtigungsnorm finden noch die speziellen Ermächtigungsnormen des Thüringer Kommunalabgabengesetzes (ThürKAG) Anwendung: §§ 10, 12, 15 Abs. 1 Nr. 3a ThürKAG, i. V. m. §§ 20, 31 Thüringer Gesetz über die kommunale Gemeinschaftsarbeit (ThürKGG), i. V. m. §§ 19, 20 Thüringer Kommunalordnung – ThürKO –), i. V. m. §§ 78, 90 und 88 Abs. 1 Abgabenordnung (AO), i. V. m. § 12 der Gebührensatzung zur Entwässerungssatzung des Zweckverbandes (GS-EWS), aus denen sich ergibt, dass ein Wasser- und Abwasserzweckverband die zur Erhebung und Bemessung der Beitragshöhe erforderlichen Daten erheben darf.
Der Zweckverband erhebt als kommunaler Wasserver- und Abwasserentsorger auf Grundlage des sogenannten Schmutzwassermaßstabes Gebühren für die Schmutzwasserbeseitigung, wobei in diesen bislang auch die Aufwendungen für die Niederschlagswasserbeseitigung enthalten sind.
Die Schmutzwassergebühren werden auf Grundlage des anerkannten Frischwassermaßstabes erhoben und die geplanten Niederschlagswassergebühren auf Grundlage des anerkannten Flächenmaßstabes (abflusswirksame Flächen).
Regenrückhaltungen, durch welche das Abwassernetz entlastet wird, sollen gebührenmindernd berücksichtigt werden.
Um Gebühren nach diesen Maßstäben erheben, also die anfallenden Wassermengen kalkulieren zu können, ist es erforderlich, folgende relevante Daten zu erheben: die Grundstücksdaten Flur, Flurstück, insbesondere die Größe, die Eigentümerdaten, um feststellen zu können, wer der Gebührenschuldner ist; ferner die abflusswirksamen Flächen/Einleitungen und Regenrückhaltung, wozu auch Dachneigungen und Versiegelungen gehören.
Aufgrund dessen konnte der TLfDI keinen Rechtsverstoß des Wasser- und Abwasserverbandes feststellen.

Schmutzwassergebühren werden häufig auf Grundlage des sogenannten Frischwassermaßstabes erhoben und die geplanten Niederschlagswassergebühren auf Grundlage des Flächenmaßstabes (ab-

flusswirksame Flächen). Um Gebühren nach diesen Maßstäben erheben, also die anfallenden Wassermengen kalkulieren zu können, ist es erforderlich, folgende relevante Daten zu erheben: die Grundstücksdaten Flur, Flurstück, insbesondere die Größe, die Eigentümerdaten, um feststellen zu können, wer der Gebührenschuldner ist; ferner die abflusswirksamen Flächen/Einleitungen und Regenrückhaltung, wozu auch Dachneigungen und Versiegelungen gehören.
Die rechtlichen Voraussetzungen für diese Datenerhebung durch den Wasser- und Abwasserverband waren durch §§ 10, 12, 15 Abs. 1 Nr. 3a Thüringer ThürKAG, i. V. m. §§ 20, 31 Thüringer Gesetz über die kommunale Gemeinschaftsarbeit (ThürKGG), i. V. m. §§ 19, 20 Thüringer Kommunalordnung – ThürKO –), i. V. m. §§ 78, 90 und 88 Abs. 1 Abgabenordnung (AO), i. V. m. § 12 der Gebührensatzung zur Entwässerungssatzung des Zweckverbandes (GS-EWS) gegeben, wonach ein Wasser- und Abwasserzweckverband die zur Erhebung und Bemessung der Beitragshöhe erforderlichen Daten erheben darf.

6.49 Datenschutz beim Theater

Im April 2017 erhielt der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) die Anfrage eines Thüringer Theaters. Im Rahmen der internen Revision zur Tätigkeit des betrieblichen Datenschutzbeauftragten hatte sich herausgestellt, dass sich der dafür zuständige Mitarbeiter aufgrund von Weisungsfunktionen in einem Interessenkonflikt befand. Daher erwog das Theater, einen externen Beauftragten zu bestellen und wollte vom TLfDI wissen, ob es als öffentlich gefördertes Unternehmen dazu berechtigt sei oder ob tatsächlich ein interner Beauftragter eingesetzt werden müsse.
In seiner Antwort legte der TLfDI dar, dass das Theater einschließlich der zugehörigen Staatskapelle eine Gesellschaft mit beschränkter Haftung (GmbH) ist, die öffentlich finanziell gefördert wird. Gemäß § 2 Abs. 2 Satz 1 Thüringer Datenschutzgesetz (ThürDSG) gelten „Als öffentliche Stellen (…) auch juristische Personen und sonstige Vereinigungen des privaten Rechts, (…) an denen eine oder mehrere der in Absatz 1 genannten juristischen Personen des öffentlichen Rechts beteiligt sind.“ Das Land Thüringen hält entscheidende Gesellschafteranteile am Theater und der Staatskapelle. Soweit öffentliche Stellen am Wettbewerb teilnehmen, sind auf sie gem. § 26

Satz 1 und Satz 2 ThürDSG nur der fünfte Abschnitt des ThürDSG und ansonsten die Bestimmungen des Bundesdatenschutzgesetzes (BDSG) mit Ausnahme des Zweiten Abschnitts und des § 38 BDSG anzuwenden. Nach Auffassung des TLfDI stand das anfragende Theater in Konkurrenz zu anderen Theatern und Orchestern und nahm deshalb als öffentliche Stelle am Wettbewerb teil. Somit galt für dieses Theater auch nicht § 10a ThürDSG, der die Bestellung eines Datenschutzbeauftragten regelt, sondern § 4f BDSG. Gemäß § 4f Abs. 2 Satz 3 1. Halbsatz BDSG kann zum Beauftragten für den Datenschutz auch eine Person außerhalb der verantwortlichen Stelle bestellt werden. Zu beachten ist jedoch, dass diese externe Person gem. § 4f Abs. 2 Satz 1 BDSG die zur Erfüllung ihrer Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzt. Somit stand nach Auffassung des TLfDI der Bestellung einer externen Person zum Beauftragten für den Datenschutz bei dem anfragenden Theater grundsätzlich nichts entgegen.

Sofern ein öffentliches Unternehmen am allgemeinen Wettbewerb teilnimmt, d. h. in Konkurrenz zu anderen Unternehmen steht, ist es als Wettbewerbsunternehmen nach § 26 Satz 1 und Satz 2 ThürDSG in Verbindung mit § 4f Abs. 2 Satz 3 1. Halbsatz BDSG berechtigt, eine externe Person mit dem Datenschutz im Unternehmen zu beauftragen. Voraussetzung ist gem. § 4f Abs. 2 Satz 1 BDSG, dass diese Person die erforderliche Fachkunde und Zuverlässigkeit besitzt.

6.50 Unberechtigte Speicherung, Nutzung und Auswertung von Druckerdaten im Linienverkehr einer kommunalen Busgesellschaft?

Ein Busunternehmer wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und bat um Überprüfung folgenden Sachverhaltes:
Mit dem Einbau neuer Fahrscheindrucker könne der Öffentliche Personennahverkehr (ÖPNV) sämtliche Daten sowie jeden gefahrenen Kilometer und die Geschwindigkeit der Busse überprüfen, speichern und auswerten und die Daten für sich nutzen. Diese neuen Fahrscheindrucker seien nicht abzuschalten, sodass auch bei Fahrten, die nicht den ÖPNV betreffen würden, eine Datenübertragung erfolge. So könne auch nachverfolgt werden, welche Chartertouren bzw. Leerfahrten übernommen würden.

Die Überprüfung des TLfDI hat Folgendes ergeben:
In technischer Hinsicht stellt sich der Sachverhalt so dar, dass die verbauten Fahrzeugrechner ausschließlich nach den VDV-Richtlinien (Verband Deutscher Verkehrsunternehmen) arbeiten. So benutzen diese Fahrzeugrechner im Fahrzeug das IBIS (Integriertes Bordinformationssystem) eines bestimmten Standards. Hier werden vom Fahrzeugrechner Linien- und Haltestelleninformationen an die Anzeigen und die verbauten Peripheriegeräte übergeben. Eine Speicherung dieser Daten findet nicht statt. Ebenso erfolgt keine Speicherung der gefahrenen Kilometer, der Strecke oder der gefahrenen Geschwindigkeit. Es findet auch kein Abgriff des im Fahrzeug verbauten CAN-Busses (Controller-Area-Network) statt. Nur über diesen CAN-Bus könnten diese Informationen, wie gefahrene Geschwindigkeit oder Strecke, abgegriffen werden. Diese Systeme stellt der Anbieter jedoch nicht zur Verfügung. Für die an den Haltestellen der Verwaltungsgemeinschaft (VG) zur Kundeninformation aufgestellten Dynamischen Fahrgastinformationsanzeiger (DFI) werden die Anzeigen in Echtzeit bedient, das heißt, dass in den Anzeigen der reguläre Fahrplan abgelegt ist und bei größeren Fahrplanabweichungen zeitlicher Art oder von der Fahrstrecke diese Abweichung als Kundeninformation zur Anzeige an den DFI gebracht wird. Diese Abweichungen werden aus dem Fahrzeug vom Fahrzeugrechner direkt gemeldet und zur Dynamischen Fahrgastanzeige gebracht, aber nicht gespeichert. Eine Zuordnung zum Fahrer wird hier ebenfalls nicht vorgenommen und ist auch nicht vorgesehen. Zur Anwendung kommen ausschließlich die Standardschnittstellen VDV 452 (Fahrplanimport) und VDV 453 (Anschlusssicherung und DFI). Diese Daten dienen ausschließlich der Echtzeitinformation der Fahrgäste und werden nicht gespeichert. Zusammenfassend lässt sich sagen, dass nach derzeitigem Erkenntnisstand des TLfDI das eingesetzte System dem Thüringer Datenschutzgesetz (ThürDSG) nicht widerspricht, da keinerlei personenbezogene Fahrer- oder Firmendaten verwendet oder gespeichert werden. Alle Daten dienen nur als Informationsquelle für die zukünftige Übergabe der Ankunftszeit der Linienbusse. Eine Erhebung oder Kontrolle außerhalb des Linienverkehrs kann nicht erfolgen, da es nur an bestimmten Haltestellen zu einem Abgleich der Soll- und Ist-Daten kommt. Wenn sich ein Bus nicht im Linienverkehr (Fahrer hat sich nicht angemeldet und keine Fahrt einer Linie eingegeben) befindet, stehen dem Gerät keine Daten zur Verfügung, auf welche es zurückgreifen könnte.

Die Sachverhaltsschilderung des Busunternehmers war damit nicht korrekt. Der Fahrscheindrucker konnte keine personenbezogenen Daten übermitteln.

In technischer Hinsicht konnte der TLfDI die Befürchtung des Busunternehmers entkräften, dass durch den Fahrscheindrucker des ÖPNV unbefugt Daten übertragen wurden.

6.51 Neues Personalausweis-Gesetz: Daten in Hülle und Fülle für den Staat

Das Zeitalter der digitalen Gesellschaft geht auch nicht spurlos am Personalausweisgesetz vorbei. Im Jahr 2010 wurde der neue digitale Personalausweis eingeführt. Man sah neben der Speicherung von Fingerabdrücken und einer qualifizierten elektronischen Signatur zur rechtssicheren digitalen Unterschrift, auch die Speicherung einer elektronischen Identifikationsmöglichkeit (eID-Funktion) vor.
Letztere sollte dazu dienen, sich gegenüber den Online-Diensten von Behörden und Unternehmen eindeutig identifizieren zu können.
Bürger konnten bei Ausgabe des Personalausweises wählen, ob sie diese Identifikationsmöglichkeit (eID-Funktion) zukünftig nutzen möchten.
Der Bundestagsdrucksache 18/11279 vom 22. Februar 2017 zur Änderung des Personalausweisgesetzes konnte man aber nun entnehmen, dass die Nutzung und die Verbreitung der eID-Funktion bisher hinter den Erwartungen zurückblieben. Bei zwei Dritteln der rund 51 Millionen ausgegebenen Ausweise sei die eID-Funktion deaktiviert.
Aber es gibt auch kaum Anwendungen diesbezüglich. Datenschützer warnten zudem permanent davor, die eID-Funktion zu nutzen, wenn nicht sichergestellt ist, dass heimlich das Passwort der eID-Funktion ausgelesen werden kann, z. B. durch Schadsoftware, welche die Tastatur-Eingabe am Rechner mit ausliest.
Nur die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zertifizierten Lesegeräte mit einer eigenen Tastatureingabe können dem derzeit Rechnung tragen. Alle anderen vom BSI zugelassenen Geräte sind aus Sicht des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) nicht empfehlenswert. Möchte der Bund ein sicheres Verfahren anbieten, so muss auch aus datenschutzrechtlicher Sicht die Sicherheit des kompletten

Verfahrens sichergestellt werden. Dem ist weiterhin nicht so. Die Verantwortung auf den Bürger zu delegieren, ist nicht mehr zeitgemäß, zudem erfolgen immer mehr Hackerangriffe auf IT-Systeme. Zukünftige repräsentative Verfahren wie z. B. Online-Abstimmungen, Wahlen etc. wären mit Lesegeräten ohne eigene Tastatureingabe wie oben beschrieben von vornherein anfällig oder manipulierbar.
Da nur wenige Bürger die eID-Funktion bei Antragstellung des Personalausweises freigeschaltet haben wollten, entschloss sich der Gesetzgeber, nun das Personalausweisgesetz (PAuswG) dahingehend zu ändern, dass die eID-Funktion für alle zukünftigen Personalausweise von vornherein freigeschaltet wird.
Zudem regelte man gleichzeitig in § 25 PAuswG, dass unter bestimmten Voraussetzungen zukünftig bestimmte Behörden im automatisierten Verfahren das Lichtbild aus dem Personalausweisregister abrufen können.
Dies konnten die unabhängigen Datenschutzbeauftragten des Bundes und der Länder nicht unkommentiert lassen und positionierten sich in ihrer Entschließung bereits im Januar 2017 dahingehend, dass die eID-Funktion weiterhin freiwillig sein muss und die zum 1. Mai 2021 vorgesehene Einführung eines nahezu voraussetzungslosen Abrufs des Lichtbildes im automatisierten Verfahren durch die Polizeibehörden des Bundes und der Länder sowie die Verfassungsschutzbehörden und Nachrichtendienste abgelehnt wird (siehe Anlage 10).
Die neuen Regelungen sind im Bundesgesetzblatt Nr. 46 vom 14. Juli 2017 veröffentlicht.

Die unabhängigen Datenschutzbeauftragten des Bundes und der Länder fordern, dass weiterhin die Funktion der elektronischen Identifizierung mittels digitalen Personalausweises freiwillig bleibt. Derzeit sind keine entsprechenden Bestrebungen bekannt, die eine verpflichtende Einführung der elektronischen Identifizierung erfordern. Zudem lehnen sie die vorgesehene Einführung eines nahezu voraussetzungslosen Abrufs des Lichtbildes im automatisierten Verfahren durch die Polizeibehörden des Bundes und der Länder sowie die Verfassungsschutzbehörden und Nachrichtendienste ab.



Personal Personalakte – © Wolfilser / Fotolia.com

7. Personaldaten

7.1 Kein Einblick in den kompletten Mutterpass

Eine Beamtin wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und beklagte sich über die Vorgehensweise ihres Dienstherrn. Die Beamtin informierte diesen über ihre Schwangerschaft und den bevorstehenden Geburtstermin mündlich. Daraufhin verlangte der Dienstherr zum Nachweis für die Personalabteilung eine Kopie aus ihrem Mutterpass, die den Umstand der Schwangerschaft bestätigte sowie den Namen der Beamtin und den voraussichtlichen Geburtstermin beinhaltete. Dies verweigerte die Beamtin, da außer den genannten Daten weitere, für den Dienstherrn nicht benötigte Informationen auf diesen Seiten enthalten sind. Stattdessen legte sie kurz darauf eine ärztliche Bescheinigung vor, damit alle für den Dienstherrn erforderlichen Daten vorliegen. Verbunden damit übergab die Beamtin eine Quittung für die Ausstellung der Bestätigung, da diese Auslagen gemäß § 8 Absatz 3 Thüringer Mutterschutzverordnung durch den Dienstherrn zu tragen sind. Diese Übernahme der Kosten wurde mit Verweis auf die geltende Dienststelleninformation abgelehnt. In dieser wird Bezug auf einen vom zuständigen Ministerium ergange-

nen Erlass genommen. Dieser besagt, dass für den Nachweis über eine Schwangerschaft keine Form vorgeschrieben wird und eine Kopie des Mutterpasses genüge. Hierbei sind der Name und der voraussichtliche Geburtstermin von Bedeutung. Alle anderen im Mutterpass enthaltenen Daten und Informationen sind nicht mit zu kopieren und unterliegen dem Datenschutz.
Der TLfDI wandte sich daraufhin an die für die Beamtin zuständige Landespolizeidirektion (LPD) und bat um Stellungnahme. Außerdem teilte der TLfDI mit, dass die derzeit gültige Dienststelleninformation den Eindruck erwecke, dass man der in der Thüringer Mutterschutzverordnung festgelegten Kostenübernahmepflicht entgehen wollte. Die Vorlage einer Kopie aus dem Mutterpass nur mit den erforderlichen Daten, nämlich dem Namen der Betroffenen und dem voraussichtlichen Entbindungstermin, stößt grundsätzlich auf keine datenschutzrechtlichen Bedenken. Allerdings könnte die praktische Umsetzung ein Problem darstellen. Denn wie soll es der Schwangeren möglich sein, einen geeigneten Nachweis zu erbringen, wenn dieser sich als lückenhafte Kopie erweist? In der Regel geht der Name der Schwangeren aus der zweiten Seite des Mutterpasses hervor, wobei diese Seite auch Eintragungen über Untersuchungsergebnisse vorsieht, die für die Aufgabenerfüllung der Dienststelle nicht erforderlich sind, und daher, soweit sie in einer Kopie nicht abgedeckt sein sollten, von der Dienststelle zwingend zu schwärzen wären, da die Diagnosen von der Dienststelle nicht verarbeitet werden dürfen. Weiterhin ist hier ein Arztstempel vorgesehen, wobei dieser sich auf die dort zu vermerkenden Untersuchungsergebnisse beziehen sollte. Der voraussichtliche Geburtstermin lässt sich nur auf der sechsten Seite des Mutterpasses entnehmen, wobei auf dieser Seite weder der Name der betroffenen Schwangeren noch der Name der die Prognose errechnenden Person vorgesehen ist. Auf dieser Seite sind allerdings weitere Feststellungsmöglichkeiten des behandelnden Arztes enthalten, die ebenfalls für die Dienststelle nicht erforderlich und damit hinsichtlich einer Verarbeitung unzulässig sind.
Die Landespolizeidirektion bestätigte, dass die Kopie der relevanten Daten des Mutterpasses zur Berechnung des Beschäftigungsverbotes ausreicht. Ein ärztliches Zeugnis sei dafür nicht erforderlich und werde regelmäßig wegen der dadurch für den Dienstherrn bzw. Arbeitgeber entstehenden Kosten nicht angefordert. Der Fall der Beschwerdeführerin war der LPD bekannt. Nach dort vorliegenden

Informationen wurde auch in diesem Fall kein ärztliches Zeugnis von der Bediensteten abgefordert.
Die LPD stimmt der Auffassung des TLfDI, dass eine Pflicht zur Vorlage des Mutterpasses nicht datenschutzkonform ist, vollinhaltlich zu. Die Formulierung entstammt dem Erlass des zuständigen Ministeriums und wird in der benannten Dienststelleninformation zitiert. Zugleich wird aber darauf hingewiesen, dass lediglich eine Kopie ausgewählter Daten des Mutterpasses notwendig ist.
In der Mehrheit der Fälle nutzten die schwangeren Bediensteten diese Möglichkeit. Soweit die Kopie vereinzelt darüber hinausgehende Daten enthält, werden diese regelmäßig von den zuständigen Sachbearbeitern des Personalbereichs geschwärzt. Die Beschwerde wurde gleichwohl zum Anlass genommen, die betreffenden Sachbearbeiter bezüglich dieser Problematik zu sensibilisieren und zur beständigen, sorgfältigen Prüfung der Kopien anzuhalten.
Der TLfDI wies die LPD darauf hin, dass bereits bei der Schwärzung durch den zuständigen Personalsachbearbeiter eine Erhebung von Daten aus dem Mutterpass erfolge, die nicht erforderlich ist. Der Mitarbeiter nimmt die Daten bei der Speicherung unweigerlich wahr und erfährt Details über die Schwangerschaft der Betroffenen, die er für die Aufgabenwahrnehmung nicht benötigt. Die LPD wurde daher aufgefordert, das Verfahren so zu gestalten, dass entweder bereits geschwärzte Kopien des Mutterpasses vorgelegt werden können oder die Betroffenen ein ärztliches Attest vorzulegen haben. Für den Fall der Beschwerdeführerin wurde angeregt, die Kosten des Attestes zu übernehmen, da diese aus den genannten Gründen die Vorlage des Mutterpasses zu Recht verweigert hatte.

Schwangere Polizeibeamtinnen unterliegen ab einem gewissen Stadium der Schwangerschaft einem Beschäftigungsverbot. Um diesen Zeitpunkt feststellen zu können, muss der Dienstherr den Umstand der Schwangerschaft und den voraussichtlichen Geburtstermin erfahren. Nicht erforderlich sind weitere Informationen über die Schwangerschaft, sodass entweder insoweit geschwärzte Kopien des Mutterpasses vorgelegt werden können oder, falls dies der Dienststelle nicht ausreicht, ein ärztliches Attest über die Schwangerschaft.

7.2 Personalakten oder die wundersame Datenvermehrung

Im Oktober 2015 bat eine Angestellte des Finanzamtes (FA) Jena den TLfDI darum, ihre Personalakte datenschutzrechtlich auf korrekte Aktenführung zu überprüfen. Die Beschwerdeführerin war der Ansicht, dass ihre Personalakte in diesem Sinne nicht ordnungsgemäß geführt werde. Sie führte aus, dass sich in der Akte mehrere, von ihr aufgezählte, Dokumente befänden, die nach ihrer Ansicht dort gar nicht hinein gehörten bzw. längst hätten entfernt werden müssen. Die Beschwerdeführerin gestattete dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) zum Zwecke der Prüfung die Einsicht in ihre Personalakte.
Daraufhin beantragte der TLfDI zur datenschutzrechtlichen Kontrolle nach § 37 Thüringer Datenschutzgesetz (ThürDSG) Einsicht in die bei der Thüringer Landesfinanzdirektion (LFD) geführte Personalhauptakte sowie in die beim FA Jena geführt Personalnebenakte der Beschwerdeführerin. Das FA Jena übersandte daraufhin die Personalnebenakte zur LFD nach Erfurt, sodass der TLfDI hier Einsicht in beide Akten nehmen konnte.
Bei der Einsichtnahme ergab sich, dass bereits optisch die Nebenakte des FA Jena umfangreicher war als die eigentliche Personalhauptakte der LFD. Auf entsprechende Nachfrage des TLfDI legte die Ansprechpartnerin der LFD dar, dass bereits der Umfang darauf schließen lasse, dass Unterlagen aufgenommen wurden, die nicht für die Nebenakte bestimmt waren. Bei der Führung der Nebenakte dürfe sich maximal ein Doppel ergeben, d. h. die Nebenakte darf maximal genauso „dick“ wie die Hauptakte sein und keinesfalls umfangreicher.
Der TLfDI wies darauf hin, dass in der Nebenakte nur Kopien der Unterlagen der Personalakte aufgenommen werden dürften, die für die Aufgabenerfüllung der Beschäftigungsbehörde, d. h. des FA, erforderlich sind. Eine deckungsgleiche Aufgabenerfüllung der personalverwaltenden Stelle LFD und des FA kann nicht vorliegen und ist gesetzlich auch nicht vorgesehen (§ 81 Abs. 2 Satz 3 Thüringer Beamtengesetz). Somit muss zunächst grundsätzlich festgelegt sein, welche konkreten Aufgaben in der Beschäftigungsbehörde wahrgenommen werden und welche Unterlagen die Beschäftigten betreffend in Kopie hierfür erforderlich sind. Unterlagen, die für die Weiterleitung bestimmt sind, dürfen nicht in Kopie abgeheftet werden. Bestehen Teilakten (Bezüge o. ä.), ist kein Grund ersichtlich, die

Unterlagen auch in die Personalakte der LFD oder gar in die Personalnebenakte des FA zusätzlich aufzunehmen. Im Hinblick darauf erörterte der TLfDI mit der LFD verschiedene Unterlagen. Der TLfDI beanstandete verschiedene datenschutzrechtliche Mängel nach § 39 ThürDSG.
Die LFD folgte den datenschutzrechtlichen Ausführungen des TLfDI und sicherte die entsprechende Überarbeitung und Sichtung der Personalhaupt- und der -nebenakte zu. Im Rahmen dieser Überarbeitung wurden verschiedenen Unterlagen aus der Personalakte der Beschwerdeführerin entfernt, da ihre Abheftung in der Akte von vornherein unzulässig war. Andere Unterlagen wurden entfernt, da ihre Aufbewahrungsfristen in der Personalakte längst abgelaufen waren. Weiterhin wurden Unterlagen entfernt, die regelmäßig nur auf Antrag der Betroffenen aus der Personalhauptakte genommen werden. Der Aktenvermerk über die der Beschwerdeführerin gewährte Akteneinsicht wurde ebenfalls entfernt, da es nicht erforderlich ist, die Wahrnehmung dieses den Bediensteten zustehenden Rechts zu protokollieren.
Im Rahmen seiner datenschutzrechtlichen Kontrolle stellte der TLfDI außerdem fest, dass sich in der Personalakte Unterlagen befanden, die grundsätzlich in Teilakten (Bezügeakte, Kindergeldakte) oder in anderen Teilen der Personalakte zu führen sind. Auch diese Dokumente wurden durch die LFD jetzt korrekt zugeordnet; alle Unterlagen, die beispielsweise zur Zahlung der Vergütung erforderlich sind, wurden der zentralen Gehaltsstelle übergeben.
Der TLfDI wies die LFD darauf hin, Aufbewahrungsfristen einzuhalten und die entsprechenden Unterlagen nach Ablauf dieser Fristen umgehend aus der Personalakte zu entfernen und zu vernichten.
Im Zuge dieser im Rahmen der datenschutzrechtlichen Kontrolle aufgedeckten Mängel teilte die LFD dem TLfDI mit, dass sie beabsichtigt, alle Personalakten auf vergleichbare Verstöße zu sichten und unter Berücksichtigung der datenschutzrechtlichen Anforderungen sowie der geltenden Aufbewahrungsfristen zeitnah zu bereinigen. Weiterhin kündigte die LFD an, ihre Mitarbeiter datenschutzrechtlich zu schulen, um künftig die entsprechenden Vorschriften einzuhalten. Damit wurde die vom TLfDI ausgesprochene Beanstandung im Juni 2016 behoben.

Personalhauptakten sind bei der personalverwaltenden Stelle zu hinterlegen. In die Nebenakte zur Personalakte dürfen nur Kopien

der Unterlagen aus der Personalakte aufgenommen werden, keine Originale. Zudem dürfen nur die Dokumente aufgenommen werden, die für die Aufgabenerfüllung der jeweiligen Beschäftigungsbehörde erforderlich sind. Unterlagen, die für die Weiterleitung bestimmt sind, dürfen nicht in Kopie abgeheftet werden. Unterlagen aus bestehenden Teilakten sind nicht in Kopie in die Personalhaupt- oder -nebenakte aufzunehmen.

7.3 Mitarbeiter krank? – Da fragen wir doch mal den Arzt!

Dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) ging ein Hinweis zu, dass in der Personalverwaltung einer Stadt in Thüringen der Datenschutz nicht besonders ernst genommen werde. Unter anderem hatte sich danach die Stadtverwaltung veranlasst gesehen, sich bei einem behandelnden Arzt über einen erkrankten Mitarbeiter der Stadtverwaltung zu erkundigen. Der TLfDI hielt es für erforderlich, die Personalaktenführung der Stadtverwaltung vor Ort zu prüfen. Er führte eine datenschutzrechtliche Kontrolle nach § 37 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) durch. Bei der Kontrolle war der Bürgermeister der Stadt zugegen sowie der behördliche Datenschutzbeauftragte und weitere Mitarbeiter der Verwaltung. Bei der Kontrolle machten die Mitarbeiter des TLfDI folgende Feststellungen:
Das Büro des zuständigen Personalsachbearbeiters ist neben einem anderen Büro untergebracht, wobei beide Räume durch eine Tür verbunden sind. Dabei handelt es sich nicht um eine sogenannte Schallschutztür. Ansprechpartner bestätigten, dass Mitarbeiter, die sich in Personalsachen an den zuständigen Sachbearbeiter wenden, regelmäßig Gespräche aus dem Nachbarzimmer hören. Dadurch herrsche bei vertraulichen Personalgesprächen eine erhebliche Unsicherheit, ob diese im Nachbarzimmer zur Kenntnis genommen werden können. Dies bestätigte sich auch bei einem durch die Mitarbeiter des TLfDI vor Ort durchgeführten Versuch.
Es wurde exemplarisch in drei Personalakten Einsicht genommen. Die erste Personalakte betraf einen Mitarbeiter, dem durch die Stadt gekündigt worden war. In seiner Personalakte gab es eine Beiakte „Disziplinarvorgänge“ in der der gesamte Vorgang zur Vorbereitung einer Kündigung bis zum gerichtlichen Vergleich den Mitarbeiter betreffend abgeheftet war. Grundsätzlich wird nach Angaben der Ansprechpartner ein Kündigungsvorgang geführt, der nach Ab-

schluss des Verfahrens zur Personalakte genommen wird. Ob dies im vorliegenden Fall so gehandhabt wurde, war nachträglich anhand der Abheftung nicht festzustellen. Nach Angaben der Ansprechpartner werden arbeitsrechtliche Streitigkeiten unter Inanspruchnahme von Rechtsanwälten geführt. Festzustellen war im vorliegenden Fall, dass der Schriftverkehr mit dem die Stadtverwaltung vertretenden Rechtsanwalt zumindest teilweise per E-Mail erfolgte.
Außerdem fand sich auch der Mailverkehr zur Vorbereitung der Kündigung in den Akten. Dabei wurde beim behandelnden Arzt des Mitarbeiters nachgefragt, wann dieser sich in der Praxis befunden hatte. Außerdem wurde die Krankenkasse per Mail zur Krankschreibung befragt. Beide Stellen haben ausweichende Antworten gegeben, sodass letztlich keine Gesundheitsdaten an die Stadtverwaltung übermittelt worden sind.
In einer nächsten überprüften Personalakte fand sich die Geburtsurkunde eines Kindes, das inzwischen Mitte dreißig ist. Abgeheftet waren auch Formblätter zur Wiedereingliederung aus einem lange zurückliegenden Jahr. In der dritten in Augenschein genommenen Akte befanden sich keine Besonderheiten.
Der TLfDI bewertete die gemachten Feststellungen wie folgt:
Nach § 9 Abs. 1 Satz 1 ThürDSG haben die öffentlichen Stellen die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der datenschutzrechtlichen Bestimmungen zu gewährleisten. In § 9 Abs. 2 ThürDSG sind die Gewährleistungsziele, denen die technischen und organisatorischen Maßnahmen dienen, definiert. Da es sich bei Personalaktendaten um sensible personenbezogene Daten der Beschäftigten handelt, die auch besonders geschützte personenbezogene Daten nach § 4 Abs. 5 ThürDSG umfassen können, ist besonderes Augenmerk auf die Gewährleistung der Vertraulichkeit nach § 9 Abs. 2 Nr. 1 ThürDSG zu richten. Zur Gewährleistung der Vertraulichkeit von Personalaktendaten gehört auch, dass Personalgespräche mit Beschäftigten geführt werden, ohne dass Unbefugte Inhalte zur Kenntnis nehmen können. Unbefugt sind alle Personen, die nicht im Rahmen der Personalverwaltung mit der Bearbeitung von Personalangelegenheiten beauftragt sind (§ 80 Abs. 1 ThürBG). Da nach den Feststellungen Gespräche, die der Vertraulichkeit unterliegen, von anderen Bediensteten, die nicht mit Personalangelegenheiten beauftragt sind, im Nebenzimmer mitgehört werden können, ist die Vertraulichkeit in der Stadtverwaltung nicht gewährleistet. Es sind daher Maßnahmen zu treffen, die

die Vertraulichkeit von Personalgesprächen sicherstellen. Entweder ist ein geeigneter Schallschutz einzurichten, um zu verhindern, dass Personen, die nicht mit der Personalverwaltung betraut sind, Personalaktendaten durch das gesprochene Wort zur Kenntnis nehmen können. Alternativ kann auch durch geeignete Raumverteilung sichergestellt werden, dass sich nur befugte Personen in dem angrenzenden Raum aufhalten bzw. dort untergebracht sind. Allerdings wäre auch in diesem Fall zu beachten, dass vertrauliche Vieraugengespräche ebenfalls einen geeigneten Schallschutz benötigen.

Der Umgang mit Personaldaten sowie die Personalaktenführung für Beschäftigte im öffentlichen Dienst des Landes richtet sich gemäß § 33 ThürDSG grundsätzlich nach den dienstrechtlichen Vorschriften, §§ 79 bis 87 Thüringer Beamtengesetz (ThürBG).

Beim Austausch von Personalaktendaten im Falle eines Rechtsstreits mit einem beauftragten Rechtsanwalt sind die erforderlichen organisatorischen und technischen Maßnahmen zum Schutz gegen unbefugte Kenntnis zu treffen. Die Nutzung von E-Mail ist bekanntlich nur dann ein sicherer Übertragungsweg, wenn geeignete Verschlüsselungstechnik zum Einsatz kommt, um unbefugte Kenntnis auf dem Übertragungsweg auszuschließen. Zur Wahrung der Vertraulichkeit kann auch der Postweg genutzt werden, der aufgrund des verschlossenen Umschlags und der strafbewehrten Wahrung des Postgeheimnisses einen Schutz vor unbefugter Kenntnis des Inhalts bietet. Weiterhin ist bei der Nutzung von E-Mail im Zusammenhang mit Personalangelegenheiten auch unter Einsatz von geeigneter Verschlüsselungstechnik darauf zu achten, dass empfangene und versandte Dokumente im E-Mail-Postfach ebenfalls gegen unbefugte Kenntnis zu schützen sind. Sofern mit vertretenden Rechtsanwälten der Schriftverkehr weiterhin über E-Mail erfolgen soll, ist ein geeignetes Verschlüsselungsverfahren einzusetzen. Der ungesicherte Austausch von Personalaktendaten über E-Mail stellt nach Auffassung des TLfDI einen erheblichen Verstoß gegen den § 9 Abs. 2 Nr. 2 ThürDSG dar, der gemäß § 39 Abs. 1 ThürDSG gegenüber der Stadtverwaltung beanstandet wurde.

Auch die Anfragen an den behandelnden Arzt und die Krankenkasse des Betroffenen stellen wegen Verstoßes gegen den Grundsatz der Erhebung beim Betroffenen nach § 19 Abs. 2 Satz 1 ThürDSG einen erheblichen Verstoß gegen datenschutzrechtliche Vorschriften dar und wurden gemäß § 39 Abs. 1 ThürDSG beanstandet. Der Stadt wurde aufgegeben, geeignete Maßnahmen zu treffen, um zukünftig

unzulässige Nachfragen zu Erkrankungen von Mitarbeitern zu verhindern. Für die Nachfrage beim behandelnden Arzt und der Krankenkasse gibt es keine Rechtsgrundlage. Es gilt der Grundsatz der Erhebung personenbezogener Daten beim Betroffenen, § 19 Abs. 2 Satz 1 ThürDSG. Ohne die Mitwirkung des Betroffenen dürfen Daten nur erhoben werden, wenn eine der in § 19 Abs. 2 Nr. 1 bis 3 ThürDSG genannten Voraussetzungen vorliegt. Eine solche Voraussetzung lag nicht vor. Letztendlich kam es aber durch die ausweichenden Antworten des angeschriebenen Arztes und der Krankenkasse, die sich ihrerseits bei einer entsprechenden Auskunft wegen Verletzung der ärztlichen Schweigepflicht bzw. des Sozialgeheimnisses rechtswidrig verhalten hätten, nicht zu einer unzulässigen Datenerhebung durch die Personalverwaltung.
Zum fraglichen Zweck des Nachweises eigener Kinder für die Berücksichtigung bei der Pflegeversicherung, für die weder ein Kindergeldanspruch besteht noch eine weitergehende Berücksichtigungsverpflichtung, reichen aus datenschutzrechtlicher Sicht die Vorlage der Geburtsurkunde und ein bestätigender Vermerk des zuständigen Sachbearbeiters aus. Geburtsurkunden müssen daher nicht dauerhaft in der Personalakte verwahrt werden. Sollte die Urkunde zur Vorlage bei einer anderen Stelle erforderlich sein, reicht ebenfalls ein Vermerk über die Weiterleitung aus. Eine Kopie der Urkunde in der Personalakte aufzubewahren, für die keine weitere Aufgabenerfüllung der aktenführenden Stelle ersichtlich ist, ist grundsätzlich nicht erforderlich.
Unterlagen zur Wiedereingliederung stehen im Zusammenhang mit Erkrankungen. Sie sind nach § 87 Abs. 2 Satz 1 ThürBG nach Ablauf von fünf Jahren nach Abschluss des Vorgangs aus der Personalakte zu entfernen.
Die Stadtverwaltung hat die künftige Beachtung der datenschutzrechtlichen Vorschriften zugesagt.

Nach § 9 Abs. 1 Satz 1 ThürDSG haben die öffentlichen Stellen die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der datenschutzrechtlichen Bestimmungen zu gewährleisten. Da Personalaktendaten auch immer geschützte personenbezogene Daten nach § 4 Abs. 5 ThürDSG umfassen können, ist besonderes Augenmerk auf die Gewährleistung der Vertraulichkeit nach § 9 Abs. 2 Nr. 1 ThürDSG zu richten. Dazu gehört es, dass Personalgespräche mit Beschäftigten geführt werden

können, ohne dass Unbefugte vom Inhalt Kenntnis erlangen könnten. Zu den erforderlichen technischen und organisatorischen Maßnahmen gehört es auch, dass E-Mail-Verkehr mit Beschäftigtendaten nur über ein geeignetes Verschlüsselungsverfahren stattzufinden hat. Keinesfalls zulässig sind wegen des Grundsatzes der Erhebung beim Betroffenen Anfragen bei Ärzten oder Krankenkassen.

7.4 Der mitteilsame Amtsarzt

Im 11. Tätigkeitsbericht (TB) des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) wurde unter 6.8 über die Übermittlungsbefugnis des Amtsarztes an die Dienststelle des untersuchten Beamten berichtet. Damals lag eine Beschwerde vor, weil der Amtsarzt der untersuchten Person keine Auskunft über die der Dienststelle übermittelten Feststellungen zum Gesundheitszustand erteilt hatte und erst durch die Personalakteneinsicht erfuhr, dass viel zu viele Angaben in der Stellungnahme zur Dienstfähigkeit enthalten waren. Unter anderem betraf dies Diagnosen, die gar nicht mit der Dienstfähigkeit im Zusammenhang standen. Trotz Zusage des Amtsarztes hatte die betroffene Person nach Ablauf einer angemessenen Frist noch keine Kopie eines den gesetzlichen Anforderungen genügenden Gutachtens erhalten. Dem wurde aufgrund der im letzten TB bereits dargestellten ausgesprochenen Beanstandung nach § 39 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) in Verbindung mit § 33 Abs. 3 und 5 Thüringer Beamtengesetz (ThürBG) zwischenzeitlich nachgekommen.
Um sich nun nicht nur auf Zusagen der verantwortlichen Stelle zu verlassen, nahm dies der TLfDI zum Anlass, im Rahmen einer datenschutzrechtlichen Kontrolle nach § 37 ThürDSG in die Personalakte der betroffenen Person Einsicht zu nehmen und zu überprüfen, ob sich dort nur noch die erforderlichen Angaben befinden.
Die Einsicht in die in jeweils verschlossenen Umschlägen zur Personalakte genommenen amtsärztlichen Gutachten ergab, dass das zeitlich letzte Gutachten den Anforderungen des § 33 ThürBG genügte. Es waren keine Diagnosen und keine Details zur durchgeführten Untersuchung enthalten. Lediglich die von der Dienststelle gestellte Frage war beantwortet worden. Es handelt sich offenbar um das aufgrund des Vorgehens und der Forderung des TLfDI ausgetauschte Gutachten. Ein vorheriges Gutachten des Amtsarztes mit umfangrei-

cher Anamnese, Befunden und der Angabe einer Vielzahl von Diagnosen war aber ebenfalls abgeheftet.
Ein weiteres älteres Gutachten enthielt zwar keine Diagnosen, allerdings wurde ausführlich die persönliche Verhaltensweise des Betroffenen gegenüber dem Amtsarzt dargestellt. Diese Bewertung der Persönlichkeit war aber für die letztendliche Entscheidung über die Reduzierung der Arbeitszeit und für den Vorschlag einer Nachuntersuchung erkennbar nicht erforderlich.
Daher hat der TLfDI gefordert, diese nicht erforderlichen Angaben aus der Personalakte zu entfernen. Hierzu bestehen zwei Möglichkeiten: Entweder werden die von der Personalverwaltung nicht zu erhebenden und nicht zu nutzenden Diagnosen und weitgehenden Ausführungen des Amtsarztes abgedeckt und kopiert, damit nur die letztendliche Bewertung, die für die Aufgabenerfüllung der Personalverwaltung erforderlich ist, sichtbar bleibt. Alternativ kann das amtsärztliche Gutachten an den Amtsarzt zurückgegeben und eine auf die zulässigen und erforderlichen Angaben reduzierte Version verlangt werden.
Eine andere Schwachstelle trat bei der Kontrolle in der die Personalakten führenden Dienststelle zusätzlich zu Tage: Auch in der abgespeckten datenschutzgerechten Form handelt es sich bei den amtsärztlichen Mitteilungen immer noch um sehr sensible personenbezogene Daten der hiervon Betroffenen. Folglich müssen auch die technischen und organisatorischen Maßnahmen wirksam getroffen sein, die eine unbefugte Kenntnisnahme ausschließen. Unbefugt ist jede Person, die nicht im Rahmen der Personalverwaltung mit der Bearbeitung von Personalangelegenheiten beauftragt ist (§ 80 Abs. 1 ThürBG). Im Klartext bedeutet das, dass derartige Personaldokumente ungeöffnet die zuständige Personalverwaltung erreichen müssen. Auch wenn in der Dienststelle festgelegt ist, dass Schreiben an die Personalverwaltung bzw. in vertraulichen Personalangelegenheiten ungeöffnet an die Personalverwaltung zu leiten sind, muss dies für die Poststelle erkennbar sein. Ist ein solches Schreiben – wie festzustellen war – nur an die allgemeine Postadresse ohne Zusatz gerichtet, muss es von den Mitarbeitern der Poststelle erstmal geöffnet werden, um die zuständige Stelle innerhalb des Hauses festzustellen und um gleichzeitig zu spät auch festzustellen, dass es aufgrund des Inhalts hätte gar nicht geöffnet werden dürfen.
Um unbefugte Kenntnis von amtsärztlichen Gutachten innerhalb der Empfängerbehörde zukünftig auszuschließen, wurde angeregt, in den

Anschreiben an die Amtsärzte neben den konkreten Fragestellungen auch eine „Handlungsanweisung“ zum Versand der Antworten beizufügen. Diese könnte wie folgt lauten:

- **„Bitte kennzeichnen Sie Ihre Antwort sichtbar im Adressfeld oder auf dem Briefumschlag mit *vertrauliche Personalangelegenheit*,** um sicherzustellen, dass sie ungeöffnet zur Personalverwaltung gelangt.“

Der TLfDI hat dies zum Anlass genommen, alle Gesundheitsämter darauf hinzuweisen.

Von der Dienststelle angeforderte amtsärztliche Gutachten zur Dienstfähigkeit dürfen nur die in § 33 ThürBG genannten Angaben enthalten. Sie sind im Adressfeld als vertrauliche Personalsache zu kennzeichnen, damit sie von der Poststelle ungeöffnet die Personalverwaltung erreichen können.

7.5 Doppelte Kontrollen der Arbeitszeit zulässig?

Dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) lag der Hinweis vor, dass in einer Abteilung eines Thüringer Landratsamtes parallel zur generellen Arbeitszeiterfassung ein weiteres automatisiertes Verfahren zur Verarbeitung von Mitarbeiterdaten im Einsatz war, das im Verfahrensverzeichnis nach § 10 (Thüringer Datenschutzgesetz) ThürDSG nicht aufgenommen worden war. Der TLfDI hatte sich im vorliegenden Fall zu einer unangekündigten Kontrolle nach § 37 ThürDSG vor Ort entschlossen, um sicherzustellen, dass die angesprochene automatisierte Datenverarbeitung nicht anlassbezogen verändert werden konnte, weil der Hinweisgeber gerade diese Befürchtung geäußert hatte.

Nach § 34 Abs. 2 ThürDSG bedarf der erstmalige Einsatz automatisierter Verfahren, mit denen personenbezogene Daten verarbeitet werden, hinsichtlich der Datenarten und der regelmäßigen Datenübermittlungen der vorherigen schriftlichen Freigabe durch die verantwortliche Stelle. Dies ist auch die Voraussetzung, dass ein Verfahren in das zu führende Verfahrensverzeichnis nach § 10 ThürDSG aufzunehmen ist. Bei der in der kontrollierten Abteilung geführten zusätzlichen „Arbeitszeiterfassung“ handelte es sich um eine automatisierte Datei zur Erfassung der Arbeitszeiten der dort tätigen Außendienstmitarbeiter. Unstreitig wurde eine datenschutzrechtliche

Freigabe weder beantragt noch erteilt. Wird ein Verfahren ohne die erforderliche vorherige Freigabe geführt, stellt dies einen erheblichen datenschutzrechtlichen Verstoß dar, der gemäß § 39 i. V. m. § 34 Abs. 2 ThürDSG beanstandet werden kann. Eine datenschutzrechtliche Freigabe für das Verfahren in der festgestellten Ausgestaltung konnte indes aus Sicht des TLfDI nicht erteilt werden. Neben der Erfassung der regulären Arbeitszeiten sollte das Verfahren nämlich dazu dienen, die Zeiten einer Prüftätigkeit in Stellen außerhalb der Behörde zu erfassen, um hierfür die festgeschriebenen Gebühren geltend machen zu können. Eine doppelte Erfassung der Arbeits- und Abwesenheitszeiten war indes aus Gründen der Datensparsamkeit und mangels Erforderlichkeit zur Aufgabenerfüllung nicht zulässig.
Auch wenn Korrekturmeldungen zu nicht erfassten Arbeitszeiten über die Amtsleiterin an das Sachgebiet Personal zu leiten waren, rechtfertigte dies keine ständig verfügbare automatisierte Doppelerfassung der Arbeitszeitdaten in der Abteilung. Auch der gegenüber der Amtsleiterin geäußerte Wunsch der Mitarbeiter des Amtes, zur Sicherheit eine parallele Arbeitszeiterfassung nutzen zu können, um nach längerer Abwesenheit leichter die entsprechenden Korrekturblätter abgeben zu können, bildete keine Rechtfertigung für die doppelte Arbeitszeiterfassung. Ebenso ist die Möglichkeit einer Plausibilitätsprüfung kein Rechtfertigungsgrund. Im Zweifelsfall konnte der entsprechende Bedienstete durch einen Teilausdruck aus dem von allen Mitarbeitern zu nutzenden Zeiterfassungssystem seine Arbeitszeiten nachweisen.
Die Führung des Parallelverfahrens wurde wegen der fehlenden datenschutzrechtlichen Freigabe beanstandet. Unmittelbar nach der datenschutzrechtlichen Kontrolle bestätigte das Landratsamt die Einstellung des Verfahrens. Damit wurde den datenschutzrechtlichen Belangen nachgekommen.
Dagegen kann durchaus auf der Grundlage der Gebührensatzung ein automatisiertes Verfahren zur Erfassung der Prüfungstätigkeit zum Zweck der Gebührenabrechnung geführt werden. Hinsichtlich der Datenarten können aber neben der Bezeichnung des Prüfers und des Prüfgegenstands nur die maßgeblichen, in der Gebührenordnung aufgelisteten Zeiten erfasst werden.

Soll ein automatisiertes Verfahren zur Erfassung von Arbeitszeiten eingesetzt werden, ist die vorherige Freigabe nach § 34 ThürDSG einzuholen. Parallel zu dem auf der Grundlage der erforderlichen

Dienstvereinbarung zur regulären Arbeitszeiterfassung geführte Verfahren zur Arbeitszeiterfassung sind grundsätzlich nicht erforderlich und damit unzulässig.

7.6 Personalnachrichten am schwarzen Brett im Kindergarten: TLfDI sieht schwarz

Der Thüringer Landesbeauftrage für den Datenschutz und die Informationsfreiheit (TLfDI) erhielt den Hinweis, dass in einem kommunalen Kindergarten wichtige Mitteilungen über das dort tätige Personal für alle Eltern oder sonst zur Abholung der Kinder befugten Personen zur Kenntnis ausgehangen wurden. Die Informationen beinhalteten Angaben zu einem namentlich genannten ausscheidenden Mitarbeiter, wobei das von ihm betreute Kind mit erhöhtem Betreuungsbedarf gleich mit benannt wurde. Eine namentlich genannte Erzieherin war wieder eingestellt worden, unterliege aber aufgrund ihrer Schwangerschaft einem Berufsverbot. Zur weiteren Beschäftigungssituation wurde darauf hingewiesen, dass alle bis auf eine Erzieherin wieder auf 40 Arbeitsstunden gesetzt waren. Die fehlenden Stunden sollte eine namentlich genannte Person als Hilfskraft übernehmen. Dass diese Hilfskraft qualifiziert war, wurde durch Details aus ihrem Lebenslauf insbesondere zum beruflichen Werdegang belegt.

Bei allem Verständnis dafür, dass die Eltern der dort betreuten Kinder durchaus ein Interesse daran haben, über die Personalausstattung des Kindergartens informiert zu sein und gerne mehr über die Erzieher wissen wollen, insbesondere auch, weshalb eine geschätzte Kraft nun plötzlich nicht mehr verfügbar ist, ist eine derartige Information aus datenschutzrechtlicher Sicht natürlich nicht zulässig. Rein rechtlich handelt es sich bei dem Aushang um eine Übermittlung von Personalaktendaten an Dritte in Form einer Veröffentlichung. Diese Verarbeitung personenbezogener Daten ist nur zulässig, wenn dies eine Rechtsvorschrift erlaubt oder anordnet oder die/der Betroffene eingewilligt hat (vergleiche § 4 Abs. 4 Thüringer Datenschutzgesetz – ThürDSG). Maßgebliche Norm für die Verarbeitung von Beschäftigtendaten ist § 33 ThürDSG, der auf die dienstrechtlichen Vorschriften (§§ 78-87 Thüringer Beamtengesetz – ThürBG) verweist. Nach diesen Vorschriften sind die Personalaktendaten vertraulich zu behandeln. Auskünfte an Dritte dürfen nach § 85 Abs. 2 ThürBG grundsätzlich nur mit Einwilligung der/des Betroffenen gegeben

werden. Allerdings setzt die Auskunftserteilung nach dieser Vorschrift ein konkretes zu überprüfendes Auskunftsbegehren des Empfängers der Informationen voraus, das in diesem Zusammenhang nicht unterstellt werden konnte. Der Kindergartenträger und dessen Leitung wurden daher aufgefordert, den Aushang umgehend zu entfernen, weil keine Rechtsgrundlage ersichtlich war.
Der kommunale Träger teilte daraufhin mit, aufgrund der Elternmitwirkung gemäß § 10 Thüringer Kitagesetz müsse der Elternbeirat vom Träger und der Leitung der Einrichtung rechtzeitig und umfassend über wesentliche Entscheidungen in Bezug auf die Kindertageseinrichtung informiert werden. Insbesondere müsse vor einer Entscheidung über die personelle Besetzung eine Anhörung durchgeführt werden. Das ausgehängte Schriftstück habe man deshalb per E-Mail an den Vorsitzenden des Elternbeirats übersandt. Die Information aller Eltern über den Aushang sei auf ausdrücklichen Wunsch der betroffenen darin genannten Erzieher erfolgt. Zum Beleg dafür legte man eine Einverständniserklärung der im Kindergarten beschäftigten Erzieher vor, die undatiert, aber ersichtlich nach dem erfolgten Aushang, ausgefüllt worden war. Auch hatte man vermerkt, dass einzelne Personen telefonisch die Einwilligung erteilt hätten.
Der TLfDI wies darauf hin, dass im Rahmen einer gesetzlich vorgeschriebenen Anhörung den Anzuhörenden nur die personenbezogenen Daten zur Kenntnis gegeben werden dürfen, die für die Aufgabenerfüllung erforderlich sind (§ 21 ThürDSG). Zur Mitteilung geeignet waren daher nur die Personen und gegebenenfalls deren für eine Stelle erforderliche Qualifikation. Weitere Details aus den Lebensläufen und insbesondere Einzelheiten zur Schwangerschaft dürfen nicht mitgeteilt werden. Angaben darüber hinaus können aber weder als erforderlich noch zulässig angesehen werden.
Die Anforderungen an eine rechtswirksame Einwilligung zur Veröffentlichung sind in § 4 Abs. 3 ThürDSG niedergelegt. Eine Einwilligung muss zwingend vor der beabsichtigten Datenverarbeitung vorliegen. Ein nachträgliches Einverständnis heilt den Formmangel nicht. Weiterhin muss die Einwilligung den konkreten Zweck der Datenverarbeitung erkennen lassen, wobei der konkrete Bezug zur Aufgabenerfüllung und die dafür erforderlichen Daten für Betroffene erkennbar sein müssen. Zudem muss die Einwilligung auf der freien Willensentscheidung des Betroffenen beruhen. Dazu gehört auch, dass Betroffene sowohl über den Inhalt einer Veröffentlichung als

auch über den Zweck und den Empfängerkreis ausreichend informiert sind. Im Beschäftigtenverhältnis ist besonders zu beachten, dass das Vorliegen der Freiwilligkeit in der Regel zumindest zweifelhaft ist, weil sich die Beschäftigten unter Druck gesetzt fühlen können. Von einer Freiwilligkeit ist daher nur dann auszugehen, wenn den Beschäftigten bei Verweigerung einer Einwilligung keinerlei Nachteile entstehen oder sie solche zu befürchten haben. Davon kann man jedoch nur in den wenigsten Ausnahmefällen ausgehen.
Die vorgelegte Einverständniserklärung genügte den Anforderungen an eine rechtswirksam erteilte Einwilligung des jeweils Betroffenen nicht. Die Veröffentlichung der Beschäftigtendaten durch öffentlichen Aushang ohne Rechtsgrundlage wurde gemäß § 39 Abs. 1 in Verbindung mit § 33 ThürDSG beanstandet. Der kommunale Träger wurde aufgefordert, durch Auswertung des Vorfalls, Schulung der Beschäftigten und Einbindung des behördlichen Datenschutzbeauftragten zukünftig derartige erhebliche Verstöße gegen datenschutzrechtliche Vorschriften auszuschließen. Dem wurde nachgekommen.

Die Veröffentlichung von Personaldaten durch öffentliche Stellen kann regelmäßig nicht auf die Einwilligung der Betroffenen gestützt werden. Es fehlt zumeist die Freiwilligkeit, die für eine rechtswirksame Einwilligung maßgeblich ist.

7.7 KollegInnen müssen nicht alles wissen

Dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) lag eine Anfrage zur Zulässigkeit der Erfassung und Übermittlung von Arbeitszeitdaten der Mitarbeiter einer Stadtverwaltung vor. Das zur Arbeitszeiterfassung eingesetzte automatisierte Verfahren erlaube nämlich unter anderem jedem Bediensteten, einzusehen, aus welchen Gründen andere Bedienstete Fehlzeiten haben.
Nach § 33 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) gelten für die Verarbeitung und Nutzung personenbezogener Daten von Beschäftigten im öffentlichen Dienst, die nicht verbeamtet sind, die für Beamten geltenden dienstrechtlichen Vorschriften (§§ 79 bis 87 des Thüringer Beamtengesetzes – ThürBG) grundsätzlich entsprechend. Arbeitszeitdaten darf die öffentliche Stelle nach § 79 Abs. 1 ThürBG verarbeiten, weil dies zur Durchführung des Beschäfti-

gungsverhältnisses, insbesondere auch für den Personaleinsatz erforderlich ist. Nähere Festlegungen zur Erfassung und zum Umgang mit Arbeitszeitdaten sind in einer Dienstvereinbarung mit dem Personalrat zu treffen. Darin ist auch konkret festzuschreiben, wer aus welchem Grund auf Arbeitszeitdaten zugreifen darf. Hierfür muss auch immer eine Erforderlichkeit zur Aufgabenerfüllung vorliegen.
Nach der in der Stadtverwaltung geltenden Dienstvereinbarung hätten nur der Bürgermeister, die urlaubs- und krankheitsbedingte Vertretung des Bürgermeisters und der von ihm ernannte Datenschutzbeauftragte auf alle Daten der Mitarbeiter zugreifen dürfen. Darüber hinaus hätten die Amtsleiter beschränkt auf „deren“ Mitarbeiter die Arbeitszeitdaten, insbesondere die Anwesenheitszeiten, einsehen können. Auf Nachfrage des TLfDI stellte sich jedoch heraus, dass tatsächlich jeder Mitarbeiter im jeweiligen Amtsbereich (dort als „Abteilung“ bezeichnet) feststellen konnte, aus welchen Gründen andere Mitarbeiter im Zuständigkeitsbereich fehlten. Dies war aus der übersandten Dienstvereinbarung nicht erkennbar und offenbar ursprünglich nicht vorgesehen.
Soweit eine Abwesenheit durch Urlaub, Krankheit, Behördentag, Kind krank, Gleitzeitabbau oder sonstige Dienstfreiheit begründet ist, besteht für die Personalverwaltung die Erforderlichkeit der Erfassung, es besteht aber keine Erforderlichkeit, dass diese konkreten Gründe auch von anderen Mitarbeitern zur Kenntnis genommen werden. Nach den dienstrechtlichen Vorschriften dürfen Auskünfte über Mitarbeiter an andere Mitarbeiter nur im Rahmen des § 85 Thüringer Beamtengesetz gegeben werden. Mangels dort genannter konkreter Auskunftsbefugnisse wäre allenfalls eine Auskunft mit Einwilligung der betroffenen Beschäftigten in Betracht gekommen. Allerdings scheidet auch diese Möglichkeit in diesem Zusammenhang aus, denn eine Einwilligung eines einzelnen Betroffenen im Beschäftigtenverhältnis wäre regelmäßig mangels Freiwilligkeit unwirksam (vgl. § 4 Abs. 2 ThürDSG). Etwas Anderes gilt, wenn eine solche gesetzlich vorgesehen ist oder es für den Beschäftigten eine wirkliche Alternative gibt. Die Übermittlung von Fehlzeiten an die Beschäftigten war daher unzulässig. Es kommt nicht darauf an, aus welchem in der Person des Betroffenen liegenden Grund eine Person fehlt, soweit dies privat durch Urlaub, Erkrankung oder durch sonstige Freistellungsgründe geschieht. Daher ist üblicherweise eine Abwesenheit aus privaten Gründen entweder lediglich mit einem

Sammelbegriff zu bezeichnen oder kann durch eine hierfür gewählte Farbe ersichtlich gemacht werden.
Dienstliche Fehlzeiten wie Dienstgang, Dienstreise oder Weiterbildung zeigen an, dass die betreffende Person grundsätzlich im Dienst und auch grundsätzlich ansprechbar ist. Gegen die Nennung dieser Gründe und auch deren Kenntnis durch die Kollegen bestanden keine Bedenken.
Der TLfDI hat die unzulässige Datenübermittlung der privat veranlassten Fehlzeiten nach § 39 i. V. m. § 33 ThürDSG beanstandet und die Stadtverwaltung aufgefordert, die Anwesenheits- oder Abwesenheitsanzeige so zu gestalten, dass für die anderen Mitarbeiter die konkreten Gründe für eine Abwesenheit, die in der Person des Betroffenen lagen oder die privat veranlasst waren, nicht mehr zu erkennen waren. Es reichte aus, dass lediglich ersichtlich war, dass die Person nicht anwesend und auch nicht ansprechbar war. Dem kam die Stadtverwaltung nach.

Eine Rechtsgrundlage dafür, dass andere Mitarbeiter die Gründe von Fehlzeiten, die nicht dienstlich bedingt sind, differenziert zur Kenntnis nehmen, besteht nicht. Aus einem An- oder Abwesenheitskalender darf für andere Mitarbeiter lediglich ersichtlich sein, ob ein Mitarbeiter ansprechbar ist. Bei Fehlzeiten wegen Urlaub, Krankheit oder in der Person des Beschäftigten liegenden Abwesenheitsgründen reicht es aus, lediglich mit einem Sammelbegriff („Privat“) oder mit einer hierfür zu verwendenden Farbe ersichtlich zu machen, dass ein Beschäftigter nicht im Dienst und nicht ansprechbar ist.

7.8 Ausscheiden aus dem Dienst: An die große Glocke?

Eine Bürgerin teilte dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) mit, dass sie bei einer Stadtverwaltung angestellt war. Sie hatte kurz vor Weihnachten die Zeitung aufgeschlagen und gelesen, dass der Bürgermeister der Gemeinde in einer Pressemitteilung mitgeteilt hat, dass sie ihr Amt zum Ende des Jahres auf eigenen Wunsch verlasse. Sie war bis dato Werkleiterin in einem städtischen Unternehmen gewesen und hatte der Veröffentlichung dieses Umstands ihres Weggangs in der Zeitung nicht zugestimmt. Sie wollte auch weiterhin nicht, dass derartige Informationen an die Öffentlichkeit gelangten und bat den TLfDI, tätig zu werden.

Die datenschutzrechtliche Prüfung ergab:
Bei der Veröffentlichung des Namens der Betroffenen und deren Funktion sowie der Beendigung des Beschäftigungsverhältnisses und des Grundes – auf eigenen Wunsch – handelte es sich um personenbezogene Daten einer Bediensteten im öffentlichen Dienst. Nach § 33 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) gelten für das Verarbeiten oder Nutzen von personenbezogenen Daten über Bedienstete bei öffentlichen Stellen die §§ 79 bis 87 des Thüringer Beamtengesetzes (ThürBG) entsprechend, es sei denn, besondere Rechtsvorschriften des Arbeitsrechts oder tarifvertragliche Regelungen gehen vor. Da keine besonderen Dienstvorschriften in diesem Sinne vorliegen, kommt § 85 Abs. 2 ThürBG zur entsprechenden Anwendung. Danach dürfen von der personalverwaltenden Stelle Auskünfte über Personalaktendaten an Dritte nur mit Einwilligung der Betroffenen gegeben werden, es sei denn, dass die Abwehr einer erheblichen Beeinträchtigung des Gemeinwohls oder der Schutz berechtigter höherrangiger Interessen des Dritten die Auskunftserteilung zwingend erfordern. Die Gründe für die Beendigung eines Beschäftigungsverhältnisses sind unzweifelhaft Personalaktendaten. Auch wenn es für die Bürger durchaus interessant sein könnte, weshalb eine Beschäftigte aus der Stadtverwaltung ausgeschieden ist, stellt dies dennoch keinen der geschilderten gesetzlichen Ausnahmegründe dar. Auch ist das Informationsrecht der Medien in einem solchen Zusammenhang nicht höherrangig zu bewerten. Nach Darlegung der Betroffenen wurde, wie bereits erwähnt, keine Einwilligung zur Veröffentlichung erteilt, sodass auch eine Zulässigkeit der Auskunft mit Einwilligung der Betroffenen, die absolut freiwillig sein müsste, ausschied. Der TLfDI beanstandete das Verhalten des Bürgermeisters.
Er wurde zur Behebung der beanstandeten Verstöße aufgefordert, geeignete Maßnahmen zu treffen, die darauf zielen, zukünftig derartige datenschutzrechtliche Verstöße zu unterbinden. Die Stadtverwaltung kam den Aufforderungen nach.

Die Auskunft einer personalverwaltenden Stelle an eine Zeitung oder ein anderes Medium zum Zweck der Veröffentlichung von Personaldaten, insbesondere zur Beendigung des Beschäftigungsverhältnisses wäre nur mit einer von Freiwilligkeit geprägten Einwilligung des Betroffenen zulässig.

7.9 Aufnahme von Disziplinarvorgängen in die Personalakte

Ein Polizeibeamter des Freistaats Thüringen wandte sich hilfesuchend an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Er bat um datenschutzrechtliche Prüfung, weil er der Meinung war, es seien unzulässigerweise Unterlagen in seine Personalakte aufgenommen worden.
Ihm war im Rahmen einer Anhörung nach § 83 Thüringer Beamtengesetz (ThürBG) Gelegenheit zur Äußerung dazu gegeben worden, dass die Unterlagen zu einer Strafanzeige in seine Personalakte aufgenommen werden sollen, obwohl sie von der Staatsanwaltschaft eingestellt worden war und der Dienstherr keinen Anlass für die Eröffnung eines Disziplinarverfahrens gesehen hatte. Nach der genannten Vorschrift sind Beamte zu Beschwerden, Behauptungen und Bewertungen, die für sie ungünstig sind oder nachteilig werden können, vor der Aufnahme in die Personalakte zu hören. In dem Anhörungsschreiben wurde mitgeteilt, dass aufgrund eines polizeilichen Ermittlungsverfahrens gegen den Beschwerdeführer wegen Nötigung die Einleitung eines Disziplinarverfahrens geprüft worden sei. Im Ergebnis sei von der Einleitung eines Disziplinarverfahrens abgesehen worden. Dem Anhörungsschreiben war die Entscheidung des Dienstvorgesetzten dazu in Kopie beigefügt. Dieser Entscheidung lag die Einstellung des Ermittlungsverfahrens durch die Staatsanwaltschaft zugrunde.
Nach § 86 Abs. 1 ThürBG sind Personalaktendaten über Beschwerden, Behauptungen und Bewertungen aus der Personalakte zu entfernen und zu vernichten, falls sie sich als unbegründet und falsch erwiesen haben. Dies allerdings nur, falls § 78 Abs. 2 und 3 Satz 1 Thüringer Disziplinargesetz (ThürDG) keine Anwendung findet. Das ThürDG bestimmt, dass in der Personalakte enthaltene Vorgänge und Eintragungen über Disziplinarmaßnahmen erst nach Eintritt des Verwertungsverbots aus der Akte zu entfernen sind. Nach § 78 Abs. 3 Satz 1 des ThürDG besteht ein Verwertungsverbot für Disziplinarvorgänge, die nicht zu einer Disziplinarmaßnahme geführt haben. Dieses besteht für Disziplinarvorgänge, die nicht zu einer Disziplinarmaßnahme geführt haben, nach § 78 Abs. 3 Satz 2 ThürDG zwei Jahre nach der Entscheidung. Nach § 78 Abs. 2 ThürDG sind die in der Personalakte enthaltenen Vorgänge und Eintragungen über die Disziplinarmaßnahme nach dem Eintritt des Verwertungsverbotes von Amtswegen zu entfernen oder zu vernichten.

Der Beschwerdeführer war der Auffassung, dass, da weder eine Strafbarkeit noch eine disziplinarrechtliche Relevanz seines Verhaltens festgestellt worden sei, keine weiteren Auswirkungen auf das Dienstverhältnis zu erwarten und die entsprechenden Unterlagen aus der Personalakte zu entfernen seien. Dennoch wurde der Vorgang in die Personalakte aufgenommen mit der Begründung, es handele sich um einen disziplinarrechtlichen Vorgang, der in unmittelbarem Zusammenhang mit dem Dienstverhältnis stehe. Deshalb müssten immer auch die Unterlagen bei Nichteinleitung eines Disziplinarverfahrens zur Personalakte genommen werden.
Auch wenn im vorliegenden Fall keine nachteiligen Auswirkungen auf das Beamtenverhältnis zu erwarten waren, sah der TLfDI keine Aufnahmefähigkeit der beschriebenen Unterlagen in die Personalakte, denn allein das Vorhandensein eines derartigen Vorgangs ist mit einer negativen Tendenz behaftet und kann dem Betroffenen unter Umständen zum Nachteil gereichen. Wird ein strafrechtliches Ermittlungsverfahren nach § 170 Abs. 2 Strafprozessordnung eingestellt, kann dies bedeuten, dass sich die Anzeige als unbegründet oder möglicherweise sogar als falsch erwiesen hat. Demgemäß wären die Unterlagen nach § 86 Abs. 1 Nr. 1 ThürBG unverzüglich aus der Personalakte zu entfernen bzw. erst gar nicht zur Personalakte zu nehmen. Diese Auffassung wurde auch dem Thüringer Ministerium für Inneres und Kommunales (TMIK) als oberstem Dienstherr der Thüringer Polizisten gegenüber vertreten, dass sich aus Sicht des TLfDI auf Rechtsprechung des Bundesverwaltungsgerichtes berufen hatte, die zeitlich vor der Umsetzung der Datenschutzrichtlinie (95/46/EG vom 24. November 1995) lag. Das TMIK legte dar, dass aus seiner Sicht kein Entfernungsbedarf bestehe, weil eine Stigmatisierung der Betroffenen nicht vorliege, sondern im Gegenteil eine Entlastung bzw. Reinwaschung von zu Unrecht erhobenen Vorwürfe darstelle. Aus Sicht des TLfDI würde diesem Anliegen noch stärker Rechnung getragen, wenn derartige Vorgänge erst gar nicht in die Personalakten gelangen würden. Die Aufbewahrung derartiger Vorgänge in Sachakten hätte darüber hinaus auch den Vorteil, dass die Vernichtung nicht vom Antrag eines Betroffenen abhinge, sondern automatisch nach Ablauf der Aufbewahrungsfrist erfolgen muss. Das TMIK wurde daher gebeten, seine Auffassung nochmals zu überdenken. Eine Kontrolle des TLfDI von Stichproben aus Personalakten in einer Landespolizeidirektion in diesem Zusammenhang ergab, dass nur in einem Fall der kontrollierten Personalakten ein Disziplin-

narverfahren tatsächlich eingeleitet worden war. In allen anderen Fällen fanden sich entsprechende Unterlagen über Verdachtsprüfungen gleichwohl in der Personalakte. Dem TMIK wurde nochmals die Auffassung des TLfDI verdeutlicht. In einem Gespräch mit Vertretern des TMIK wurde Einvernehmen dahingehend erzielt, dass Vorgänge, zu denen Vermerke über die Nichteinleitung von Disziplinarverfahren vorliegen, nach § 78 Abs. 3 ThürDSG grundsätzlich zu den Personalakten zu nehmen sind. Dies setzt allerdings eine Einzelfallprüfung voraus, dass die Unterlagen – ebenso wie alle anderen Personalaktenunterlagen – Auswirkungen auf das Dienstverhältnis haben können. Dabei soll nur der Nichteinleitungsvermerk in den hierfür vorgesehenen Teil der Personalakte genommen werden. Die übrigen für die Prüfung der Einleitung eines Disziplinarverfahrens herangezogenen Unterlagen enthalten unter Umständen eine Fülle von personenbezogene Daten, die im eingestellten strafrechtlichen Ermittlungsverfahren erhoben und verarbeitet wurden, die grundsätzlich nicht für die laufende Personalverwaltung erforderlich sind. Diese Unterlagen sollen gesondert in einer Beiakte aufbewahrt werden.

Personalaktendaten über Beschwerden, Behauptungen und Bewertungen sind, falls sie sich als unbegründet oder falsch erwiesen haben, mit Zustimmung des Beamten unverzüglich aus der Personalakte zu entfernen, § 86 ThürBG. Wird die Einleitung eines Disziplinarverfahrens geprüft und abgelehnt, stellt dies bereits einen Disziplinarvorgang dar mit der Konsequenz, dass die hierzu genutzten Unterlagen ebenfalls zur Personalakte gehören, § 73 Abs. 3 ThürDSG, sofern die Einzelfallprüfung ergibt, dass ein Zusammenhang mit dem Dienstverhältnis vorliegt. Dabei soll auch nur der Nichteinleitungsvermerk zur Personalakte genommen werden und die weiteren zur Prüfung genutzten Unterlagen in einer gesonderten Beiakte für die vorgesehen Frist von zwei Jahren aufbewahrt werden

7.10 Aufzeichnungen und Auswertung von Telefongesprächen in einer Rettungsleitstelle

Sensibilisiert durch die Problematik der Aufzeichnung und Auswertung von Notrufen und anderen Anrufen durch die Polizei (vgl. Punkt 8.2) erhielt der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) eine Anfrage, ob es

denn in Ordnung sei, dass in einer Rettungsleitstelle alle Telefon- und Funkgespräche aufgezeichnet würden, ohne dass die Anrufer hierauf hingewiesen würden, und inwieweit die Mitschnitte denn ausgewertet werden dürften, insbesondere wenn sich darunter auch Privatgespräche befänden.

Telefon- und Funkgespräche dürfen nur aufgezeichnet werden, wenn eine Rechtsvorschrift dies erlaubt oder eine Einwilligung des Gesprächsteilnehmers vorliegt, § 4 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG). Die Zulässigkeit und der Umgang mit Aufzeichnungen bei Rettungsleitstellen ergibt sich in erster Linie aus § 31 Thüringer Rettungsdienstgesetz (ThürRettG) in Verbindung mit § 30 ThürRettG. Nach § 31 Abs. 3 ThürRettG sind die am Rettungsdienst Beteiligten „verpflichtet, die Einsätze in der Notfallrettung und im Krankentransport … im erforderlichen Umfang zu dokumentieren." Die durch die Zentralen Leitstellen vermittelten Einsätze sind dabei aufzuzeichnen und auszuwerten. Wenn keine Notrufe betroffen sind, ist das regelmäßige Mithören oder Aufzeichnen von Telefon- und Funkgesprächen zu rein dienstlichen Zwecken durch den Dienstherren grundsätzlich nicht erlaubt. Hat der Dienstherr das Führen privater Telefongespräche erlaubt, so ist an den hierfür vorgesehenen Anschlüssen regelmäßig das Aufzeichnen dieser Gespräche verboten, denn es gilt das Telekommunikationsgeheimnis, § 88 Telekommunikationsgesetz, das sowohl gegenüber den Bediensteten als auch gegenüber deren Kommunikationspartnern zu wahren ist.

Der TLfDI fragte die Rettungsleitstelle zu den konkreten Regelungen im Zusammenhang mit der Aufzeichnung von Telefon- und Funkgesprächen an. Der Träger der Rettungsleitstelle teilte mit, dass alle Telefonate über die Notrufnummer 112 mitgeschnitten und aufgezeichnet würden. Es gäbe noch eine weitere Festnetznummer, die der Rettungsleitstelle zugeordnet sei und von externen Krankenhäusern und Notrufeinrichtungen zur direkten Kontaktaufnahme genutzt werde. Technisch sei diese Leitung erforderlich, weil damit die Leitstellentelefone auch nach außen telefonieren könnten. Auch alle Gespräche über diese Leitung würden mitgeschnitten und aufgezeichnet. Die Mitschnitte und deren Speicherung dienten der Langzeitdokumentation, die Nummer 9.2 des Thüringer Landesrettungsdienstplanes vorschreibt. Man habe aber auch noch zwei interne Telefonnummern, über die die Beschäftigten der Leitstelle interne und externe Telefonate führen könnten, ohne dass diese aufgezeichnet würden.

Eine Dienstanweisung, aus der die notwendigen Festlegungen zur Gesprächsaufzeichnung, die Voraussetzungen, die Speicherungsdauer und Auswertungsmöglichkeiten eindeutig hervorgehen, hat der Träger dem TLfDI bislang nicht vorgelegt. Er teilte mit, es sei ein Neuerlass der notwendigen Dienstanweisung beabsichtigt und ebenfalls die notwendige rein vorsorgliche Beteiligung des Personalrats. Hierzu bat er um datenschutzrechtliche Hinweise, um das Verfahren zu optimieren. Die Beratungsfunktion des TLfDI nach § 40 Abs. 7 ThürDSG setzt jedoch voraus, dass die Stelle, aufgrund der Gegebenheiten vor Ort, zumindest einen Entwurf einer Dienstvereinbarung zur Verfügung stellt. Nachdem die Stelle die „alte“ Dienstvereinbarung und die beabsichtigten Änderungen übersandt hatte, gab der TLfDI eine Stellungnahme ab und wies auf verschiedene Unklarheiten hin. So muss der Komplex zur Aufzeichnung von Gesprächen aufgrund der Bedeutung deutlich und ausführlich in die Dienstvereinbarung aufgenommen werden und nicht nur als kleiner Unterabschnitt unter „Sonstiges“. Zunächst muss die Rechtsgrundlage für Aufzeichnungen konkret benannt werden. Allein ein Verweis auf eine Auflistung von infrage kommenden Gesetzen ohne Paragrafenangaben reicht nicht aus. Darüber hinaus muss in der Dienstvereinbarung erkennbar und differenziert dargelegt werden, ob die Gespräche automatisiert oder händisch aufgezeichnet werden. Bei nicht automatischer Aufzeichnung müssen konkrete Abgrenzungskriterien aufgezählt werden. Der TLfDI bat daher um Übersendung einer entsprechend überarbeiten Dienstvereinbarung.

Telefon- und Funkgespräche dürfen nur aufgezeichnet werden, wenn eine Rechtsvorschrift dies erlaubt oder eine Einwilligung des Gesprächsteilnehmers vorliegt, § 4 ThürDSG. Die Zulässigkeit und der Umgang mit Aufzeichnungen bei Rettungsleitstellen ergibt sich in erster Linie aus § 31 Thüringer Rettungsdienstgesetz (ThürRettG) in Verbindung mit § 30 ThürRettG. Es dürfen nur die zu dokumentierenden Gespräche aufgezeichnet werden. Zur konkreten Ausgestaltung bedarf es ergänzender Festlegungen der verantwortlichen Stelle in Form einer Dienstanweisung oder Dienstvereinbarung.

7.11 Ist denn auch genug Personal da?

Die beim Thüringer Landesverwaltungsamt angesiedelte Heimaufsicht ist zuständig für die Durchsetzung des Thüringer Wohn- und

Teilhabegesetzes (ThürWTG) bei Einrichtungen für Menschen mit Behinderung. Ein Landesverband, von dem eine Vielzahl von Einrichtungen für Menschen mit Behinderungen in Thüringen als Mitglieder beraten wird, hat sich mit der Bitte um datenschutzrechtliche Beratung an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) gewandt. Hintergrund war, dass die zuständige Heimaufsicht von den Mitgliedseinrichtungen regelmäßig mittels eines Vordruckes die Auflistung der in der Einrichtung arbeitenden Mitarbeiter nach Namen, Lebensalter, Qualifikation und geleisteten Arbeitsstunden, gestützt auf die §§ 5 und 6 der Heimpersonalverordnung (HeimPersV), anfordert. Auch sollten einmal jährlich Angaben bezüglich der Ausfallzeiten bzw. Langzeiterkrankungen der Mitarbeiter gemacht werden. Der der Anfrage beigefügte Vordruck zur Auflistung der Mitarbeiterdaten findet ausweislich der aufgedruckten Informationen seine Rechtsgrundlage in § 10 Abs. 3 Nr. 2 und Abs. 1 Nr. 5 ThürWTG. Der TLfDI bat die Heimaufsicht um Mitteilung, für welche konkreten Zwecke der vorliegende Bogen vorgesehen ist und ob er ggf. auch für andere Zwecke genutzt wird, ohne dass dies kenntlich gemacht wird.

Die Heimaufsicht teilte mit, dass Sinn und Zweck der Erhebung und Verwendung der Personaldaten sei, nachzuweisen, dass die Beschäftigten in ausreichender Zahl entsprechend den Anforderungen vorhanden sind und die persönliche und fachliche Eignung vorliegt. Nach § 10 Abs. 1 Satz 2 Nr. 4 und Nr. 5 ThürWTG sind der Heimaufsicht Erstmeldungen unter Angabe des Namens, der beruflichen Ausbildung und des beruflichen Werdegangs des Leiters der stationären Einrichtung bzw. des Pflegedienstleiters sowie der jeweiligen Stellvertreter und die Namen und die berufliche Ausbildung der Pflege- und Betreuungskräfte mit Geburtsjahr, vorgesehener Tätigkeit und wöchentlicher Arbeitszeit zu machen. Weitere Angaben und Nachweise können nach § 10 Abs. 2 ThürWTG verlangt werden. Auch sind nach Aufnahme des Betriebs Veränderungen in der Leitung unverzüglich zu melden, § 10 Abs. 3 Nr. 1 Buchstabe a) ThürWTG. Veränderungen bei den Mitarbeitern sind quartalsmäßig mitzuteilen. Die entsprechenden Mitteilungen beschränken sich dann auf die tatsächlichen Änderungen, eine vollständige Auflistung ist zu diesem Zweck nicht notwendig.

Nach dem von der Heimaufsicht geschilderten Sachverhalt erfolgt eine jährliche Abfrage des gesamten Personalbestands, was für Regelprüfungen im Sinne des § 15 Abs. 1 Satz 2 ThürWTG grundsätz-

lich zulässig ist. Die Übermittlung von Prüfergebnissen an andere Institutionen/Einrichtungen der Eingliederungshilfe nach dem Sozialgesetzbuch (SGB) Zwölftes Buch (XII) erfolgt anonymisiert, d. h. ohne Angabe von personenbezogenen Daten.
Gegen die dargestellte Verfahrensweise der Heimaufsicht bestanden angesichts der bestehenden gesetzlichen Befugnis keine datenschutzrechtlichen Bedenken. Dies wurde dem Landesverband mitgeteilt.

Gegen die Datenabfrage der Heimaufsicht von den Mitgliedseinrichtungen nach § 10 ThürWTG zum Zweck des Nachweises, dass die Beschäftigten in ausreichender Zahl vorhanden sind und die persönliche und fachliche Eignung vorliegt, bestehen angesichts der eindeutigen gesetzlichen Regelung datenschutzrechtlich keine Bedenken.

7.12 Namen an den Amtsstuben

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) erhielt die Anfrage eines Beschäftigten im öffentlichen Dienst, ob es aus datenschutzrechtlichen Aspekten zulässig ist, dass der vollständige Vor- und Zuname des Beamten oder Beschäftigten an den Dienstzimmern in einem Landratsamt angebracht ist. Beweggrund für die Anfrage waren bekannt gewordene Aktivitäten der sogenannten Reichsbürger gegen Beschäftigte im öffentlichen Dienst. Demnach ließen Reichsbürger fiktive Geldforderungen in ein amerikanisches UCC-Register eintragen, um diese dann über ein maltesisches Inkassobüro bei den vermeintlichen Schuldnern eintreiben zu lassen (sogenannte Malta-Masche). Bei der Online-Eintragung in das Register, das in jedem US-Bundesstaat existiert und eine Art Pfandregister darstellt und der Eintragung von Sicherungsrechten dient, wird nämlich nur geprüft, ob die notwendigen Angaben eingegeben werden, nicht jedoch, ob eine Forderung tatsächlich besteht. Der Bedienstete befürchtete, selbst Opfer werden zu können, da sein Vor- und Zuname an seiner Tür zum Dienstzimmer für jeden Besucher ersichtlich war.
Das Thema Namensschilder an den Türen in öffentlichen Stellen ist immer wieder Gegenstand der datenschutzrechtlichen Diskussion (vgl. bereits 2. Tätigkeitsbericht des TLfD unter 6.8). Entscheidet sich eine öffentliche Stelle dazu, die Namen ihrer Bediensteten samt ihrer Dienstbezeichnung an den Türen anzubringen, wird dies in der

Regel mit Bürgerfreundlichkeit und Ansprechbarkeit begründet. Mit diesem Vorgehen ist eine Datenübermittlung gemäß § 22 Thüringer Datenschutzgesetz (ThürDSG) an die Besucher durch Veröffentlichung der Namen der Bediensteten verbunden, auch wenn die Namen zunächst nur im Amt zur Kenntnis genommen werden können. Die Rechtsprechung hat durch verschiedene Entscheidungen die Veröffentlichung von Mitarbeiterdaten öffentlicher Stellen weitgehend für zulässig erklärt. Der TLfDI vertritt auch weiterhin die Auffassung, dass eine Erforderlichkeit für die Veröffentlichung von Mitarbeiterdaten, um die Ansprechbarkeit der Ämter zu ermöglichen, gegeben sein muss. Die Angabe des Vornamens ist demnach grundsätzlich nicht erforderlich, seine Veröffentlichung darf daher nur mit Einwilligung des betreffenden Bediensteten erfolgen (§ 4 Abs. 1 ThürDSG). Die Wirksamkeit der Einwilligung setzt voraus, dass die Bediensteten frei entscheiden können, ob sie ihren Vornamen auf dem Türschild haben wollen oder nicht (§ 4 Abs. 2 ThürDSG).

Selbstverständlich besteht die Gefahr, dass die Namen von Beschäftigten im öffentlichen Dienst beispielsweise unter Zuhilfenahme des Internets mit weiteren Angaben zusammengeführt werden können. Es kann ein Leichtes sein, beispielsweise die Privatadresse oder Vereinszugehörigkeiten oder private Aktivitäten hinzuzufügen, wenn auch diese veröffentlicht sind. In Bereichen, in denen eine besondere Gefährdung für die Privatsphäre der Beschäftigten droht, sollte daher immer sorgfältig geprüft werden, ob und in welcher Form die Namen der Beschäftigten veröffentlicht werden. Eine vollständige Anonymität der öffentlich Bediensteten in ihrer Tätigkeit ist jedoch weder möglich noch geboten. Immerhin sind amtliche Schreiben grundsätzlich im Auftrag oder Vertretung der Behörde zu unterzeichnen. Allein die Befürchtung, der Name des Bediensteten könne für eingangs dargestellte Zwecke genutzt werden, reicht grundsätzlich nicht aus, die generelle Anbringung von Namensschildern an den Bürotüren als unzulässig zu bewerten.

Ist ein Bediensteter mit der Anbringung des Namens an der Bürotür nicht einverstanden, kann er sich auch an den örtlichen Personalrat und/oder an den behördlichen Beauftragten für den Datenschutz wenden. Sollte seinem Anliegen seitens seiner Beschäftigungsbehörde nicht nachgekommen werden, besteht die Möglichkeit der Anrufung des TLfDI nach § 11 Thüringer Datenschutzgesetz, der die Erforderlichkeit und Zulässigkeit im Einzelfall überprüft.

Es ist grundsätzlich zulässig, die Nachnamen und die Dienstbezeichnung an den Bürotüren in öffentlichen Stellen anzubringen. Der Vorname des Betroffenen hingegen darf nur mit dessen Einwilligung auf das Türschild. Droht aufgrund der Tätigkeit eine besondere Gefährdung für die Privatsphäre, muss auf die Beschriftung an der Tür verzichtet werden.

7.13 Daten gegen Fördermittel

Die Durchführung der Programme „Öffentlich geförderte Beschäftigung und gemeinwohlorientierte Arbeit in Thüringen“ (ÖGB) und „Arbeit in Thüringen“ war auch mit der Verarbeitung personenbezogener Daten der an den Projekten dieser Programme Teilnehmenden verbunden. Die Gesellschaft für Arbeits- und Wirtschaftsförderung des Freistaats Thüringen mbH (GFAW) bat den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) diesbezüglich um Beratung.

Da die Maßnahmen aus Mitteln des Freistaats Thüringen finanziert werden, müssen einerseits bei den Teilnehmern der Projekte die Voraussetzungen für die Teilnahme vorliegen und andererseits die Verwendung der Mittel nach der Thüringer Landeshaushaltsordnung nachprüfbar sein. Mit dem Antrag auf Teilnahme und damit der Anerkennung der Teilnahmebedingungen erklären sich die Teilnehmer bereits damit einverstanden, dass ihre Daten auf der Rechtsgrundlage der Förderrichtlinien erhoben und verarbeitet werden.

Zum Zeitpunkt des Eintritts in das Projekt mussten die Teilnehmer Angaben zur persönlichen und beruflichen Situation auf einem hierfür vorgesehen Erhebungsbogen, der in elektronischer Form zur Verfügung gestellt werden sollte, machen. Dazu gehörten auch Fragen zu einer möglichen Behinderung und zum möglichen Migrationshintergrund, deren Beantwortung allerdings freiwillig war. Hierauf wird auch bei der elektronischen Erfassung deutlich hingewiesen.

Bei Austritt aus dem Projekt werden wiederum weitere Angaben benötigt, die auf die Veränderung der beruflichen Situation der Teilnehmer abzielten, um die Effizienz der Förderung prüfen zu können.

Mit der Erfassung der Teilnehmerdaten waren die Maßnahmeträger beauftragt, bei denen die geförderten Personen eingesetzt waren. Die erhobenen Daten wurden von den Maßnahmeträgern im Auftrag des

Thüringer Ministeriums für Arbeit, Soziales, Gesundheit, Frauen und Familie (TMASGFF) über das bei der GFAW betriebene Portal bei der Thüringer Aufbaubank (TAB) erfasst und in einer Datenbank bei der TAB gespeichert. Von dort wurden die Daten ohne Namen und Adressen der Teilnehmer an das TMASGFF weitergegeben.
Zur Bewertung der Wirksamkeit der Maßnahme und deren Effizienz werden Forschungsinstitute beauftragt, die die Evaluierung der entsprechenden Förderprogramme untersuchen.
Da die Teilnehmerdaten für die dargestellten Zwecke erforderlich waren, wurde besonderes Augenmerk auf die Information und Aufklärung der Teilnehmer gelegt, denn jeder muss wissen können, wer wann wie mit seinen personenbezogenen Daten umgeht. Hierzu wurde von der GFAW ein Merkblatt für die Teilnehmer an der Fördermaßnahme erarbeitet, das nach Prüfung durch den TLfDI die aus datenschutzrechtlicher Sicht erforderlichen Informationen enthält.

Welche personenbezogenen Daten von Teilnehmern einer Fördermaßnahme erhoben und erarbeitet werden dürfen, hängt von deren konkreter Erforderlichkeit zur Aufgabenerfüllung ab. Besondere Bedeutung kommt in diesem Zusammenhang der Information der Betroffenen zu. Entsprechende Merkblätter müssen daher in gut verständlicher Form die Rechtsgrundlage für die Verarbeitung personenbezogener Daten angeben, die verarbeitende und verantwortliche Stelle bezeichnen und die Verarbeitung der personenbezogenen Daten nachvollziehbar aufzeigen. Auch muss ein Merkblatt Auskunft darüber geben, wie lange die Daten aufbewahrt werden.

7.14 Dienstvereinbarung zur elektronischen Kommunikation: dienstlich und privat dem Datenschutz verpflichtet

Im Februar 2016 bat ein kommunaler Datenschutzbeauftragter den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), in Unterstützung nach § 40 Abs. 7 Thüringer Datenschutzgesetz den Entwurf einer Dienstvereinbarung (DV) über den Zugang und die Nutzung von elektronischen Kommunikationssystemen in der Stadtverwaltung datenschutzrechtlich zu bewerten. Hintergrund war, dass der Entwurf der DV auf Widerstand bei den Beschäftigten der Behörde gestoßen war, weil die private Nutzung des dienstlichen E-Mail-Accounts verboten und die Einhaltung dieses Verbots durch Protokollierung und Auswertung der Internet- und

E-Mail-Nutzung der Mitarbeiter überprüft werden sollte. Der TLfDI verwies zunächst auf die Orientierungshilfe zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz (abrufbar unter https://www.tlfdi.de/mam/tlfdi/gesetze/orientierungshilfen/oh_arbeitsplatz.pdf) und befürwortete das Verbot der privaten Nutzung des dienstlichen E-Mail-Accounts, da es nicht ratsam ist, als Teledienstanbieter gegenüber den Bediensteten zu gelten und wies auf folgende Punkte hin: In der DV war festgelegt, dass die Internet-Protokolle durch einen vom Bürgermeister schriftlich beauftragten Mitarbeiter regelmäßig stichprobenhaft hinsichtlich der aufgerufenen Internetseiten gesichtet und in aggregierter Form (ohne Nennung von Namen und anderen Identifizierungsmerkmalen) ausgewertet werden. Die Auswertung der Übersicht des Gesamtdatenvolumens sollte monatlich ebenfalls durch diesen Mitarbeiter sowie durch den behördlichen Datenschutzbeauftragten erfolgen. Der Personalrat kann auf eigenen Wunsch beteiligt werden.

In der DV wird gefordert, dass die Beschäftigten, wenn sie private E-Mails empfangen, den Absender der privaten E-Mail darüber informieren müssen, dass die Nutzung des dienstlichen E-Mail-Accounts für private Zwecke nicht statthaft ist. Mit dieser Information wird jedoch gleichzeitig das Bestehen eines dienstlichen E-Mail-Accounts bestätigt. Somit würde die bestehende Forderung, eine Bekanntgabe der dienstlichen E-Mail-Adresse ohne dienstliche Notwendigkeit zu vermeiden, unterlaufen. Daher sollte die Verpflichtung zur Information eines privaten Absenders nur auf diejenigen Absender beschränkt werden, der dem Beschäftigten bekannt ist. Weiterhin war in der DV festgelegt, dass mit Beendigung des Beschäftigungsverhältnisses die E-Mail-Adresse des jeweiligen Beschäftigten ihm nicht mehr zur weiteren Nutzung zur Verfügung steht. Der Beschäftigte muss die außerbehördlichen Kommunikationspartner über diesen Umstand informieren. Dazu regte der TLfDI eine Prüfung an, ob die entsprechende E-Mail-Adresse nicht gänzlich gelöscht werden könne, anstatt sie – gemäß Formulierung – nur der Nutzung des ausgeschiedenen Beschäftigten zu entziehen. Denn bei Fortbestehen der Adresse können dort weiterhin E-Mails eingehen, die weiterbearbeitet werden oder im Falle privater Inhalte gelöscht werden müs-

sen. Dass an einen bestimmten Mitarbeiter gerichtete dienstliche E-Mails an zuständige Beschäftigte weitergeleitet werden, ist nicht in jedem Falle erforderlich. Daher sollte von den zuständigen Behördenmitarbeitern geprüft werden, ob die E-Mail-Absender lediglich eine Nachricht erhalten, dass die angeschriebene E-Mail-Adresse nicht mehr besteht oder dass sich der Absender an eine andere Stelle, beispielsweise die allgemeine Poststelle wenden soll.
Der TLfDI regte außerdem an, für alle Geheimnisträger Funktionsaccounts (auf die fachliche Funktion bezogene, nicht namentliche E-Mail-Adressen) einzurichten, die definitiv von einer Kontrolle auszunehmen sind.

Die Protokollierung und Auswertung der Internet- und E-Mail-Nutzung der Mitarbeiter zur Kontrolle von Missbrauch ist nur in sehr engen Grenzen zulässig. Mit Beendigung des Beschäftigungsverhältnisses eines Bediensteten sollte dessen dienstlicher E-Mail-Account gelöscht werden, um zu vermeiden, dass auf dem Account weiterhin E-Mails eingehen. Für den dienstlichen E-Mail-Kontakt mit Außenstehenden empfiehlt es sich, die Funktionspostfächer als E-Mail-Adresse anzugeben, da somit auch für private Absender ersichtlich ist, dass der E-Mail-Kontakt ausschließlich auf die dienstliche Nutzung beschränkt ist.

7.15 Beschwerde über Zugriff auf Personalakten beim Landgericht

Ein Richter wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), weil er vom Vorsitzenden der Kammer an einem Landgericht, der er angehörte, auf seine Unterlagen, die er zur Bewerbung in den Justizdienst des Landes eingereicht hatte, angesprochen wurde. Er vermutete daher eine unzulässige Einsichtnahme in seine Personalakte.
Nach § 11 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) kann sich jedermann unmittelbar an den Landesbeauftragten für den Datenschutz mit dem Vorbringen wenden, dass bei der Verarbeitung oder Nutzung seiner personenbezogenen Daten durch öffentliche Stellen seine schutzwürdigen Belange beeinträchtigt werden. Das Thüringer Datenschutzgesetz ist nach § 2 Satz 6 ThürDSG für Gerichte nur anwendbar, soweit sie in Verwaltungsangelegenheiten

tätig werden. Unter den Begriff der Verwaltungstätigkeit fällt dabei auch die Personalverwaltung bei Gericht.
Der Landesbeauftragte für den Datenschutz kontrolliert nach § 37 ThürDSG bei allen öffentlichen Stellen die Einhaltung der Bestimmungen dieses Gesetzes und anderer Rechtsvorschriften über den Datenschutz. Im Hinblick auf Personalakten finden sich datenschutzrechtliche Bestimmungen in den §§ 79 bis 87 des Thüringer Beamtengesetzes (ThürBG). Nach § 79 Abs. 1 ThürBG darf der Dienstherr personenbezogene Daten über Bewerber, Beamte und ehemalige Beamte nur verarbeiten, soweit dies zur Begründung, Durchführung, Beendigung oder Abwicklung des Dienstverhältnisses oder zur Durchführung organisatorischer, personeller und sozialer Maßnahmen erforderlich ist oder eine Rechtsvorschrift dies erlaubt. Zugang zu Personalakten dürfen nur Beschäftigte haben, die im Rahmen der Personalverwaltung mit der Bearbeitung von Personalangelegenheiten beauftragt sind, und nur, soweit dies zu Zwecken der Personalverwaltung oder der Personalwirtschaft erforderlich ist, § 80 Abs. 1 ThürBG.
Vom Präsidenten des Landgerichts als Verwaltungsbehörde und personalnebenaktenführender Stelle wurde auf die Anfrage des TLfDI mitgeteilt, dass der Vorsitzende Richter zunächst aus der Personalakte Kenntnisse über die frühere Tätigkeit des Beschwerdeführers ohne die Möglichkeit der Einsicht in die Personalakte erhalten hatte, weil der berufliche Werdegang für den beabsichtigten Einsatz in der Kammer von Bedeutung war. Hiergegen war datenschutzrechtlich nichts einzuwenden, denn die bekannt gewordenen personenbezogenen Daten zum beruflichen Werdegang können für den Einsatz in der Kammer und damit für die Durchsetzung der Personalentscheidung (Einsatz in der Kammer) als erforderlich angesehen werden. Eine unzulässige Nutzung der Informationen zum Werdegang als Personalaktenbestandteil für Zwecke außerhalb des Personaleinsatzes konnte nicht festgestellt oder unterstellt werden.
Ergänzend wurde mitgeteilt, dass der Vorsitzende Richter am Landgericht zu einem späteren Zeitpunkt Einsicht in die dort geführten Personalunterlagen zu dem Beschwerdeführer erhalten hatte. Dazu sei er in seiner Aufgabenerfüllung als dienstältester und lebensältester Vorsitzender Richter am Landgericht, der bei Abwesenheit/Verhinderung des Präsidenten und des Vizepräsidenten gemäß § 21h Gerichtsverfassungsgesetz zu deren Vertretung berufen war, grundsätzlich befugt gewesen, sofern eine Personalentscheidung zu

treffen war. Welcher konkrete Anlass zur Personalakteneinsicht geführt hat, konnte im Nachhinein allerdings noch nicht festgestellt werden. Dies ist weiter zu überprüfen.

Zugang zu Personalakten dürfen nur Beschäftigte haben, die im Rahmen der Personalverwaltung mit der Bearbeitung von Personalangelegenheiten beauftragt sind, und nur, soweit dies zu Zwecken der Personalverwaltung oder der Personalwirtschaft erforderlich ist, § 80 Abs. 1 ThürBG.
Informationen zum beruflichen Werdegang können für den konkreten Einsatz in einem bestimmten Bereich erforderlich sein und begegnen in einem solchen Fall keinen datenschutzrechtlichen Bedenken.

7.16 Der Justiz-Postweg einer „vertraulichen Personalsache“

Ein Richter an einem Thüringer Amtsgericht beschwerte sich beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) darüber, dass ein inhaltlich an ihn gerichtetes Schreiben in einer vertraulichen Personalangelegenheit ohne den Vermerk „vertrauliche Personalsache“ und unter Nennung einer nicht existierenden Person (der Vorname des Beschwerdeführers war mit dem Nachnamen eines anderen Richters kombiniert) vom Präsidenten des Oberlandesgerichts versandt wurde. Dies habe nämlich dazu geführt, dass der Brief von mehreren Personen geöffnet worden war, um den Adressaten festzustellen. Außerdem befänden sich in seiner Personalakte Unterlagen, die längst hätten entfernt werden müssen.
Der TLfDI schrieb den Präsidenten des Oberlandesgerichts (OLG) an und bat um Stellungnahme zu dem Schreiben und gleichzeitig um Auskunft darüber, welche Personalaktenunterlagen über den Betroffenen wo vorhanden sind, um diese nach § 37 Thüringer Datenschutzgesetz zu überprüfen. Zur Erläuterung ist auszuführen, dass die Aufgabenwahrnehmung der Personalverwaltung im Justizbereich auf verschiedene Stellen aufgeteilt ist. Das führt dazu, dass sich Personalaktendaten eines Richters beim Amtsgericht, dem für den Gerichtsbezirk zuständigen Landgericht, dem Oberlandesgericht und darüber hinaus auch im für Justiz zuständigen Ministerium befinden. Alle diese Unterlagen bilden in ihrer Gesamtheit die Personalakte, die sich in Grundakte und Teilakten gliedern kann, § 81 Abs. 2

Satz 1 Thüringer Beamtengesetz (ThürBG). Teilakten können nach § 81 Abs. 2 Satz 2 ThürBG bei der für einen betreffenden Aufgabenbereich zuständigen Behörde geführt werden, bestes Beispiel ist hierfür die Besoldungsakte. Nebenakten (Unterlagen, die sich auch in der Grundakte oder in Teilakten befinden) dürfen nur geführt werden, wenn die personalverwaltende Behörde nicht zugleich Beschäftigungsbehörde ist oder wenn mehrere personalverwaltende Behörden für den Betreffenden zuständig sind (§ 81 Abs. 2 Satz 3 ThürBG). Dabei dürfen nur Unterlagen mit personenbezogenen Daten bei der jeweiligen Stelle vorhanden sein, die zur rechtmäßigen Aufgabenerledigung erforderlich sind. Der TLfD hatte sich bereits im Berichtszeitraum 1996/1997 (vgl. 2. TB des TLfD 6.5) damit beschäftigt.

Der Präsident des Oberlandesgerichts teilte mit, der Betroffene habe zu Recht moniert, dass ein inhaltlich an ihn gerichtetes Schreiben mit einer falschen Namensnennung versandt wurde. Es habe sich aber nicht um eine klassische „vertrauliche Personalsache“ gehandelt, sondern es stand im Zusammenhang mit der Bearbeitung von Dienstaufsichtsbeschwerden, die der Beschwerdeführer eingereicht hatte. Die Unterlagen hierzu und auch das Schreiben werden als Verwaltungsvorgang, für den der Präsident des OLG zuständig ist, geführt. Bei der Ausfertigung der Schreiben sei es versehentlich zu der falschen Namensnennung gekommen, die letztendlich im Adressfeld genannte Person gab es nicht. Da das Schreiben an die genannte Person „persönlich“ adressiert war, hätte es nach den geltenden Regelungen auch nur von dieser Person geöffnet werden dürfen.

Zur Frage der vorhandenen Personalakte wurde erläutert, das Original der Personalakte werde beim Dienstherrn, dem Thüringer Ministerium für Migration, Justiz und Verbraucherschutz geführt. Der unmittelbare Dienstvorgesetzte, der Landgerichtspräsident, und der höhere Dienstvorgesetzte, der Präsident des Thüringer OLG, führten jeweils Spiegelakten. Dies ließ die Vermutung zu, dass möglicherweise deckungsgleiche Personalunterlagen bei den genannten Stellen vorhanden sein könnten, was eigentlich aufgrund der gesetzlichen Vorschriften ausgeschlossen sein sollte, es sei denn, alle Stellen nehmen dieselben Aufgaben zu dem Betroffenen wahr oder benötigten für die jeweilige Aufgabenerfüllung alle Unterlagen. Daher wurde eine datenschutzrechtliche Kontrolle vor Ort angesetzt, die zu folgendem Ergebnis führte:

Das besagte falsch adressierte Schreiben befand sich im Original nebst geöffnetem Umschlag in einer gesondert geführten Sachakte zu einer Dienstaufsichtsbeschwerde. Auf dem Briefumschlag war der Eingangstempel des Justizzentrums Jena ersichtlich. Das Adressfeld war durchgestrichen und handschriftlich der Vermerk „trotz Aushang an Gerichtstafel lässt sich Empfänger nicht ermitteln“ aufgebracht. Ein Hinweis auf den Aussteller dieses Vermerks fand sich nicht. Ob das Schreiben im Amtsgericht geöffnet wurde, ließ sich letztendlich nicht mehr feststellen. Da die Anrede im Schreiben selbst den Beschwerdeführer bezeichnete, hätten im Falle einer Öffnung des Schreibens die möglichen Betroffenen angesprochen werden können, um eine Klärung herbeizuführen.
Eine Vorschrift zum Aushang an der Gerichtstafel in vergleichbaren Fällen existiert nicht. Ein Aushang war daher nicht zulässig. Wer die Postsendung an der Gerichtstafel ausgehangen hatte, konnte jedoch ebenfalls nicht festgestellt werden. Weitergehende Ermittlungsmöglichkeiten, dies aufzuklären, boten sich allerdings nicht.
Wie es zu der Kombination des Vornamens des betreffenden Richters mit dem Nachnamen eines anderen Richters gekommen ist, ließ sich nur durch ein Versehen erklären. Während der Kontrolle wurde ein neues an den Beschwerdeführer gerichtetes Schreiben vorgelegt, in dem das Bedauern über die fehlerhafte Adressierung zum Ausdruck gebracht wurde. Es war davon auszugehen, dass durch die vorgenommene interne Prüfung und Auswertung des Vorfalls durch das OLG zur Sensibilisierung hinsichtlich der Kontrolle der richtigen Adressierung geführt hat. Weitere zu treffende geeignete Maßnahmen zur Sicherstellung der Einhaltung der datenschutzrechtlichen Vorschriften waren nicht ersichtlich und damit auch nicht zu fordern.
Die Einsicht in die beim OLG geführte Personalakte ergab, dass es sich um eine Personalnebenakte handelte. Zu diesem grundsätzlichen Komplex der Führung von Personalakten und Personalnebenakten der Richter wurde ergänzend ebenfalls in die beim Thüringer Ministerium für Migration, Justiz und Verbraucherschutz geführten Personalunterlagen Einsicht genommen. Der Vollständigkeit halber ist beabsichtigt, auch in die Personalnebenakte im Landgericht Einsicht zu nehmen, um eine grundsätzliche datenschutzrechtliche Bewertung auf der Grundlage der Aufgabenverteilung vorzunehmen und entsprechende Forderungen aufstellen zu können. Die Prüfung ist noch nicht abgeschlossen.

Auch wenn die erforderlichen Regelungen nach § 9 ThürDSG getroffen sind, damit Schreiben ungeöffnet und damit inhaltlich auch nur dem Adressaten zur Kenntnis gelangen, ist der menschliche Faktor, dass es bei der Adressierung zu einem Versehen kommen kann, nicht vollständig auszuschließen. Es kommt maßgeblich auf die konkrete Aufgabenerfüllung im Bereich der Personalverwaltung an, um zu beurteilen, welche Personalaktendaten dort in welcher Form – Grundakte, Teilakten, Nebenakten – vorhanden sein dürfen (§ 81 Abs. 2 ThürBG).

7.17 Die Stadtverwaltung als Personalvermittler: (kein) Datenschutz für Bewerbungsunterlagen

Eine Beschwerdeführerin hatte sich bei einer Thüringer Stadt auf deren ausgeschriebene Stelle als „Stadtarchitektin“ beworben. Einige Zeit später erhielt die Beschwerdeführerin Post von einem privaten Architekturbüro, das ihr ein Stellenangebot unterbreitete. Das Architekturbüro gab in seinem Schreiben an, die Informationen über die Stellensuche der Beschwerdeführerin von der Stadt erhalten zu haben, bei der sich die Beschwerdeführerin als Architektin beworben hatte. Die Beschwerdeführerin vermutete, dass sie Stadt ihre Bewerbungsunterlagen unberechtigterweise weitergeben hatte.
Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) bat daraufhin die Stadtverwaltung um Stellungnahme zu dem Sachverhalt. Insbesondere wollte der TLfDI wissen, welche Personen der Stadtverwaltung Zugang zu Bewerbungsunterlagen haben, wie und wo die Unterlagen aufbewahrt und wann die Unterlagen ggf. vernichtet werden.
In ihrer Stellungnahme beantwortete die Stadtverwaltung alle gestellten Fragen und teilte mit, dass der Bauamtsleiter der Stadtverwaltung offensichtlich regelmäßig private Unternehmen über eingegangene Bewerbungen in der Stadt informiert hatte. Dementsprechend hatte er auch das Architekturbüro über die Bewerbung der Beschwerdeführerin in Kenntnis gesetzt, ohne dass er dazu befugt war. Somit hatte der Amtsleiter unbefugt personenbezogene Daten an einen Dritten außerhalb der Stadtverwaltung weitergegeben.
Der TLfDI bewertete diesen Sachverhalt datenschutzrechtlich folgendermaßen:
Nach § 33 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) in Verbindung mit § 79 Abs. 1 Thüringer Beamtengesetz (ThürBG) darf

eine öffentliche Stelle als Dienstherr personenbezogene Daten über Bewerber verarbeiten, soweit dies zur Begründung eines Dienstverhältnisses erforderlich ist. Die Bewerberdaten unterliegen insoweit einem besonderen Schutz und dürfen nur den Stellen oder Personen zugänglich gemacht werden, die am Bewerbungsverfahren beteiligt sind (§ 80 Abs. 1 ThürBG).
Nach Darlegung der Stadtverwaltung hatten auf die Bewerbung der Beschwerdeführerin der Bürgermeister, die mit Personalangelegenheiten befassten Personen sowie der Bauamtsleiter und die Stadtarchitektin Zugang. Insofern waren die fachlich zuständigen Personen einbezogen. Hiergegen hatte der TLfDI datenschutzrechtlich nichts einzuwenden. Jedoch ermächtigt die Kenntnis von Bewerberunterlagen mit personenbezogenen Daten durch befugte Personen nicht dazu, diese Daten an Dritte weiterzugeben. Somit hatte der Bauamtsleiter die personenbezogenen Daten unbefugt weitergegeben.
Auch wenn offensichtlich „nur“ der Bauamtsleiter bewusst gegen die datenschutzrechtlichen Vorschriften verstoßen hat, ist dies der öffentlichen Stelle, die den Datenschutz nach § 34 ThürDSG sicherzustellen hat, zuzurechnen; im vorliegenden Falle der Stadtverwaltung bzw. dem sie vertretenden Bürgermeister.
Daher beanstandete der TLfDI die unbefugte Datenweitergabe gemäß § 39 ThürDSG. Zudem forderte der TLfDI den Bürgermeister auf, die erforderlichen Maßnahmen zu treffen, um zukünftig die Einhaltung der datenschutzrechtlichen Vorschriften sicherzustellen. Dazu regte der TLfDI an, Bewerberunterlagen als „vertraulich“ zu kennzeichnen und die Weitergabe an Dritte explizit zu versagen. Der TLfDI wies darauf hin, dass wegen des Verstoßes gegen datenschutzrechtliche Vorschriften dienst- bzw. arbeitsrechtliche Konsequenzen erforderlich sind.
Nach § 43 Abs. 1 ThürDSG handelt ordnungswidrig, wer unbefugt personenbezogene Daten, die nicht offenkundig sind, übermittelt oder nutzt. Zuständig für die Verfolgung ist nach § 8 Abs. 1 der Thüringer Verordnung zur Bestimmung von Zuständigkeiten im Geschäftsbereich des Innenministeriums (InMinZustVTH) diejenige Behörde, der der Vollzug derjenigen Vorschriften obliegt, gegen die sich der Verstoß richtet. Hierzu ist die Angelegenheit der für die Verfolgung von Ordnungswidrigkeiten zuständigen Verwaltungsbehörde zuzuleiten.

Nach § 33 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) darf eine öffentliche Stelle als Dienstherr personenbezogene Daten über Bewerber verarbeiten. Dies gilt auch für die Begründung von Beschäftigungsverhältnissen. Die öffentliche Stelle, die den Datenschutz nach § 34 ThürDSG sicherzustellen hat, ist für durch Mitarbeiter/innen begangene Verstöße in ihrem Geschäftsbereich verantwortlich. Nach § 43 Abs. 1 ThürDSG handelt ordnungswidrig, wer unbefugt personenbezogene Daten, die nicht offenkundig sind, übermittelt oder nutzt. Somit sind entsprechende Verstöße arbeits- bzw. dienstrechtlich zu ahnden.



Rücken eines Polizisten – © Picture-Factory / Fotolia.com

8. Polizei

8.1 Immelborn – Ad Acta: Zwischenbericht des Untersuchungsausschusses 6/2 liegt jetzt vor: Handeln des TLfDI rechtmäßig – Amtshilfeverweigerung durch das ehemals CDU-geführte Innenministerium rechtswidrig!

Nun liegt er vor: Der 739 Seiten umfassende **Zwischenbericht des Untersuchungsausschusses** (UA) 6/2 zur Causa Immelborn (Drucksache 6/4641 v. 23. Oktober 2017), der das **rechtmäßige Amtshilfeersuchen** des TLfDI und dessen **rechtmäßiges Vorgehen** in der Aktenlager-Angelegenheit feststellt sowie die **skurrilen Vorgänge im Thüringer Innenministerium** offenlegt inklusive der **rechtswidrigen Ablehnung des Amtshilfeersuchens**.

Die Plenardebatte offenbarte zudem, dass die CDU im Untersuchungsausschuss ein externes Rechtsgutachten zu sämtlichen Rechtsfragen einholen wollte. Diese Idee scheiterte indes wiederum an der **Justiz**, die es für **offensichtlich abwegig** hielt, die **Aufgabe des Untersuchungsausschusses**, nämlich zu ermitteln und zu bewerten, auf einen externen Gutachter zu verlagern.

Der Untersuchungsausschuss gelangt überdies zu dem Ergebnis: Der von der CDU-Fraktion geäußerte Verdacht, der TLfDI habe die Klage auf Amtshilfe erhoben, um im Wahlkampf der TIM-Hausleitung schaden zu wollen, hat sich nicht erhärtet (Zwischenbericht, Rn. 1041).

Wer Interesse daran hat, nachzulesen, auf welchen krummen Wegen die CDU-Hausleitung des Innenministeriums gezielt, unter Verkennung vorliegender Rechtsgutachten und in rechtswidriger Weise darauf hingewirkt hat, dem TLfDI die Amtshilfe zu versagen, der sei auf die Rn. 1031 ff. des Zwischenberichts verwiesen.

Das Sondervotum der CDU-Fraktion finden Sie auf den Seiten 727 ff.

Der TLfDI dankt der Thüringer Polizei für ihre korrekte Bereitschaft zur rechtmäßigen Amtshilfe bei dem Mammut-Projekt Aktenlager-Immelborn.

8.2 Wer hört wann, wo und auf welcher Rechtsgrundlage mit? – Aufzeichnung von Telefonaten auf den Dienstapparaten der Thüringer Polizei

In der Sommerpause des Thüringer Landtags läuft auch der Dienstbetrieb in den Ministerien gemächlicher als sonst – eben weil viele Mitarbeiterinnen und Mitarbeiter im Urlaub sind. Demzufolge ist auch in der Thüringer Presse in den Monaten Juli und August oft vom „Sommerloch“ die Rede. Im August 2016 war das „Sommerloch“ jedoch schlagartig passé, als nämlich folgender Vorwurf im Raum und in den Zeitungen stand: Auf bestimmten Dienstapparaten der Thüringer Polizei sollten über Jahre nicht nur eingehende Notrufe, sondern darüber hinaus alle eingehenden und ausgehenden Anrufe aufgezeichnet worden sein. Diesem ungeheuerlichen Verdacht, den ein Beschwerdeführer auch gegenüber dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) geäußert hatte, gingen der TLfDI und seine Mitarbeiterinnen und Mitarbeiter natürlich postwendend nach. Zuallererst war aber natürlich der Rechtsrahmen vom TLfDI „abzuklopfen“, innerhalb dessen Telefonaufzeichnungen in der Thüringer Polizei erfolgen dürfen:

- Nach § 2 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) gelten dessen Bestimmungen für die Verarbeitung und Nutzung von personenbezogenen Daten durch die Behörden des Landes. Soweit besondere Rechtsvorschriften des Bundes oder des Landes auf personenbezogene Daten anzuwenden sind, gehen sie den Bestimmungen des ThürDSG vor, § 2 Abs. 3 ThürDSG. Im hier zu untersuchenden Fall waren sowohl die spezielleren datenschutzrechtlichen Polizeivorschriften und ergänzend dazu die Regelungen des ThürDSG heranzuziehen.
- Nach § 31 Abs. 1 Satz 1 des Thüringer Gesetzes über die Aufgaben und Befugnisse der Polizei (Polizeiaufgabengesetz – PAG) kann die Polizei personenbezogene Daten nur erheben, soweit dies durch dieses Gesetz oder besondere Rechtsvorschriften über die Datenerhebung der Polizei zugelassen ist.
- § 32 Abs. 1 PAG regelt die Voraussetzungen, unter denen die Polizei Daten erheben kann. Nach dieser Vorschrift ist eine Datenerhebung unter anderem dann zulässig, wenn dies zur Gefahrenabwehr, insbesondere zur vorbeugenden Bekämpfung von Straftaten, ferner zum Schutz privater Rechte, zur Vollzugshilfe oder zur Erfüllung anderer Aufgaben der Polizei, die dieser durch andere Rechtsvorschriften übertragen worden sind.
- Gemäß § 40 Abs. 1 PAG kann die Polizei rechtmäßig erlangte personenbezogene Daten in Akten oder Dateien speichern, verändern und nutzen, soweit dies zur Erfüllung ihrer Aufgaben, zu einer zeitlich befristeten Dokumentation oder zur Vorgangsverwaltung erforderlich ist. Die Dauer der Speicherung ist auf das erforderliche Maß zu beschränken. Für automatisierte Daten sind Termine festzulegen, zu denen spätestens überprüft werden muss, ob die suchfähige Speicherung von Daten weiterhin erforderlich ist (Prüfungstermine), § 38 Abs. 1 Satz 1 und 2 PAG.
- Neben der Daten verarbeitenden Stelle haben nach § 34 ThürDSG die Landesministerien für ihren Bereich die Ausführungen dieses Gesetzes sowie anderer Rechtsvorschriften über den Datenschutz sicherzustellen. Das Gesetz begnügt sich damit nicht nur mit der an den jeweiligen Adressaten gerichteten, den einzelnen materiellen Regelungen immanenten Durchführungspflichten, sondern verpflichtet außerdem die obersten Behörden, in ihrem Bereich für die Verwirklichung des Datenschutzes zu sorgen (Simitis, BDSG, 8. Aufl. Nr. 2 zu § 18, der § 34 für den Bereich des Bundes entspricht). Der Inhalt dieser Durchfüh-

rungspflicht besteht darin, die Ausführungen des ThürDSG und anderer Rechtsvorschriften, wie des PAG, über den Datenschutz sicherzustellen. Verwaltungsvorschriften sind dabei Mittel zur Durchführung des Datenschutzes.

Ausgehend von diesem rechtlichen Grundgerüst stellte der TLfDI bei seinen Kontrollen und Vor-Ort-Terminen in der Polizeiinspektion Greiz, der Landespolizeiinspektion Suhl, der Landespolizeidirektion, dem Thüringer Landeskriminalamt und dem Thüringer Ministerium für Inneres und Kommunales unter anderem Folgendes fest:

1. Am 1. September 1999 trat die mit der damaligen Landesbeauftragten für den Datenschutz (TLfD) abgestimmte Dienstanweisung „Aufzeichnung von Telefongesprächsinhalten in der Thüringer Polizei des Thüringer Innenministeriums, Abteilung 4“, (DA AvTgi-ThPol) in Kraft. Die DA regelte die automatische Aufzeichnung des polizeilichen Notrufs. Darüber hinaus regelte die DA die manuell ausgelöste Bedarfsaufzeichnung in bestimmten Fällen. Sie definierte die zur Aufzeichnung von Gesprächsinhalten genutzten Kommunikationsmittel und legte die hierzu autorisierten Funktionsbereiche fest.

In Nummer 3 der DA wurde klargestellt, dass die fallweise oder regelmäßige Aufzeichnung des Inhalts von Telefongesprächen nur zulässig ist, soweit eine Befugnisnorm oder überwiegende Interessen der Gefahrenabwehr oder der Strafverfolgung dies erlauben oder der Betroffene eingewilligt hat. Als Rechtfertigungsgründe für die Aufzeichnung wurden unter Nummer 3.3 der DA die ausdrückliche, mutmaßliche oder stillschweigende Einwilligung, die Nothilfe und der rechtfertigende Notstand genannt.

Recherchen des TLfDI ergaben jedoch, dass diese Vorgaben aus der DA AvTgi-ThPol sowohl in der Thüringer Polizei als auch im Thüringer Innenministerium bzw. Thüringer Ministerium für Inneres und Kommunales (TMIK) nicht eingehalten worden waren. Aus den dem TLfDI vorgelegten Unterlagen des TMIK ergab sich, dass eine dreistellige Zahl an Telefonanschlüssen Telefonate „permanent oder bei Bedarf“ im Zeitraum von 2011 bis Mitte 2016 aufgezeichnet hatte. Damit wurden nicht nur die Inhalte der ankommenden Notrufe, die über die 110-Leitungen zunächst bei den Polizeidienststellen und seit 2012 bei der Landeseinsatzzentrale der Polizei (LEZ) eingingen, gespeichert, sondern weit mehr und andere Telefongespräche, die keine Notrufe beinhalteten.

Dieser Sachverhalt stand in Widerspruch zu den Darstellungen des Thüringer Innenministeriums gegenüber dem TLfDI aus dem

Jahr 2013. Damals hatte der TLfDI im Rahmen seiner Untersuchung der sogenannten Babyphonefunktion (Raumüberwachung bei Nichtnutzung des Telefons) von Telefonapparaten und der Möglichkeit von Telefonaufzeichnungen in der Landesverwaltung (siehe dazu den Beitrag Nr. 15.1 des 10. Tätigkeitsberichts des TLfDI, Seite 242 ff.) auch beim Thüringer Innenministerium unter anderem nachgefragt, wie viele Telefonapparate es dort gebe, die sowohl Telefongesprächsinhalte als auch Gespräche bei der Raumüberwachung aufzeichnen. Das Thüringer Innenministerium antwortete im Frühjahr 2013 dem TLfDI Folgendes: „Die Aufzeichnung von Gesprächsinhalten erfolgt nur in Fällen des Notrufs und der Gefahrenabwehr bzw. der Strafverfolgung auf der Grundlage des PAG [des Polizeiaufgabengesetzes] bzw. der StPO [der Strafprozessordnung]. In diesen Gesetzen sind die Kriterien abschließend geklärt. Bezüglich der Fragen zu Kriterien und Unterlagen wird auf die DA AvTgiTHPol […] verwiesen.“ Diese Auskünfte des Thüringer Innenministeriums wertete der TLfDI als wahrheitswidrige Behauptungen, die einen Verstoß gegen die Unterstützungspflicht aus § 38 Abs. 1 Satz 1 Nr. 1 ThürDSG darstellten. Der TLfDI beanstandete daher die fehlerhaften Auskünfte des Thüringer Innenministeriums aus dem Jahr 2013 Ende August 2016.

Der TLfDI stellte im Rahmen seiner Recherchen ferner fest, dass spätestens seit Errichtung der Landespolizeidirektion und deren LEZ im Jahr 2012 Daten in Form der Aufzeichnungen der Telefonate erhoben wurden, obwohl die Voraussetzungen des § 32 Abs. 1 PAG nicht vorlagen. Denn zur Gefahrenabwehr erforderlich im Sinne von § 32 Abs. 1 PAG war aus der Sicht des TLfDI lediglich die Aufzeichnung von Notrufen. Diese konnten einerseits auf der allgemeinen Einwahlnummer 110 eingehen. In diesem Fall wurde der Anruf in der LEZ automatisch gespeichert. Wurde der Anruf aber andererseits nicht über eine „Notrufnummer“ getätigt, so war die Aufzeichnung im Einzelfall, wenn es sich tatsächlich um einen Notruf handelte, zwar zulässig. Diese Möglichkeit eines potenziellen Notrufs rechtfertigte aber nicht, alle eingehenden und auch ausgehenden Gespräche aufzuzeichnen. Die permanente Aufzeichnung auch von Nicht-Notrufen auf der dreistelligen Zahl der übermittelten Telefon-Nebenstellen, die keine reinen Notrufnummern waren, war damit unzulässig.

Zulässig wäre allenfalls eine sogenannte Aufschaltung im Fall eines tatsächlich eingehenden Notrufs gewesen oder in dem Fall, dass der

Anrufende mit dem Anruf eine Straftat begeht, beispielsweise, weil er den diensthabenden Beamten am Telefon oder auch andere Personen bedrohte. Für die Speicherung aller anderen aufgezeichneten Telefonate, die über Telefone geführt wurden, die keine Notfalltelefone waren, gab es hingegen keine rechtliche Grundlage.
Da die festgestellten Datenerhebungen nach § 32 Abs. 1 PAG im vorliegenden Fall nicht gerechtfertigt waren, konnten sie gem. § 40 Abs. 1 Satz 1 PAG auch nicht gespeichert werden – weil diese Regelung als Tatbestandsmerkmal „rechtmäßig erlangte personenbezogene Daten“ voraussetzt. Folglich waren sowohl die Datenerhebungen als auch die Datenspeicherungen vom TLfDI gem. § 39 Abs. 1 ThürDSG zu beanstanden.
2. Ferner zu beanstanden hatte der TLfDI, dass es im früheren Thüringer Innenministerium unterlassen worden war, die mit der Einrichtung der LEZ und der damit verbundenen Umstrukturierung des Notfallsystems erforderliche Überarbeitung der DA AvTgi-ThPol zu veranlassen. Das Thüringer Innenministerium hätte als die für die Sicherstellung des Datenschutzes nach § 34 Abs. 1 ThürDSG zuständige Stelle die gewonnenen Erfahrungen bei der Durchsetzung der DA überprüfen müssen. Spätestens zum Zeitpunkt der Einrichtung der LEZ im Jahr 2012 hätte daher geprüft werden müssen, ob in den übrigen nachgeordneten Stellen nach der DA verfahren wird. Zu diesem Zeitpunkt hätte es dort nur noch Bedarfsaufschaltungen geben dürfen. Dies hätte dem nachgeordneten Bereich mitgeteilt werden müssen. Auf die Überarbeitungsbedürftigkeit der DA AvTgi-ThPol hatte die Landespolizeidirektion das frühere Thüringer Innenministerium bzw. das Thüringer Ministerium für Inneres und Kommunales mehrfach hingewiesen.
Eine Überarbeitung der DA AvTgi-ThPol erfolgte aber erst unter Beteiligung des TLfDI im Frühjahr 2017. Die neue Dienstanweisung über die Aufzeichnung von Sprachkommunikation in der Thüringer Polizei (DA AvSK-ThPol) ist zum 1. Mai 2017 in Kraft getreten (siehe dazu Thüringer Staatsanzeiger, Nr. 24/2017, Seite 783 bis 794). Unter anderem wurden die Vorgaben in Nr. 3.3 der DA AvSK-ThPol für die permanente automatische Aufzeichnung sprachlich präziser gefasst, und es wurde ausdrücklich geregelt, dass automatische Aufzeichnungen nur noch bei Notrufen, dem polizeilichen Funkverkehr und bei manuellem Bedarf im Einzelfall zulässig sind.

Die Aufzeichnungen von ein- und ausgehenden Telefonaten, die keine Notrufe darstellten, in Thüringer Polizeidienststellen über viele Jahre haben bei einigen Thüringer Bürgerinnen und Bürgern traurige Erinnerungen an die Zeit vor 1989 geweckt. Umso wichtiger war und ist es daher, dass in einem demokratischen Rechtsstaat eine unabhängige Datenschutzbehörde über die Beachtung und Einhaltung des Grundrechts auf informationelle Selbstbestimmung aus Art. 1 Abs. 1 in Verbindung mit Art. 2. Abs. 1 GG wacht und bei Verstößen auch den staatlichen Einrichtungen, wie z. B. der Polizei, „auf die Füße tritt". Der TLfDI nimmt hier „kein Blatt vor den Mund" und fordert die Behörden und Ministerien zur Umsetzung der datenschutzrechtlichen Regelungen im PAG und im ThürDSG auf.

8.3 Wer kopiert oder importiert Daten bei PCs der Polizei? – DeviceWatch weiß alles

Stellen Sie sich vor, Sie müssen Ihren Rechner schützen, weil Ihr Kind Ihnen beim letzten „Herunterladen" von Spielen oder Musikvideos aus dem Netz wieder einmal einen gemeinen Computervirus mit auf die Festplatte „gebracht" hat. Das finden Sie natürlich gar nicht toll, weil Sie zum einen nicht sicher sein können, ob sich hinter dem Virus ein fieser Trojaner verbirgt, also eine Art Spähsoftware, die ihre personenbezogenen Daten an fremde Personen oder Firmen übermittelt. Zum anderen kostet es Sie Zeit und Geld, diesen Virus wieder von der Festplatte Ihres Computers zu entfernen.
Mit ähnlichen Problemen, wie gerade dargestellt, sah sich auch die Thüringer Polizei bereits vor fast zehn Jahren konfrontiert. Rückblende: Im Sommer 2008 entschloss sich das damalige Thüringer Innenministerium (TIM) zur Anschaffung der Software DeviceWatch, unter anderem in der Polizei. Die Software konnte nach den Herstellerangaben eine Vielzahl von Funktionen abdecken. Faktisch genutzt wurde jedoch nur folgende Funktion:
Die Software war und ist in der Lage, das Laden und Speichern von Dateien durch **Anwendungen** zu prüfen und, soweit entsprechend konfiguriert, auch die Inhaltsdaten zu prüfen und das Laden und Speichern aktiv zu verhindern.
Sprung zurück in das Jahr 2016: Auf den datenschutzrechtlich fragwürdigen Einsatz von DeviceWatch in der Thüringer Polizei aufmerksam gemacht wurde der Thüringer Landesbeauftragte für den

Datenschutz und die Informationsfreiheit (TLfDI) im Sommer des Jahres.
Der TLfDI reagierte sofort und forderte alle erforderlichen Unterlagen zum Einsatz der DeviceWatch beim Thüringer Landeskriminalamt (TLKA) an, das den Einsatz der Software in der Thüringer Polizei federführend betreut. Ferner überprüfte der TLfDI am 26. August, 12. September und 7. Oktober 2016 beim TLKA die zentrale Konfiguration von DeviceWatch, die mittlerweile unter dem Namen „itWatch Endpoint Security Suite“ erhältlich ist.
Der TLfDI stellte die folgenden rechtlichen Verstöße beim Einsatz von DeviceWatch fest, die er gegenüber dem TLKA beanstandete:

- **Fehlen eines Verfahrensverzeichnisblatts gem. § 10 Abs. 1 und 2 Thüringer Datenschutzgesetz (ThürDSG)**

Der TLfDI beanstandete ein fehlendes Verfahrensverzeichnisblatt gem. § 10 Abs. 2 ThürDSG für die Software DeviceWatch bzw. deren Nachfolger „itWatch Endpoint Security Suite.

- **Fehlende Rechtsgrundlage für die Anfertigung von Kopien verwendeter Dateien, die DeviceWatch erkannte (Schattenkopien)**

Eine Rechtsgrundlage, die eine Anfertigung von Kopien jener Dateien mit personenbezogenen oder personenbeziehbaren Daten gestattete, die die Software DeviceWatch ausfindig gemacht hatte, war für den TLfDI nicht ersichtlich. § 32 Abs. 1 Polizeiaufgabengesetz schied hier ebenso wie § 20 Abs. 1 und 4 ThürDSG aus, weil nicht ersichtlich war, warum es erforderlich sein sollte, dass von einer Datei, die ein Bediensteter der Polizei von seinem Dienstcomputer auf einen externen Datenträger übertragen will oder umgekehrt, noch eine Kopie (sogenannte Schattenkopie) angefertigt wird.

- **Fehlende schriftliche Freigabeerklärung gem. § 34 Abs. 2 Satz 1 ThürDSG**

Weiterhin beanstandete der TLfDI die für den konkreten Einsatz von DeviceWatch fehlende schriftliche Freigabeerklärung gem. § 34 Abs. 2 Satz 1 ThürDSG. Diese hätte hier vorliegen müssen, weil mit DeviceWatch ein automatisiertes Verfahren in der Thüringer Polizei zum Einsatz kam, das personenbezogene Daten verarbeitete.

- **Fehlendes Sicherheitskonzept gem. § 9 Abs. 2 Satz 1 ThürDSG**

Nicht vorlegen konnte das TLKA dem TLfDI des Weiteren ein Sicherheitskonzept gem. § 9 Abs. 2 Satz 1 ThürDSG, auf dessen Grundlage die zu treffenden technischen und organisatorischen

Maßnahmen zu ermitteln sind, und die dann die in § 9 Abs. 2 Nr. 1 bis 6 genannten Gewährleistungen enthalten müssen.

- **Verstoß gegen § 9 Abs. 2 Nr. 5 und 6 ThürDSG mangels Anwendung des Vier-Augen-Prinzips bei der Protokollrecherche.**

Den Forderungen des TLfDI, ihm ein Verfahrensverzeichnisblatt sowie eine schriftliche Freigabeerklärung für den Einsatz von DeviceWatch vorzulegen, ist das TLKA mittlerweile gefolgt. Ebenso legte das LKA ein überarbeitetes Sicherheitskonzept für DeviceWatch bzw. deren Nachfolgesoftware „itWatch Endpoint Security Suite“ sowie eine überarbeitete Richtlinie zur Durchführung von Protokollrecherchen beim TLKA vor, die dem Vier-Augen-Prinzip genügte.

Darüber hinaus ging der TLfDI auch der Frage nach, ob die Einführung der Software DeviceWatch seinerzeit im Geschäftsbereich des früheren TIM mitbestimmungspflichtig nach dem Thüringer Personalvertretungsgesetz (ThürPersVG) gewesen ist. Die fehlende Mitbestimmung des Hauptpersonalrats bei der Einführung und Anwendung von DeviceWatch bzw. deren Nachfolger „itWatch Endpoint Security Suite“ stellte nach Auffassung des TLfDI einen Verstoß gegen § 74 Abs. 2 Nr. 11 ThürPersVG dar.

Das Thüringer Ministerium für Inneres und Kommunales (TMIK) erklärte im Sommer 2017 auf die Forderung des TLfDI, die Personalratsbeteiligung gem. § 74 Abs. 2 Nr. 11 ThürPersVG zum Einsatz von DeviceWatch unverzüglich nachzuholen, dass dies bereits kurz nach dem Bekanntwerden der Kritik an der eingesetzten Software im Oktober 2016 geschehen war.

Der „Fall DeviceWatch“ in der Thüringer Polizei macht zwei wichtige Erkenntnisse deutlich: Zum einen ist nicht jede sicherheitstechnisch erforderliche Neuerung auch datenschutzrechtlich zulässig. Dies gilt insbesondere für das Erstellen von sogenannten Schattendateien. Denn damit ist das Verhalten eines Mitarbeiters – vorsichtig formuliert – nachvollziehbar. Zum anderen belegt der „Fall DeviceWatch“ eindrucksvoll, dass sicherheitsrelevante Softwareanschaffungen auch datenschutzrechtlich „zu Ende gedacht“ werden müssen: Dies beginnt mit der Erstellung eines Verfahrensverzeichnisblattes, führt über eine schriftliche Freigabeerklärung für die Software gem. § 34 Abs. 2 Satz 1 ThürDSG bis hin zur Erstellung eines Sicherheitskonzeptes auf der Grundlage von § 9 Abs. 2 Satz 1

ThürDSG und endet mit der Überarbeitung einschlägiger Richtlinien, z. B. zur Durchführung von Protokollrecherchen. Last but not least hat die zuständige Stelle auch immer § 74 Abs. 2 Nr. 11 ThürPersVG „im Hinterkopf“ zu bedenken, der ein Mitbestimmungsrecht des Personalrates bei der Einführung, Anwendung, wesentlichen Änderung oder Erweiterung technischer Einrichtungen, die geeignet sind, das Verhalten oder die Leistung der Beschäftigten zu überwachen oder zu erfassen, vorsieht. Wenn’s zuviel wird: Der TLfDI berät lieber im Vorfeld – als hinterher zu beanstanden!

8.4 Gemeinsames Kompetenz- und Dienstleistungszentrum auf dem Gebiet der polizeilichen Telekommunikationsüberwachung

Auf dem Gebiet der polizeilichen Telekommunikationsüberwachung planen die Länder Berlin, Brandenburg, Sachsen-Anhalt, der Freistaat Sachsen und der Freistaat Thüringen ein Gemeinsames Kompetenz- und Dienstleistungszentrum (GKDZ) zu errichten.
Das GKDZ soll als Anstalt des öffentlichen Rechts auf der Grundlage eines Staatsvertrages errichtet werden.
Vor diesem Hintergrund wollen die Trägerländer die Zusammenarbeit auf dem Gebiet der polizeilichen Telekommunikationsüberwachung intensivieren.
In den Trägerländern verfügt bislang jeder Polizeibereich über eigene, auf die Bedürfnisse des jeweiligen Geschäftsbereichs zugeschnittene IT-Unterstützungsleistungen für die Telekommunikationsüberwachung. Diese dezentralen Unterstützungsprozesse sollen in einer separaten, länderübergreifenden Organisations- bzw. Wirtschaftseinheit mit entsprechender Rechtsform, einem kooperationsgebundenen Dienstleister auf dem Gebiet der polizeilichen Telekommunikationsüberwachung, weitestgehend gebündelt, konsolidiert, modernisiert und damit zukunftsfähig werden. Grundlegende polizeifachliche Entscheidungen zur Telekommunikationsüberwachung verbleiben in den Polizeibereichen der Trägerländer. Ziele sind die Steigerung der Effizienz und die Sicherstellung einer bedarfsgerechten sowie an der technischen und rechtlichen Entwicklung ausgerichteten Telekommunikationsüberwachungspraxis.
Das Thüringer Ministerium für Inneres und Kommunales (TMIK) legte Anfang Dezember 2015 dem TLfDI einen Entwurf des Staats-

vertrages vor, zu dem der TLfDI eine datenschutzrechtliche Stellungnahme abgab. Dieser wies unter anderem auf Folgendes hin:
„Zu beachten ist, dass die jeweiligen Polizeibehörden der einzelnen Länder grundsätzlich nur auf ihre eigenen Datensätze Zugriff haben dürfen. Ein Zugriff auf diese Daten durch Dritte ist grundsätzlich unzulässig und auszuschließen. Aufgrund des sensiblen Charakters der Daten ist auf eine strenge Zweckbindung der Daten zu achten.“ Diese Zweckbindung ergibt sich aus dem Polizeiaufgabengesetz und der Strafprozessordnung.
Weiterhin bat der TLfDI in seiner Stellungnahme, den Aufgabenumfang des GKDZ im Staatsvertrag konkret festzulegen. Schließlich ging der TLfDI in seiner Stellungnahme auch wie folgt auf die Frage einer Auftragsdatenverarbeitung ein:
„Im Rahmen des Auftragsdatenverarbeitungsverhältnisses (Thüringer Polizei – GKDZ) ist der Auftrag schriftlich zu erteilen, wobei die Datenverarbeitung oder -nutzung, die technisch-organisatorischen Maßnahmen und etwaige Unterauftragsverhältnisse festzulegen sind. Bei einer möglichen Anbieterauswahl durch das GKDZ wird – insbesondere im Lichte des Urteils des EuGH vom 6. Oktober 2015 C-262/14 (Safe Harbor) – heute durch das EU-US Privacy Shield-Abkommen ersetzt – seitens des TLfDI darauf hingewiesen, dass eine Datenübermittlung in die USA grundsätzlich bedenklich ist. In diesem Zusammenhang wird auf das etwaige Gefährdungspotential amerikanischer Software hingewiesen.
Zum Schutz der personenbezogenen Daten wird dringend empfohlen, festzulegen, dass die bei einer Telekommunikationsüberwachung erhobenen Daten dem jeweiligen Stand der Technik (§ 9 Thüringer Datenschutzgesetz) entsprechend bei der Datenübermittlung und Datenspeicherung zu verschlüsseln sind. Angeregt wird beispielsweise die Formulierung aus § 6a Passgesetz als Grundlage zu übernehmen und wie folgt anzupassen:
‚Die beteiligten Stellen haben dem jeweiligen Stand der Technik entsprechende Maßnahmen zur Sicherstellung von Datenschutz und Datensicherheit zu treffen, die insbesondere die Vertraulichkeit und Unversehrtheit der Daten sowie die Feststellbarkeit der übermittelnden Stelle gewährleisten; im Fall der Nutzung allgemein zugänglicher Netze und bei der Datenspeicherung im GKDZ sind dem jeweiligen Stand der Technik entsprechende Verschlüsselungsverfahren anzuwenden.‘“

Im Juli 2017 unterzeichneten der Innensenator von Berlin sowie die Innenminister von Brandenburg, Sachsen und Sachsen-Anhalt den „Staatsvertrag über die Errichtung eines Gemeinsamen Kompetenz- und Dienstleistungszentrums (GKDZ) der Polizeien der Länder Berlin, Brandenburg, Sachsen, Sachsen-Anhalt und Thüringen auf dem Gebiet der polizeilichen Telekommunikationsüberwachung als rechtsfähige Anstalt des öffentlichen Rechts“. Am 8. September 2017 unterzeichnete der Thüringer Innenminister den Staatsvertrag. Der Staatsvertrag erfordert zu seiner Anwendung eine „Benutzerordnung“ (§ 6 Abs. 3 Nr. 3 des Staatsvertrages). Diese wurde dem TLfDI aber bisher nicht vorgelegt.
Mit Pressemitteilung vom 19. September 2017 hat das TMIK mitgeteilt, dass das Thüringer Kabinett am selben Tage den Entwurf des „Zustimmungsgesetzes zum Staatsvertrag über die Errichtung eines Gemeinsamen Kompetenz- und Dienstleistungszentrums (GKDZ) der Länder Berlin, Brandenburg, Sachsen, Sachsen-Anhalt und Thüringen auf dem Gebiet der polizeilichen Telekommunikationsüberwachung“ beschlossen und dem Thüringer Landtag zugeleitet hat.

Die Vorteile einer polizeilichen, länderübergreifenden Zusammenarbeit auf dem Gebiet des Informationsaustausches bedürfen besonderer Vorkehrungen auf dem Gebiet des Datenschutzes. Daher bedarf es für die Errichtung eines GKDZ nicht nur eines Staatsvertrages, sondern auch eines datenschutzrechtlichen Feinkonzeptes.

8.5 "Bodycams" in der Thüringer Polizei

Im Berichtszeitraum testeten mehrere Bundesländer in Pilotprojekten den Einsatz von „Bodycams“ bei der Polizei. Vorreiter in dieser Hinsicht ist das Land Hessen. Die „Bodycams“ sollen dem Eigenschutz von Polizeibeamten dienen. Durch das Bewusstsein, dass eine Aufzeichnung erfolgt, soll eine Deeskalation erreicht und ein Angriff auf Polizeibeamte vermieden werden. Hessen gibt an, hiermit gute Erfahrungen gemacht zu haben.
Nachdem ursprünglich das Innenministerium auf Anfrage dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) mitgeteilt hatte, dass derzeit weder „Bodycams“ im Einsatz noch zukünftig geplant seien, hat sich nunmehr der Standpunkt geändert. Ab dem 1. April 2017 befinden sich „Bo-

dycams“ in einer sechsmonatigen Erprobungsphase bei drei Polizeidirektionen.
Parallel dazu diskutierten die Datenschutzbeauftragten des Bundes und der Länder den Einsatz von „Bodycams“. Im Ergebnis sind die Datenschützer grundsätzlich der Auffassung, dass für den Einsatz von „Bodycams“ eine Rechtsgrundlage erforderlich sei. In dieser sollten die Voraussetzungen für den Einsatz und auch für die weitere Verarbeitung (z. B. die Auswertung und Löschung der Daten) geregelt werden.
Der TLfDI hat Verständnis für die Argumente aus den Reihen der Polizeigewerkschaften, dass „Bodycams“ auch bei der Thüringer Polizei zum Einsatz kommen sollen. Als Rechtsgrundlage für den Einsatz solcher „Bodycams“ zum Schutz der Polizeibeamten bei Personen- oder Fahrzeugkontrollen an öffentlich zugänglichen Orten kommt § 33 Abs. 6 Satz 1 Polizeiaufgabengesetz (PAG) infrage.
Vor Start des Pilotprojektes wurde der TLfDI durch das TMIK ins Benehmen gesetzt.
Ende Februar 2017 wurde dem TLfDI vom Thüringer Ministerium für Inneres und Kommunales (TMIK) eine Studie „Teilprojekt Recht“ übersandt. In dieser wurden die Rechtsgrundlagen für den Einsatz von „Bodycams“ untersucht. Im Ergebnis hielt die Studie fest, dass das Projekt ausschließlich auf § 33 Abs. 6 PAG gestützt werden sollte. Der TLfDI stimmte der Studie insofern zu, dass § 33 Abs. 6 PAG als einzige Rechtsgrundlage infrage kommt.
Die Endfassung der Konzeption wurde als Grundlage der Pilotstudie vom TLfDI als geeignet erachtet.
Nach Beendigung des Pilotprojektes sollte allerdings § 33 Abs. 6 PAG überarbeitet werden. Die bisherige Fassung dieser Norm besitzt gerade hinsichtlich des Kriteriums der Bestimmtheit und der Verhältnismäßigkeit ihre Schwächen.
Hinsichtlich der Bestimmtheit ist festzustellen, dass § 33 Abs. 6 PAG ursprünglich für eine andere Situation in das Gesetz aufgenommen wurde: Angesichts von Angriffen auf Polizeibeamte sollte § 33 Abs. 6 PAG es ermöglichen, dass Fahrzeugkontrollen der Polizei durch eine Kamera im Streifenwagen gefilmt werden können. An „Bodycams“ wurde bei Änderung des PAG damals jedoch nicht gedacht. Dementsprechend spricht § 33 Abs. 6 PAG von Personen- und Fahrzeugkontrollen und dem Einsatz technischer Mittel. Die Formulierung in § 33 Abs. 6 PAG müsste daher, sofern der Einsatz

von „Bodycams“ künftig dauerhaft erfolgen sollen, an die tatsächlichen Gegebenheiten angepasst werden.
Hinsichtlich der Verhältnismäßigkeit war vom TLfDI festzustellen, dass § 33 Abs. 6 PAG lediglich vom „Schutz der Polizeibeamten“ spricht. Konkrete Rechtsgüter, die betroffen sein müssen, werden nicht benannt. In der „Konzeption für den Testbetrieb der Bodycam in der Thüringer Polizei“ hatte die Landespolizeiinspektion Gotha indes festgelegt, dass eine Gefährdung von Leib oder Leben gegeben sein muss, um die „Bodycams“ zum Einsatz zu bringen. Dies sollte künftig nach Auffassung des TLfDI gesetzlich so geregelt sein.
In der Literatur wird eine Formulierung für eine solche gesetzliche Regelung zur Ermächtigung des Einsatzes von „Bodycams“ vorgeschlagen, die diesen Forderungen Rechnung trägt (Videoüberwachung zur Risikovorsorge – Bodycam zur Eigensicherung und Dashcam zur Beweissicherung – Eine verfassungs- und datenschutzrechtliche Analyse, Tobias Starnecker, Berlin, 2017, Seite 252). Dieser Vorschlag hat folgenden Wortlaut:
„Die Polizei kann bei der Durchführung von Maßnahmen aufgrund von Befugnissen zur Gefahrenabwehr oder zur Verfolgung von Straftaten und Ordnungswidrigkeiten an öffentlich zugänglichen Orten mittels am Körper getragener optisch-elektronischer Einrichtungen zur Anfertigung von Bild- und Tonaufzeichnungen (Bodycam) personenbezogene Daten aufzeichnen, wenn dies nach den Umständen zum Schutz gegen eine Gefahr für Leib oder Leben der Polizeibeamten erforderlich ist. Die Videoüberwachung erfolgt offen und muss erkennbar sein. Ein ausdrücklicher Hinweis auf die Videoüberwachung soll erfolgen. Von der Videoüberwachung nach Satz 1 dürfen auch Dritte betroffen werden, soweit dies nicht vermeidbar ist. Aufzeichnungen sind unzulässig in Bereichen, die der Ausübung von Tätigkeiten von Berufsgeheimnisträgern nach § 53 Abs. 1 der Strafprozessordnung dienen.“

Der Einsatz von „Bodycams“ sollte gesetzlich neu im PAG geregelt werden, da der bisherige § 33 Abs. 6 PAG hinsichtlich der Bestimmtheit der Norm und der Verhältnismäßigkeit einer Neuformulierung bedarf.

8.6 Erste gemeinsame Kontrolle der bundesweiten Rauschgiftdatei durch die Datenschutzbeauftragten von Bund und Ländern

Gegenstand einer datenschutzrechtlichen Kontrolle beim Thüringer Landeskriminalamt (TLKA) durch den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) war die Speicherung personenbezogener Daten in der Verbunddatei „Falldatei Rauschgift“ (FDR). Die FDR ist Teil der beim Bundeskriminalamt geführten bundesweiten INPOL-Datenbank und enthielt 2015 Informationen zu sehr vielen Drogendelikten. In ihr speichern das Bundeskriminalamt, das Zollkriminalamt und die Polizeibehörden der Länder.
Registrieren die Behörden einen Verstoß gegen das Betäubungsmittelgesetz, können sie Beschuldigte in der „Falldatei Rauschgift“ speichern, um weitere Straftaten zu verhindern und zukünftige Ermittlungen zu erleichtern. Rechtsgrundlage für die Führung der Datei ist § 8 Abs. 1 und 2 Bundeskriminalamtgesetz (BKAG). Für Speicherungen nach § 8 BKAG sind die Grenzen des § 2 Abs. 1 BKAG einzuhalten. Gespeichert werden dürfen demnach nur Straftaten mit länderübergreifender oder erheblicher Bedeutung. Jede Speicherung muss nach dem Gesetz einzeln geprüft und in einer sogenannten Negativprognose begründet werden. Die datenschutzrechtliche Verantwortung für die Zulässigkeit der Eingabe der Daten obliegt den eingebenden Stellen (§ 12 Abs. 2 BKAG), im Fall Thüringens also dem TLKA.
In der Praxis wurden die Vorgaben des BKAG aber nicht immer umgesetzt. Dies zeigte nicht nur die Kontrolle durch den TLfDI auf, sondern auch die diversen Kontrollen der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit und der Landesdatenschutzbeauftragten aus Baden-Württemberg, Bayern, Berlin, Brandenburg, Bremen, Hessen, Niedersachsen, Nordrhein-Westfalen, Rheinland-Pfalz, Sachsen-Anhalt und Schleswig-Holstein.
Im Rahmen der Kontrollen ist u. a. aufgefallen, dass in der Datei durchaus zahlreiche Einzelspeicherungen vorhanden sind, die eher den Bereich der Bagatellkriminalität betreffen. Dies betrifft beispielsweise Fälle, in denen Betroffene wegen des geringfügigen Konsums von Betäubungsmitteln (BtM) oder wegen des geringfügigen Besitzes von BtM erfasst wurden.

In einer gemeinsamen Entschließung forderte die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK), die beanstandeten Mängel zu beheben (https://www.tlfdi.de/mam/tlfdi/datenschutz/entschliessungen/entsch-falldatei-rauschgift.pdf).

Eine Reaktion seitens des TLKA zum Kontrollbericht liegt dem TLfDI bislang noch nicht vor. Eine weitere Befassung mit diesem Thema erfolgt im nächsten Tätigkeitsbericht.

Rechtsgrundlage für die Führung der „Falldatei Rauschgift“ (FDR) ist § 8 Abs. 1 und 2 BKAG. Für Speicherungen nach § 8 BKAG sind die Grenzen des § 2 Abs. 1 BKAG einzuhalten. Demnach muss es sich um die Verhütung und Verfolgung von Straftaten mit länderübergreifender, internationaler oder erheblicher Bedeutung handeln. Die datenschutzrechtliche Verantwortung für die Zulässigkeit der Eingabe der Daten obliegt den eingebenden Stellen (§ 12 Abs. 2 BKAG).

8.7 Kopie des Personalausweises zulässig?

Ein Bürger wandte sich im Berichtszeitraum an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), weil er sich in seinem Recht auf informationelle Selbstbestimmung beeinträchtigt sah. Der Beschwerdeführer gab gegenüber dem TLfDI an, dass er als Beschuldigter von der Landespolizeiinspektion Suhl geladen worden war. Im Rahmen dieses Termins habe die Polizei eine Kopie des Personalausweises angefertigt, welche als Ausdruck in die Akte genommen wurde.

Die Landespolizeiinspektion Suhl bestätigte den Vorfall und teilte mit, dass die Personalausweiskopie vernichtet worden sei und sich nicht in der Akte befände.

Die Anfertigung von Personalausweiskopien ist aus datenschutzrechtlicher Sicht gemäß § 4 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) nur zulässig, wenn das ThürDSG oder eine andere Rechtsvorschrift dies erlaubt oder der Betroffene eingewilligt hat. Im Falle der Einwilligung ist die Verarbeitung oder Nutzung personen-

bezogener Daten nur zulässig, wenn dies zur Erfüllung anerkannter Zwecke erforderlich ist, § 4 Abs. 1 Satz 2 ThürDSG. Nach der spezialgesetzlichen Regelung des § 20 Abs. 2 Personalausweisgesetz (PAuswG) darf der Ausweis nur vom Ausweisinhaber oder von anderen Personen mit Zustimmung des Ausweisinhabers in der Weise abgelichtet werden, dass die Ablichtung eindeutig und dauerhaft als Kopie erkennbar ist. Andere Personen als der Ausweisinhaber dürfen die Kopie nicht an Dritte weitergeben. Werden durch die Ablichtung personenbezogene Daten aus dem Personalausweis erhoben oder verarbeitet, so darf die datenerhebende oder -verarbeitende Stelle dies nur mit Einwilligung des Ausweisinhabers tun.
Eine Einwilligung durch die betroffene Person ist im vorliegenden Falle nicht erfolgt. Da auch keine andere gesetzliche Regelung einschlägig war, war das Ablichten des Personalausweises im vorliegenden Falle rechtswidrig.
In dem von dem Beschwerdeführer geschilderten Fall hatte zudem der in § 20 Abs. 1 ThürDSG geregelte Erforderlichkeitsgrundsatz keine Beachtung gefunden. Die Erstellung der Kopie müsste demnach für die Polizeidienststelle erforderlich gewesen sein, d. h. es dürfte zur Erreichung des Zwecks kein gleich geeignetes, milderes Mittel vorhanden gewesen sein. Als milderes Mittel und auch als zumindest genauso effektiv anzusehen wäre es gewesen, die erforderlichen personenbezogenen Daten einfach zu notieren. Außerdem hätte im vorliegenden Falle geprüft werden müssen, ob nicht die Vorlage des Personalausweises und ggf. die Anfertigung eines entsprechenden Vermerks (z. B. „Personalausweis hat vorgelegen“) ausreichend gewesen wäre. So erspart man sich auch die Mühe, überflüssige Daten zu schwärzen und hinterher die Kopie des Personalausweises ordnungsgemäß zu vernichten.
Der TLfDI nahm den Vorfall zum Anlass, sowohl die betroffene Landespolizeiinspektion als auch das Thüringer Ministerium für Inneres und Kommunales (TMIK) über seine Rechtsauffassung zur Anfertigung von Personalausweiskopien zu informieren, um so künftig ein Kopieren des Personalausweises – auch in anderen Fällen – zu verhindern bzw. auf die absolut erforderlichen Fälle zu minimieren.
Sowohl die Landespolizeiinspektion Suhl als auch das TMIK haben die Rechtsauffassung des TLfDI in dem dargestellten Fall geteilt. Die Landespolizeiinspektion Suhl hat daraufhin ihre Mitarbeiter mit der Problematik vertraut gemacht und darauf hingewiesen, dass zum

Zwecke der Erhebung der Personalien und zur Verbesserung der Datenqualität künftig keine Kopien von amtlichen Personalausweisen oder anderen Dokumenten zu fertigen sind.

Gem. § 20 Abs. 2 PAuswG darf der Personalausweis nur vom Ausweisinhaber oder von anderen Personen mit Zustimmung des Ausweisinhabers in der Weise abgelichtet werden, dass die Ablichtung eindeutig und dauerhaft als Kopie erkennbar ist. Andere Personen als der Ausweisinhaber dürfen die Kopie nicht an Dritte weitergeben. Ferner ist bei der Anfertigung von Ausweiskopien mit Zustimmung des Inhabers auch stets zu fragen, ob das Anfertigen einer solchen Kopie erforderlich ist (§ 4 Abs. 1 Satz 2 ThürDSG). Zu fragen ist dabei, ob nicht ein milderes, aber ebenso zweckmäßiges Mittel wie z. B. das Verfassen eines Vermerks („Personalausweis hat vorgelegen“) ausreichend ist.

8.8 Keine beglaubigte Kopie des Personalausweises für Auskunftsersuchen beim TLKA

Ein Beschwerdeführer wandte sich im Berichtszeitraum an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), da er mit einer Identitätsüberprüfung zur Weiterbearbeitung eines schriftlichen Auskunftsersuchens beim Landeskriminalamt Thüringen (TLKA) nicht einverstanden war.
Nach Eingang des Auskunftsersuchens des Beschwerdeführers beim Thüringer Landeskriminalamt, wurde er darüber informiert, dass sein Ersuchen erst bearbeitet wird, wenn eine amtlich beglaubigte oder polizeilich bestätigte Kopie eines amtlichen Lichtbildausweises (z. B. Personalausweis, Reisepass) zum Zwecke der Identitätsüberprüfung eingegangen ist.
Der TLfDI wandte sich sogleich an das Landeskriminalamt Thüringen und bat um Aufklärung des Sachverhalts. Nach Ansicht des TLfDI werden bei schriftlichen Auskunftsersuchen bei der Polizei dem Bürger mit der Forderung nach einer beglaubigten Ausweiskopie zu hohe Hürden auferlegt.
Eine beglaubigte Kopie bzgl. des Identitätsnachweises besitzt gegenüber einer einfachen Kopie keinen Mehrwert, da sie letztlich nur bestätigt, dass die Kopie mit dem Original übereinstimmt. Eine beglaubigte Personalausweiskopie an sich stellt nicht uneingeschränkt

sicher, dass tatsächlich keine unberechtigte Person Kenntnis vom Inhalt des Auskunftsersuchens erlangt.
Die Vorlage einer einfachen Kopie muss durch den Antragsteller jedoch akzeptiert werden. Bei Datenübermittlungen trägt gem. § 22 Abs. 2 Thüringer Datenschutzgesetz (ThürDSG) die übermittelnde Stelle die Verantwortung für die Zulässigkeit der Übermittlung. Bei fernmündlichen Auskunftsersuchen besteht keine Möglichkeit zur persönlichen Legitimation des Antragstellers gegenüber der angefragten öffentlichen Stelle.
Es ist aber in jedem Falle sicherzustellen, dass entsprechende Auskünfte über personenbezogene Daten an den tatsächlich Betroffenen erteilt werden. Dessen Identität ist somit in geeigneter Weise festzustellen. Diesbezüglich ist die Vorlage einer Kopie des Bundespersonalausweises das geeignetste und zugleich mildeste Mittel für den Betroffenen, um seinen Anspruch auf Auskunftserteilung zu erwirken.
Eine beglaubigte Kopie kann von der Polizei in Ausnahmefällen gefordert werden, z. B. wenn ein Manipulationsverdacht an der Kopie besteht.
Unberührt hiervon bleibt die persönliche Identifizierung des Antragsstellers auf einer Polizeidienststelle, hier reicht ein Vermerk, dass die Identität des Antragstellers geprüft wurde.
Bei einem schriftlichen Auskunftsersuchen gemäß § 47 Polizeiaufgabengesetz (PAG) sollte der Antragsteller nach Auffassung des TLfDI zukünftig grundsätzlich keine beglaubigte Personalausweiskopie mehr vorlegen müssen. Eine einfache Kopie reicht dafür grundsätzlich aus. Einzelne Datenfelder auf der Personalausweiskopie kann der Antragsteller zudem schwärzen, da sie für die Identifizierung nicht erforderlich sind (z. B. Ausweisnummer, Größe, Augenfarbe).

Bei Auskunftsersuchen nach § 47 PAG kann nur in Ausnahmefällen die Vorlage einer beglaubigten Kopie des Personalausweises gefordert werden (Zweifel an der Echtheit der Kopie). Ansonsten reicht die Vorlage einer einfachen Kopie.

8.9 Elektronische Fußfesseln und der Datenschutz

Aus einem Presseartikel im Februar 2017 ging hervor, dass der Thüringer Innenminister das Vorhaben der Bundesregierung, eine elektronische Fußfessel für sogenannte Gefährder einzuführen, begrüßte.
Daraufhin bat der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) den Thüringer Innenminister um eine Mitteilung, inwieweit die Rechtslage dementsprechend angepasst wird und in welchem zeitlichen Rahmen dies erfolgen soll. Weiterhin bat der TLfDI um eine möglichst frühzeitige Übersendung des entsprechenden Gesetzentwurfs der Bundesregierung.
Das Thüringer Innenministerium teilte dem TLfDI mit, dass sich der von der Bundesregierung beschlossene Gesetzentwurf zur Neustrukturierung des Bundeskriminalamtsgesetzes (vgl. BR-Drs. 109/17) im laufenden Gesetzgebungsverfahren befinde. In diesem Gesetzentwurf seien u. a. die Einsatzregeln für die elektronische Aufenthaltsüberwachung bei sogenannten Gefährdern festgelegt. Bereits vor dem möglichen Zustandekommen des Gesetzes werde ein potentieller Anpassungsbedarf für den Zuständigkeitsbereich der Landespolizeibehörden geprüft. Dennoch sei zunächst das Gesetzgebungsverfahren abzuwarten.

Das Gesetzgebungsverfahren und die Vorschriften für den Einsatz von elektronischen Fußfesseln für Gefährder werden vom TLfDI datenschutzrechtlich begleitet. Hierfür bat der TLfDI das Thüringer Innenministerium um entsprechende Informationen zum Gesetzgebungsverfahren.

8.10 Fallbearbeitungssystem der Polizei – auch hier gilt Datensparsamkeit – Teil 2

Bereits im vergangenen 11. Tätigkeitsbericht hatte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) darüber berichtet, dass die Thüringer Polizei das Fallbearbeitungssystem (FBS-TH) einführen möchte. Dabei handelt es sich um ein speziell auf die kriminalpolizeiliche Arbeit bezogenes automatisiertes Verfahren, welches neben dem bereits bestehenden Vorgangsbearbeitungssystem (VBS) existieren und kriminalpolizeiliche Zusammenhänge von unterschiedlichen Fällen aufzeigen soll (siehe hierzu 11. Tätigkeitsbericht zum Datenschutz: Öffentlicher Bereich,

7.19 Fallbearbeitungssystem der Polizei – auch hier gilt Datensparsamkeit, S. 241 f.).
Das FBS-TH befindet sich nach Kenntnis des TLfDI gegenwärtig im Testbetrieb. Hierzu befinden sich derzeit diverse informationstechnische Dokumente (mit einem Umfang von ca. 4.000 Seiten) in Prüfung beim TLfDI.
Über den Abschluss der datenschutzrechtlichen Prüfung wird der TLfDI informieren.

Die Polizei hat – aufgabenbedingt – Zugang zu einer Fülle von personenbezogenen Daten. Jedoch darf auch sie nicht sämtliche Daten sammeln und auswerten. Gerade bei einem Fallbearbeitungssystem wie FBS-TH hat die verantwortliche Stelle sorgfältig zu prüfen, welche Fälle in das Fallbearbeitungssystem aufgenommen werden. Dies ergibt sich nicht zuletzt aus dem Gebot der Datensparsamkeit gem. § 1 Abs. 2 Satz 1 ThürDSG.

8.11 Presse als Facebook-Fahnder?

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) erlangte im Berichtszeitraum Kenntnis davon, dass eine Landespolizeiinspektion eine E-Mail mit einer Pressemitteilung an Pressevertreter versandt hatte. Dieser Pressemitteilung waren drei Fahndungsfotos angehängt sowie der Aufruf an die Pressevertreter, die Fahndung bitte auch bei Facebook einzustellen.
Nach Auskunft der zuständigen Landespolizeiinspektion handelte es sich bei der im Medienverteiler geäußerten Bitte zur Einstellung der Fahndung in Facebook um ein individuelles Büroversehen. Adressat des Ansinnens war die Landespolizeidirektion Erfurt. Durch diese sollte eine Verlinkung zu Facebook vorgenommen werden. Für die anderen Adressaten war die Aufforderung nicht gedacht. Eine Vervielfältigung der Fahndungsfotos via Facebook durch die angeschriebenen Pressevertreter sei nicht erfolgt.
Der TLfDI wies die Thüringer Polizei darauf hin, dass durch einen Aufruf, Fahndungen auf Facebook einzustellen, nicht verhindert werden kann, dass personenbezogene Daten auch auf Servern privater Anbieter gespeichert, verarbeitet und weitergegeben werden. Es wurde daher dringend empfohlen, von derartigen Aufrufen künftig abzusehen und sämtliche Mitarbeiter dahingehend zu sensibilisieren.

Grundsätzlich darf die Polizei nur Fahndungsfotos veröffentlichen, wenn es dafür einen Gerichtsbeschluss gibt. Üblicherweise werden Daten, welche Persönlichkeitsrechte berühren, für die Dauer der Öffentlichkeitsfahndung durch die Landespolizeidirektion unter www.thueringen.de eingestellt und anschließend auf Facebook verlinkt. Hierdurch wird sichergestellt, dass personenbezogene Daten nicht auf Servern privater Anbieter gespeichert und verarbeitet werden. Unzulässig hingegen ist die Veröffentlichung von Fahndungsfotos ohne Gerichtsbeschluss auf Facebook (https://www.heise.de/newsticker/meldung/Datenschuetzer-Fahndungsfotos-nicht-bei-Facebook-veroeffentlichen-3339698.html).



8.12 DNA-Datei und Datenschutz – Teil 2

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) hatte bereits in seinem 11. Tätigkeitsbericht über die Einführung einer elektronischen Datenbank (DNA-Intern-Datei), in welcher DNA-Identifizierungsmuster von Mitarbeitern der Thüringer Polizei eingestellt werden sollen, die aufgabenbedingt häufig mit (Tatort-)Spuren zu tun haben, berichtet.

Bei der Einwilligung der Betroffenen zur Abgabe einer Speichelprobe und zur Speicherung in der Referenzdatei zur Erleichterung des Ausschlusses von sogenannten Trugspuren kommt der Freiwilligkeit maßgebliches Gewicht zu. Die/der Betroffene muss zunächst über Sinn und Zweck und Auswertungsmöglichkeiten informiert sein. Des Weiteren darf die Person bei Ablehnung der Einwilligung keine Maßnahmen arbeitsrechtlicher bzw. dienstrechtlicher Natur zu befürchten haben. Eine nunmehr vorgenommene Ergänzung im Formular zur Einwilligung offerierte aber gerade die Möglichkeit, dass

dienstrechtliche und arbeitsrechtliche Maßnahmen infrage kämen, „wenn Anhaltspunkte dafür bestehen, dass wiederholt pflichtwidrig bzw. absichtlich Kontaminationen verursacht wurden“.
Zwar ist die arbeits- und dienstrechtliche Kontrolle der betroffenen Bediensteten nicht originär beabsichtigt. Ausreichend ist jedoch allein die Möglichkeit.
Durch die abgeänderte Einwilligung erklären sich die betroffenen Bediensteten damit einverstanden, dass die Speicherung zu anderen Zwecken zu ihren Lasten ausgewertet wird. Die Einwilligung bedarf zu ihrer Rechtswirksamkeit der freiwilligen und unbeeinflussten Entscheidung von Betroffenen, mit der Erhebung, Speicherung und Nutzung ihrer Daten einverstanden zu sein. Sie verlangt ein ohne Zwang erteiltes Einverständnis mit der vorgesehenen Datenverarbeitung. Die Betroffenen dürfen sich nicht in einer Situation befinden, die sie faktisch dazu zwingt, sich mit der Erhebung und Verwendung der von ihnen verlangten Daten einverstanden zu erklären. Das Vorliegen eines gewissen Zwangs ist im Beschäftigungsverhältnis jedoch kaum auszuschließen. Die betroffenen Bediensteten werden bei lebensnaher Betrachtung durchaus damit rechnen oder jedenfalls nicht völlig ausschließen können, dass die Nichtteilnahme an dem vorgesehenen Verfahren möglicherweise einen beruflichen Nachteil mit sich bringen könnte. So wurde von gewerkschaftlicher Seite in Nordrhein-Westfalen bereits darauf hingewiesen, dass „auch Polizeibeamte in einem Abhängigkeitsverhältnis zu ihren Vorgesetzten stehen. Sie könnten sich zur Abgabe ihrer DNA-Probe genötigt sehen, weil sie sonst berufliche Nachteile befürchten.“ (https://www.gdp.de/gdp/gdpnrw.nsf/id/dna-datei)
Der eingefügte Hinweis im Einwilligungsformular vermischte damit mögliche Auswertungsmöglichkeiten mit dem ursprünglichen Zweck, die Freiwilligkeit der Einwilligung zu gewährleisten. Der TLfDI hielt und hält dies für eine Überfrachtung und gleichzeitig eine Zweckänderung der Datei.
Ferner wies der TLfDI auf Folgendes hin: Die Abgabe der DNA-Probe – vor dem Hintergrund ihrer Verwendung für arbeits- und disziplinarrechtliche Zwecke – stellt einen erheblichen Eingriff in das Recht auf informationelle Selbstbestimmung dar, der nicht durch eine einfache Dienstanweisung oder Dienstvereinbarung geregelt oder vorgeschrieben

werden kann. Vielmehr bedarf es hierfür einer bereichsspezifischen gesetzlichen Grundlage.
Insgesamt wurden die Bedenken des TLfDI weiterhin aufrechterhalten. Bis dato liegt dem TLfDI noch keine abschließende Stellungnahme zum weiteren Vorgehen des Thüringer Ministeriums für Inneres und Kommunales (TMIK) in dieser Sache vor. Der TLfDI wird daher über den Fortgang der datenschutzrechtlichen Kontrolle der DNA-Intern-Datei im nächsten Tätigkeitsbericht erneut informieren.

Die DNA-Datei soll dem Abgleich mit der fallbezogenen Spurenmusterdatei und dem rechtzeitigen Erkennen von DNA-Spuren dienen, welche durch Personen, die mit der Suche, Sicherung und Analysierung dieser Spuren befasst sind, verursacht wurden (Trugspuren). Falsche Ermittlungsansätze sollen dadurch ausgeschlossen werden. Der Abgleich soll nur fallbezogen mit den DNA-Identifizierungsmustern der für diesen Fall betrauten Mitarbeiter erfolgen. Dieser Ansatz ist auf der einen Seite – insbesondere aufgrund der Erfahrungen im Fall der verschwundenen Peggy im Jahr 2016 – sehr zu begrüßen. Auf der anderen Seite ist aber auch dem Recht auf informationelle Selbstbestimmung der mit der Auswertung von DNA-Spuren beschäftigten Mitarbeiter der Polizei Rechnung zu tragen.

8.13 Funkzellenabfrage durch Privatunternehmen?

Dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) war im Berichtszeitraum bekannt geworden, dass die in Thüringen im Rahmen einer sogenannten Funkzellenabfrage (vgl. § 100g Abs. 3 Strafprozessordnung - StPO, § 34b Abs. 3 Satz 2 Thüringer Gesetz über die Aufgaben und Befugnisse der Polizei [Polizeiaufgabengesetz - PAG]) gewonnenen Daten von Privatunternehmen verarbeitet werden sollen.
Die Funkzellenabfrage (FZA) ist eine unter Richtervorbehalt stehende offene Ermittlungsmaßnahme zum Zweck der Strafverfolgung bei Straftaten von erheblicher Bedeutung. Die Behörden fragen dabei Telekommunikationsverbindungsdaten ab, die in einer bestimmten, räumlich bezeichneten Funkzelle in einem bestimmten Zeitraum anfallen. Ziel der Maßnahme ist es, die Identität von Tatverdächtigen zu klären oder weitere Anhaltspunkte zur Aufklärung des Sachverhaltes zu erlangen.

Eine Nachfrage des TLfDI beim Thüringer Landeskriminalamt ergab, dass eine Auswertung sogenannter Funkzellendaten durch ein Privatunternehmen in absehbarer Zeit nicht vorgesehen sei.

Die Maßnahme der Funkzellenabfrage ist seit Dezember 2015 im § 100g Abs. 3 StPO gesetzlich geregelt. Voraussetzungen für eine Erhebung der notwendigen Verkehrsdaten ist die Beachtung der sogenannten Subsidiaritätsklausel, wonach u. a. die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise aussichtslos oder wesentlich erschwert wäre sowie, dass die Maßnahme in einem angemessenen Verhältnis zur Bedeutung der Sache stehen muss. Im Rahmen der Vorratsdatenspeicherung können Daten bei besonders schweren Straftaten unter den Voraussetzungen des § 113b Telekommunikationsgesetz bis zu zehn Wochen rückwirkend erhoben werden. Aufgrund gesetzlicher Benachrichtigungspflichten sind die Betroffenen gemäß § 101a Abs. 6 StPO über die Maßnahme zu benachrichtigen. Davon kann mit Zustimmung des zuständigen Gerichts im Einzelfall abgesehen werden, wenn der Zweck der Maßnahme gefährdet wäre. Eine Funkzellenabfrage durch Privatunternehmen ist in Thüringen derzeit nicht vorgesehen.

8.14 Eine Polizeibeamtin auf Abwegen

Im Berichtszeitraum hat sich der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) intensiv mit einem Beschwerdefall gegen eine Polizeidienstelle beschäftigt. Folgender Sachverhalt lag der Beschwerde zugrunde:
Gegen den Beschwerdeführer selbst wurde ein Ermittlungsverfahren bei der Staatsanwaltschaft wegen des Verstoßes gegen das Betäubungsmittelgesetz geführt. In diesem Zusammenhang ist dem Beschwerdeführer ein Schriftsatz eines Rechtsanwaltes bekannt geworden, aus welchem hervorging, dass eine Polizeibeamtin „im Rahmen ihrer beruflichen Ausübung“ Kenntnis davon erlangt habe, dass gegen den Beschwerdeführer ein Verfahren wegen des Verstoßes gegen das Betäubungsmittelgesetz geführt wird. Der vom Beschwerdeführer geäußerte Verdacht, dass sich die Polizeibeamtin die vorstehenden Angaben durch eine möglicherweise unrechtmäßige Datenerhebung aus den polizeilichen Auskunfts- und Recherchesystemen IGVP (= Integrationsverfahren Polizei) und INPOL (= Informa-

tionssystem der Polizei) verschafft habe, wurde dadurch erhärtet, dass sich der Sohn des Beschwerdeführers gerade mit der besagten Polizeibeamtin in einem Verfahren zum Aufenthaltsbestimmungsrecht des gemeinsamen Kindes befand. Im Rahmen der Prüfung durch den TLfDI sind diesem weitere Personen bekannt geworden, zu welchen die Polizeibeamtin Abfragen in den polizeilichen Auskunfts- und Recherchesystemen IGVP und INPOL vorgenommen hatte.

Eine Rechtsgrundlage für den von der Polizeibeamtin vorgenommenen Abruf der personenbezogenen Daten war nicht gegeben. Gegen die Polizeibeamtin wurde von der zuständigen Staatsanwaltschaft ein Ermittlungsverfahren eingeleitet, welches gemäß § 153 Strafprozessordnung (StPO) vorläufig gegen eine Auflage (Zahlung eines Geldbetrages) eingestellt wurde. Ein Freispruch erfolgte indessen nicht. Nach Angaben der zuständigen Staatsanwaltschaft wurde der Geldbetrag von der Polizeibeamtin zwischenzeitlich gezahlt und das Verfahren endgültig nach § 153 Abs. 2 StPO eingestellt.

Der TLfDI nahm den Vorfall zum Anlass, um bei der Thüringer Polizei nachzufragen, welche technischen und organisatorischen Maßnahmen bestehen bzw. im Nachgang des Vorfalls getroffen wurden, damit künftig rechtswidrige Datenabfragen ausgeschlossen werden können. Gemäß § 9 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) haben öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten verarbeiten, die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Bestimmungen dieses Gesetzes zu gewährleisten. Nach § 9 Abs. 2 Satz 1 ThürDSG ist unter anderem ein Sicherheitskonzept zu erstellen, auf dessen Grundlage die technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten zu treffen sind.

Die datenschutzrechtliche Prüfung des TLfDI ergab, dass für die polizeilichen Informationssysteme IGVP und INPOL Sicherheitskonzepte vorliegen. Alle Abfragen werden zudem für ein Jahr protokolliert. Darüber hinaus versicherte die Landespolizeidirektion (LPD) Erfurt dem TLfDI, dass jedem geäußerten Verdachtsfall, der einen Verstoß gegen das ThürDSG begründet, durch die LPD Erfurt nachgegangen und auch entsprechend geahndet wird (z. B. mittels Bußgeldbescheid oder Disziplinarverfahren). Ungeachtet dessen wird die LPD Erfurt regelmäßig auch präventiv tätig, z. B. durch entsprechende Veröffentlichungen und Hinweise im Intranet. Außer-

dem werden alle Bediensteten der Thüringer Polizei halbjährlich zu § 6 ThürDSG (Datengeheimnis) sowie zu Abfragen personenbezogener Daten aus polizeilichen Informationssystemen belehrt. Die Belehrungen sind mit Unterschrift zu quittieren.
Nach Einschätzung des TLfDI waren die durchgeführten technischen und organisatorischen Maßnahmen der Thüringer Polizei grundlegend geeignet, unrechtmäßige Datenerhebungen zu verhindern. Der TLfDI teilte jedoch auch die Einschätzung der LPD Erfurt, dass die getroffenen Maßnahmen nur einen grundlegenden Schutz vor unbefugten Zugriffen auf polizeiliche Informationssysteme von außen bieten können. Sie ermöglichen allerdings keinen allumfassenden Schutz vor unbefugten Abfragen von Bediensteten, wie im vorliegenden Fall geschehen.

Gegen kriminelle Energie schützen auch die besten Datenschutzregelungen nur bedingt: Gemäß § 6 Thüringer Datenschutzgesetz (ThürDSG) ist es den bei Daten verarbeitenden Stellen beschäftigten Personen untersagt, personenbezogene Daten unbefugt zu verarbeiten oder zu nutzen (Datengeheimnis). Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort. Wenn dennoch ein Bediensteter der Thüringer Polizei unrechtmäßig personenbezogene Daten über Familienmitglieder erhebt, ist dies zuerst erst ein Fall für den Staatsanwalt und dann für den TLfDI.

8.15 Polizeiproblem: Kontaktdaten von Journalisten

Im Dezember 2016 erreichte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) die Mitteilung, dass seitens der Landespolizeidirektion Erfurt (LPD) eine Aufforderung an die Thüringer Pressevertreter erging, diverse personenbezogene Daten (Name und Vorname, Anschrift, E-Mail-Adresse, Telefonnummern des Mobil- und des Festnetzes) zur Reorganisation der Kontaktdateien der Medienvertreter zu übersenden.
Die Aufforderung erfolgte per E-Mail unter Nutzung eines offenen Empfängerkreises („carbon copy“ =„Cc“), sodass mit dem Versand der E-Mail zugleich die Übermittlung von über 100 E-Mail-Adressen der Pressevertreter an jeden einzelnen Adressaten der E-Mail erfolgte.
Der zugrundeliegende Sachverhalt wurde daraufhin datenschutzrechtlich vom TLfDI überprüft. Hierzu musste zunächst die Recht-

mäßigkeit der Datenerhebung i. S. d. Abfrage der Kontaktdaten der Medienvertreter betrachtet werden. Des Weiteren wurde die Datenübermittlung durch Nutzung des offenen Verteilerkreises beim E-Mail-Versand auf datenschutzrechtliche Konformität geprüft. Seitens des TLfDI wurde der Sachverhalt bezüglich der Rechtmäßigkeit der Datenerhebung wie folgt bewertet:

Gemäß § 4 Abs. 1 ThürDSG ist die Verarbeitung (umfasst auch das Erheben personenbezogener Daten, vgl. § 3 Abs. 3 Nr. 1 ThürDSG) und Nutzung personenbezogener Daten nur zulässig, wenn dieses Gesetz oder eine andere Rechtsvorschrift sie erlaubt oder anordnet oder, soweit der Betroffene eingewilligt hat.

Der Gesetzgeber hat für den Fall der Einwilligung beim Betroffenen klare Vorgaben in § 4 Abs. 3 ThürDSG definiert. Soweit die Einwilligung bei dem Betroffenen eingeholt wird, ist er auf den Zweck und den Umfang der Verarbeitung oder Nutzung und die voraussichtliche Dauer der Speicherung seiner Daten, auf seine Rechte auf Auskunftserteilung, Berichtigung und Löschung sowie auf Verlangen auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Daneben bedarf die Einwilligung der Schriftform oder der elektronischen Form mit einer qualifizierten elektronischen Signatur. Im vorliegenden Fall stellte der TLfDI fest, dass die E-Mail der LPD an die Medienvertreter keine der genannten Vorgaben beachtete. Eine wirksame Einwilligung der Medienvertreter lag somit nicht vor.

Da auch keine Rechtsgrundlage für die geschilderte Datenerhebung aus dem ThürDSG bzw. einer anderen Rechtsvorschrift ersichtlich war, ermangelte es der Voraussetzung für eine Datenerhebung.

Bezüglich der Übermittlung der E-Mail mit offenem Empfängerkreis wurde der Sachverhalt seitens des TLfDI wie folgt bewertet:

Gemäß § 9 Abs. 1 ThürDSG haben öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten verarbeiten, die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Bestimmungen dieses Gesetzes zu gewährleisten. Das datenschutzrechtliche Gebot der „Vertraulichkeit“ gebietet danach, dass nur Befugte personenbezogene Daten zur Kenntnis nehmen können (§ 9 Abs. 2 Satz 1 Nr. 1 ThürDSG).

Im Adressfeld der LPD-E-Mail vom Dezember 2016 wurden über 100 E-Mail-Adressen an diverse Medienvertreter übermittelt und für diese sichtbar gemacht. Eine rechtliche Befugnis, die es gestattet, dass einzelne Medienvertreter die E-Mail-Adressen der jeweiligen anderen Medienvertreter zur Kenntnis nehmen, ist für den TLfDI

nicht erkennbar gewesen. Vielmehr hätte der Versand an mehrere Empfänger als Blindkopie („Bcc“) erfolgen müssen. Der TLfDI stellte daher einen Verstoß gegen das „Vertraulichkeitsgebot“ gem. § 9 Abs. 2 S. 1 Nr. 1 ThürDSG fest.
Die durch die LPD praktizierte Verfahrensweise im Hinblick auf die Datenerhebung sowie die Art und Weise des E-Mail-Versandes war somit gem. § 39 ThürDSG vom TLfDI zu beanstanden. Der TLfDI forderte überdies, dass die LPD zukünftig die Vorschriften des Datenschutzes bei der Verarbeitung und Nutzung personenbezogener Daten einhält.
Seither erfolgen Datenerhebungen seitens der LPD nur noch unter Nutzung einer den Anforderungen des § 4 Abs. 3 ThürDSG entsprechenden Einwilligungserklärung.
Nachdem dem TLfDI im Nachgang weitere Vorfälle im Zusammenhang mit der beschriebenen fehlerhaften Benutzung des Presseverteilers bekannt wurden, ergingen weiteren Beanstandungen sowie Hilfestellungen zum rechtskonformen Umgang mit Verteilerfunktionen im E-Mail-Verkehr.
Der E-Mail-Versand wird leider noch immer nicht flächendeckend mittels Nutzung der Blindkopie-Funktion („Bcc“) realisiert, sodass o. g. datenschutzrechtliche Mängel seitens der LPD noch nicht in Gänze abgestellt wurden. Der TLfDI wird die Entwicklung weiter verfolgen.

Die Erhebung personenbezogener Daten bedarf gem. § 4 Abs. 1 ThürDSG einer Rechtsgrundlage, die dies gestattet bzw. anordnet, oder einer Einwilligung des Betroffenen. Damit eine wirksame Einwilligung vorliegt, müssen die Anforderungen des § 4 Abs. 3 ThürDSG hinsichtlich der inhaltlichen Ausgestaltung der Einwilligung eingehalten werden.
Sollten öffentliche Stellen personenbezogene Daten verarbeiten, so müssen sie erforderliche technisch-organisatorische Maßnahmen treffen, dass u. a. nur Befugte personenbezogene Daten zur Kenntnis nehmen können (Vertraulichkeitsgebot gem. § 9 Abs. 2 Satz 1 Nr. 1 ThürDSG). Bei Übermittlung von Daten an mehrere Empfänger muss gewährleistet sein, dass hierdurch nicht die Adressdaten der einzelnen Empfänger gegenseitig sichtbar gemacht werden. Dies ist durch Nutzung der Funktion „Blindkopie“ („Bcc“) sichergestellt.

8.16 Verdienstausfall durch Zeugenaussage: In welchem Umfang sind personenbezogene Daten Dritter anzugeben?

Ein Bürger beschwerte sich beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) darüber, dass sich die Gerichte bei der Gewährung von Entschädigungen für den Verdienstausfall durch Zeugenaussagen an strengen Vorgaben orientieren würden. So würden beispielsweise vom Amtsgericht Arnstadt nicht die Gewerbeanmeldung und der Steuerbescheid für die Geltendmachung ausreichen. Vielmehr sollten potentielle Auftraggeber (Name, Adresse) benannt werden, die aufgrund des jeweiligen Gerichtstermins nicht die Dienste des vorgeladenen Zeugen in Anspruch nehmen konnten.
Durch Nachfrage beim Thüringer Oberverwaltungsgericht sowie beim Ministerium für Migration, Justiz und Verbraucherschutz (TMMJV) konnte der TLfDI feststellen, dass eine einheitliche Verfahrensweise hinsichtlich der Vorgaben für Verdienstausfallszahlungen nicht besteht, was der unklaren gesetzlichen Formulierung sowie der dazu ergangenen Rechtsprechung und Kommentierung geschuldet ist. Nach § 22 des Gesetzes über die Vergütung von Sachverständigen, Dolmetscherinnen, Dolmetschern, Übersetzerinnen und Übersetzern sowie die Entschädigung von ehrenamtlichen Richterinnen, ehrenamtlichen Richtern, Zeuginnen, Zeugen und Dritten (JVEG) erhalten Zeugen, denen ein Verdienstausfall entsteht, eine Entschädigung, die sich nach dem regelmäßigen Bruttoverdienst einschließlich der vom Arbeitgeber zu tragenden Sozialversicherungsbeiträge richtet und für jede Stunde höchstens 21 Euro beträgt. Aufgrund der Formulierung „Verdienstausfall entsteht“ erachten es Rechtsprechung und Kommentierung übereinstimmend als notwendig, dass durch die Heranziehung als Zeuge auch ein konkreter Verdienstausfall eintritt. § 22 JVEG enthält jedoch keine Regelung zum Nachweis der Höhe des geltend gemachten Verdienstausfalls. Abhängig Beschäftigte haben die Höhe des Verdienstausfalls in der Regel durch Vorlage einer Bescheinigung ihres Arbeitgebers nachzuweisen (Schneider/Volpert/Fölsch, Gesamtes Kostenrecht, JVEG, § 22 Randnr. 13; Binz/Dörndorfer/ Petzold/Zimmermann, JVEG, § 22 Randnr. 7).
Selbstständige können eine entsprechende Bescheinigung nur in den seltensten Fällen vorlegen. Welche Anforderungen hier zu stellen sind, wird kontrovers betrachtet. Einerseits führt die Kommentierung

aus, dass bei Aufsichtsführenden großer Betriebe die Annahme eines Verdienstausfalls bei nur kurzer Abwesenheit nicht in Betracht komme und dass die Vorlage einer Gewerbeanmeldung allein zur Glaubhaftmachung eines Verdienstausfalls nicht ausreiche (Binz/Dörndorfer/Petzold/Zimmermann, JVEG, § 22 Randnr. 6; Bayerisches Landessozialgericht, Beschluss v. 14. Juni 2006, Az: L 8 AL 491/04.Ko). Andererseits soll es bei Selbstständigen, Freiberuflern usw. in der Regel ausreichend sein, dass ein behaupteter Verdienstausfall nach der Lage des Falls wahrscheinlich ist (Binz/Dörndorfer/Petzold/Zimmermann, JVEG, § 22 Randnr. 6). lm Einzelfall komme damit ausnahmsweise eine Glaubhaftmachung gemäß § 294 Zivilprozessordnung in Betracht (Schneider/Volpert/Fölsch, Gesamtes Kostenrecht, JVEG, § 22 Randnr. 15). Danach kann, wer eine tatsächliche Behauptung glaubhaft zu machen hat, sich aller Beweismittel bedienen. Das Landessozialgericht Berlin-Brandenburg hat im Beschluss vom 10. Januar 2017 (Az: L 2 SF 248/16 E) festgehalten, dass die Anforderungen an die Feststellung eines Verdienstausfalls bei Selbstständigen nicht zu überspannen sind, sodass eine Entschädigung für Verdienstausfall daher immer zu gewähren ist, wenn Lebensstellung und ausgeübte Erwerbstätigkeit die Vermutung rechtfertigen, dass überhaupt etwas versäumt wird.

Diese differierenden Ansichten spiegeln sich nach Angaben der TMMJV auch in den Berichten der gerichtlichen Praxis des Geschäftsbereichs wider. Thüringer Oberverwaltungsgericht, Thüringer Landesarbeitsgericht und Thüringer Finanzgericht gaben an, dass dort in keinem Fall die Benennung potentieller Auftraggeber verlangt werde. In der Regel sähen die genannten Gerichte es als ausreichend an, dass der behauptete Verdienstausfall nach Lage des Einzelfalls wahrscheinlich ist. Lediglich in begründeten Einzelfällen sei die Vorlage weiterer Nachweise, etwa eines Steuerbescheides, denkbar. Das Thüringer Landessozialgericht wies in diesem Zusammenhang darauf hin, dass die Umstände des Einzelfalls, insbesondere die konkret ausgeübte selbstständige Tätigkeit berücksichtigt werden müssen. Nur dann, wenn die Angaben über die Erwerbstätigkeit nicht nachvollziehbar, widersprüchlich oder lebensfremd seien, seien weitere Nachweise erforderlich. Allerdings könne etwa bei Ärzten bereits wegen der ärztlichen Schweigepflicht nicht verlangt werden, die Namen möglicher Patienten zu nennen. Die Gerichte der ordentlichen Gerichtsbarkeit führten sinngemäß aus, dass sich der

zuständige Kostenbeamte im Rahmen der freien Beweiswürdigung davon zu überzeugen habe, ob der geltend gemachte Verdienstausfall auch tatsächlich eingetreten ist. Hierbei erachteten die meisten Gerichte die Vorlage einer Gewerbeanmeldung als ausreichend; weitergehende personenbezogene Daten würden nicht angefordert. Lediglich in Ausnahmefällen, etwa wenn ein besonders hoher Erstattungsbetrag geltend gemacht werde, werde der Antragsteller um Beantwortung weitergehender Fragen gebeten.

Die Bezirksrevisorin – diese hat u. a. folgende Aufgaben: Prüfung des (Gerichts-) Kostenansatzes, Geschäftsprüfung, Prüfung der Kostenberechnung / Verwahrgeschäfte der Notarinnen und Notare, Vertretung der Landeskasse – beim Landgericht Erfurt und damit die Amtsgerichte dieses Landgerichtsbezirks, unter anderem auch das Amtsgericht Arnstadt, legten im Vergleich mit den anderen Gerichten strengere Maßstäbe an. So führte das Landgericht Erfurt aus, dass der von Selbstständigen verlangte Nachweis über einen konkreten Verdienstausfall der Handhabung für abhängig Beschäftigte entspreche, bei denen die Vorlage eines Gehaltsnachweises nicht ausreiche, sondern eine Verdienstausfallbescheinigung des Arbeitgebers gefordert werde. Auch in solchen Fällen gebe es jedoch keine pauschale Anweisung dahingehend, dass Selbstständige ihren geltend gemachten Verdienstausfall in jedem Fall durch die Benennung potentieller Auftraggeber nachzuweisen hätten. Bei Selbstständigen sei auf die Berufsgruppe bzw. die ausgeübte Tätigkeit im Einzelfall, etwa die unterschiedliche Arbeitsweise von Gewerbetreibenden mit festen Öffnungs- oder Sprechzeiten einerseits und Selbstständigen, die ihre Arbeitszeit im Wesentlichen selbst bestimmen, andererseits, abzustellen. Nach den Ausführungen der Bezirksrevisorin des Landgerichts Erfurt könne es daher im Einzelfall erforderlich sein, den geltend gemachten Verdienstausfall glaubhaft zu belegen und zu diesem Zweck etwa potentielle Auftraggeber zu benennen. Dies stelle jedoch lediglich eine Möglichkeit zur Glaubhaftmachung dar und werde nicht zwingend erwartet. Im konkreten Fall war die Benennung potentieller Auftraggeber nicht zwingend erforderlich und sollte vielmehr ein Beispiel für die Glaubhaftmachung darstellen.

Auch in dem konkreten Fall des Amtsgerichts Arnstadt hatte die dortige Kostenbeamtin den Antragsteller dazu aufgefordert, den tatsächlichen Verdienstausfall „zum Beispiel durch Vorlage eines potentiellen Auftraggebers“ nachzuweisen. Das Landgericht Erfurt führte zur datenschutzrechtlichen Problematik aus, dass sich auch

aus der von abhängig Beschäftigten geforderten Bescheinigung des Arbeitgebers personenbezogene Daten ergäben und dass das Gericht derartige Informationen ausschließlich zur Entscheidungsfindung verwende. Auch in anderen Fällen (etwa bei der Beantragung von Prozesskosten- oder Beratungshilfe) müssten die persönlichen und wirtschaftlichen Verhältnisse in gewissem Umfang offengelegt werden, wenn Leistungen aus der Staatskasse beantragt werden.
Abschließend konnte durch den TLfDI im konkreten Fall festgestellt werden, dass die Benennung potentieller Arbeitgeber für die Berechnung des Verdienstausfalles nicht erforderlich war. Der TLfDI hat das Thüringer Oberverwaltungsgericht darum gebeten, die nachgeordneten Gerichte auf die vertretene Rechtsauffassung hinzuweisen.

Zusammenfassend betrachtet, handelt es sich bei dem konkreten Fall am Amtsgericht Arnstadt nicht um eine pauschale Verfahrensweise der Gerichte im Freistaat Thüringen, sondern um eine Ausnahme. Aus Sicht des TLfDI war die Benennung potentieller Arbeitgeber im konkreten Einzelfall nicht erforderlich. Auf seine Rechtsauffassung hat der TLfDI das Thüringer Oberverwaltungsgericht hingewiesen.
Darüber hinaus besteht für jeden Antragsteller, sofern er mit der Sachbehandlung durch den Kostenbeamten nicht einverstanden ist, die Möglichkeit, nach § 4 JVEG einen Antrag auf gerichtliche Festsetzung zu stellen. Über diesen hat das Gericht unabhängig von der vorhergehenden Kostenfestsetzung durch den Kostenbeamten zu entscheiden. Sofern der Beschwerdewert 200 Euro übersteigt, kann gemäß § 4 Abs. 3 JVEG gegen den gerichtlichen Beschluss auch Beschwerde eingelegt werden.

8.17 Ermittlungsverfahren gegen Faschings-Cowboy

Im Berichtszeitraum hatte sich ein Rechtsanwalt mit ordnungsgemäßer Bevollmächtigung seines Mandanten an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) gewandt. Sein Mandant wurde beschuldigt, während einer Faschingsveranstaltung, als Cowboy verkleidet, eine Waffe geführt und abgefeuert zu haben. Insoweit wurde dem bis dato unschuldigen Mandanten ein Verstoß gegen das Waffengesetz, hier das unerlaubte Führen einer Schusswaffe nach § 52 Abs. 3 Nr. 2a, Anlage 2 Abschnitt 2 Unterabschnitt 1 Satz 1 Waffengesetz (WaffG), zur Last gelegt.

Im Rahmen des Ermittlungsverfahrens seien Fotos vom Beschwerdeführer gefertigt worden, die neben Porträtaufnahmen für eine Wahllichtbildvorlage auch Aufnahmen des kompletten Körpers wie Tätowierungen etc. beinhaltet hätten. Das Verfahren vor dem Amtsgericht Stadtroda endete letztendlich mit einem Freispruch. Der Anwalt versuchte vergeblich, die seiner Auffassung nach zu Unrecht gefertigten Bildaufnahmen sowie die erkennungsdienstliche Behandlung seines Mandanten einer Löschung zuzuführen. Schließlich erhielt er von der zuständigen Landespolizeiinspektion (LPI) Jena lediglich die Aussage, dass man einer Löschung zwar zustimme, dies jedoch aufgrund von § 45 Abs. 4 Nr. 2 Thüringer Polizeiaufgabengesetz (ThürPAG) gegenwärtig nicht in Betracht käme. Grund dafür sei, dass eine Löschung der Daten, die den Untersuchungsgegenständen des Untersuchungsausschusses 6/1 – Rechtsterrorismus und Behördenhandeln – des Thüringer Landtags unterlägen, vor dem Hintergrund der Arbeit dieses Untersuchungsausschusses eine Beweisnot erwarten ließe, sodass eine Löschung unterbleibe (Lösch-Moratorium oder Freeze-in-Erlass genannt).
Der TLfDI ersuchte die LPI Jena daraufhin mehrfach um ausführliche Stellungnahme zum Sachverhalt sowie um Mitteilung, welche personenbezogenen Daten (auch Bildaufnahmen) zum Mandanten des Rechtsanwaltes bei der Thüringer Polizei gespeichert waren, auf welcher Rechtsgrundlage die Speicherung/Verarbeitung – trotz Freispruchs – weiterhin erfolgte sowie wann die erhobenen personenbezogenen Daten einer Löschung zugeführt werden könnten. Nachdem die mehrmaligen Anfragen durch die LPI Jena ignoriert wurden, wies der TLfDI auf die Möglichkeit der Beanstandung wegen der mangelnden Unterstützung (§ 38 Abs. 1 ThürDSG), nach § 39 Abs. 1 ThürDSG hin.
Daraufhin erhielt der TLfDI schließlich eine Mitteilung, dass, nachdem die Erlasslage zum Lösch-Moratorium (sogenannter Freeze-in-Erlass) präzisiert wurde, eine erneute Prüfung erfolgt sei. Es lagen nunmehr keine Gründe im Sinne des § 45 Absatz 4 Nummer 2 ThürPAG vor und die Daten des Beschwerdeführers konnten gelöscht werden.

Der Freeze-in-Erlass ist ein Erlass des Thüringer Ministeriums für Inneres und Kommunales (TMIK) zur Aussetzung der Aussonderung und Löschung von Akten, Unterlagen, Dateien und sonstigen sächlichen Beweismitteln. Der Freeze-in-Erlass wurde im Juni 2016 mit-

tels Änderungserlass durch das TMIK aktualisiert. Gemäß § 38 Abs. 1 Nr. 1 ThürDSG sind der TLfDI und seine Beauftragten von allen öffentlichen Stellen in der Erfüllung ihrer Aufgaben zu unterstützen. Ihnen ist im Rahmen der Kontrollbefugnis nach § 37 ThürDSG (Kontrolle durch den TLfDI) insbesondere Auskunft zu ihren Fragen sowie Einsicht in alle Unterlagen und Akten, insbesondere in die gespeicherten Daten und in die Datenverarbeitungsprogramme, zu gewähren, die im Zusammenhang mit der Kontrolle nach § 37 ThürDSG stehen.

8.18 Kindeswohl steht an erster Stelle – auch für den Datenschutz

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichte die Eingabe eines Bürgers, welcher angab, dass eine Polizeiinspektion seine personenbezogenen Daten an das Jugendamt übermittelt habe.
Der Beschwerdeführer trug dem TLfDI folgenden Sachverhalt vor: Im Rahmen einer Verkehrskontrolle war durch die zuständige Polizeiinspektion festgestellt worden, dass der Beschwerdeführer keinen Führerschein besitzt, infolgedessen er eine Anzeige wegen „Fahrens ohne Führerschein“ erhielt. Im Nachgang zu dieser Anzeige wurde eine Bekannte des Beschwerdeführers zu einem persönlichen Termin beim Jugendamt eingeladen. Im Rahmen dieses Termins legte das Jugendamt einen Brief der Polizeiinspektion (PI) vor, in dem die Straftat des Beschwerdeführers ausführlich geschildert wurde. Um den Vorfall einer datenschutzrechtlichen Klärung zuzuführen, ersuchte der TLfDI zunächst die zuständige Landespolizeiinspektion (LPI) um eine Stellungnahme.
Grundsätzlich ist eine Datenverarbeitung, worunter auch die -übermittlung fällt, gem. § 4 Abs. 1 Satz 1 Thüringer Datenschutzgesetz nur zulässig, soweit der Betroffene darin einwilligt oder eine spezielle Rechtsgrundlage die Datenübermittlung erlaubt.
Im Ergebnis der Sachverhaltsprüfung teilte die LPI mit, dass im Rahmen der polizeilichen Aufgabenerfüllungen („Kindeswohlgefährdung“) die Polizeiinspektion (PI) eine Datenübermittlung an das Jugendamt vorgenommen hatte. Die Datenübermittlung erfolgte auf der Rechtsgrundlage der § 41 Abs. 3 Thüringer Gesetz über die Aufgaben und Befugnisse der Polizei (PAG) i. V. m. § 20 Abs. 7 S. 2 Thüringer Kinder- und Jugendhilfe-Ausführungsgesetz

(ThürKJHAG). Hiernach unterrichtet die Polizei das Jugendamt in den Fällen, in denen sonstige Maßnahmen zum Schutze junger Menschen erforderlich erscheinen.
Die PI teilte mit, dass bereits seit mehreren Jahren Verfahren wegen Straftaten und Ordnungswidrigkeiten gegen den Beschwerdeführer und seine Bekannte liefen, bei denen die minderjährigen Kinder mehrfach betroffen und konkret gefährdet worden seien. Diese Taten erstreckten sich über Körperverletzungen bei häuslicher Gewalt, Verstöße gegen das Betäubungsmittelgesetz, Führen von Fahrzeugen unter Einfluss berauschender Mittel sowie Fahren ohne Fahrerlaubnis. Der Beschwerdeführer lebte mit seiner Bekannten in einer gemeinsamen Wohnung, zusammen mit den beiden minderjährigen Kindern, von denen eines das leibliche Kind des Beschwerdeführers ist.
Im Rahmen ihrer Zuständigkeit hatte die PI aufgrund vorliegender Sachverhalte die Notwendigkeit erkannt, das Jugendamt zu verständigen, um Gefahren für die betroffenen minderjährigen Kinder abzuwehren. Der beim Jugendamt geführte Vorgang wurde von der PI dahingehend ergänzt, dass der Beschwerdeführer und seine Bekannte mehrfach beim Fahren unter berauschenden Mitteln und ohne Fahrerlaubnis und mit den Kindern im Fahrzeug festgestellt worden seien. Es bestanden konkrete Gefahren, dass der Beschwerdeführer bei ungehindertem Fortgang schwere Verkehrsunfälle verursachen könnte und die Kinder im Fahrzeug zu Schaden kommen könnten. Dies belegte die PI mit einem medizinischen Gutachten, das eine hohe Konzentration von Amphetaminen und Cannabinoiden im Blut des Beschwerdeführers attestiert hatte.
Aus datenschutzrechtlicher Sicht war die Übermittlung der personenbezogenen Daten des Beschwerdeführers an das Jugendamt gemäß § 41 Abs. 3 ThürPAG i. V. m. § 20 Abs. 7 ThürKJHAG nicht zu beanstanden, weil die Übermittlung der personenbezogenen Daten für die Aufgabenwahrnehmung des Jugendamtes zum Schutz der minderjährigen Kinder erforderlich war.

Nach § 41 Abs. 3 ThürPAG kann die Polizei personenbezogene Daten an Behörden und öffentliche Stellen übermitteln, soweit dies zur Erfüllung polizeilicher Aufgaben erforderlich ist. Nach § 20 Abs. 7 S. 2 ThürKJHAG unterrichtet die Polizei das Jugendamt in den Fällen, in denen sonstige Maßnahmen zum Schutze junger Men-

schen erforderlich erscheinen. Die Datenübermittlung im vorliegenden Falle war somit zulässig.

8.19 Datenerhebung der Behörde = Datenübermittlung des Unternehmens

Im Berichtszeitraum erreichte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) die Anfrage eines betrieblichen Datenschutzbeauftragten, welcher Informationen zur Rechtmäßigkeit von Datenübermittlungen an die Polizei begehrte.
Ein von ihm als Beauftragtem für den Datenschutz beratenes Unternehmen erhielt ein Auskunftsersuchen der Polizei im Rahmen eines staatsanwaltschaftlichen Ermittlungsverfahrens, welches das Unternehmen aufforderte, teils sensible Mitarbeiterdaten an die anfragende Polizeidienststelle zu übermitteln.
Um den Sachverhalt datenschutzrechtlich bewerten zu können, müssen sowohl die Datenerhebung durch die Polizei als auch die Datenübermittlung durch das Unternehmen einer differenzierten rechtlichen Prüfung zugeführt werden.
Die Beamten des Polizeidienstes haben im Rahmen des sogenannten Legalitätsprinzips gem. § 163 Strafprozessordnung (StPO) Straftaten zu erforschen und alle keinen Aufschub gestattenden Anordnungen zu treffen, um die „Verdunklung der Sache“ zu verhüten. Zu diesem Zweck sind sie entsprechend der Ermittlungsgeneralklausel auch befugt, Ermittlungen jeder Art vorzunehmen, soweit nicht andere gesetzliche Vorschriften ihre Befugnisse besonders regeln. Für zugrundeliegendes Auskunftsersuchen kommt somit in Ermangelung einer spezialgesetzlichen Grundlage die Generalklausel als Rechtsgrundlage polizeilichen Handelns, hier im Sinne der begehrten Datenerhebung, in Betracht.
Des Weiteren muss die im Auskunftsersuchen geforderte Datenübermittlung durch das angefragte Unternehmen betrachtet werden.
Abschießend wiesen die Datenschützer auf die Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen“ des Düsseldorfer Kreises (https://www.tlfdi.de/mam/tlfdi/datenschutz/video/oh-v__-durch-nicht-__ffentliche-stellen.pdf) und auf die Orientierungs-

hilfe „Sehen und gesehen werden“ zur Videoüberwachung durch Private der Landesbeauftragten für Datenschutz und Informationsfreiheit in Nordrhein-Westfalen (https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Datenschutzrecht/Inhalt/Videoueberwachung/Inhalt/_Sehen_und_gesehen_werden_-_Video_berwachung_durch_Private_in_NRW/Sehen_und_gesehen_werden1.pdf hin.



Die Übermittlung von zu eigenen Geschäftszwecken erhobenen Daten wird in § 28 Abs. 2 Nr. 2 b) BDSG geregelt. Die Übermittlung und Nutzung personenbezogener Daten zu einem anderen Zweck ist hiernach u. a. dann zulässig, wenn sie zur Verfolgung von Straftaten erforderlich ist und kein Grund zur Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung oder Nutzung hat.
Im Falle des hier eingeleiteten, strafrechtlichen Ermittlungsverfahrens treten die Interessen des Betroffenen regelmäßig gegenüber dem staatlichen Interesse an der Strafverfolgung zurück.
Im Ergebnis ist festzustellen, dass zugrundeliegendes Auskunftsersuchen seitens der ersuchenden Polizeidienststelle entsprechend § 163 StPO rechtlich legitimiert war.
Die Datenübermittlung seitens des angefragten Unternehmens gründete auf § 28 BDSG und war ihrerseits rechtmäßig.

Wird eine öffentliche oder nicht-öffentliche Stelle auf Grundlage eines Auskunftsersuchens um die Übermittlung von personenbezogenen Daten ersucht, so bedarf es hierfür einer Rechtsgrundlage, sowohl für die Erhebung seitens der anfragenden als auch der Übermittlung seitens der angefragten Stelle.
Sollten diese Rechtsgrundlagen für die angefragte Stelle aufgrund des vorliegenden Ersuchens nicht ersichtlich sein, besteht die Möglichkeit, die anfragende Stelle um die Benennung der Rechtsgrundlage zu erbitten. Sollte dahingehend eine Beantwortung nicht erfolgen bzw. auch nach dieser noch Unklarheit bezüglich der Rechtmäßigkeit der Datenerhebung und -übermittlung bestehen, so kann sich

jedermann mit Bitte um Prüfung des Sachverhalts an den Landesbeauftragten für den Datenschutz und die Informationsfreiheit wenden.

8.20 Polizeiliche Akten nicht beim TLfDI

Im Januar 2017 fragte ein Bürger beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) an, ob er beim TLfDI Einsicht in seine polizeiliche Akte erhalten könne, um ein Aktenzeichen zu erfahren.
Der TLfDI teilte dem Bürger mit, dass dies nicht möglich sei, da personenbezogene polizeiliche Akten beim TLfDI nicht vorliegen. Der TLfDI wies den Fragesteller darauf hin, seine Anfrage gemäß § 47 Abs. 1 S. 1 Thüringer Polizeiaufgabengesetz (PAG) an das Landeskriminalamt Thüringen zu richten. Hierbei ist zu beachten, dass in dem Antrag auf Auskunft die Art der personenbezogenen Daten und der Grund des Auskunftsersuchens genau bezeichnet werden müssen.

Sofern Bürger Auskunft über ihre bei einer Behörde gespeicherten personenbezogenen Daten erhalten wollen, müssen sie sich regelmäßig an die sachlich und fachlich zuständige Behörde wenden. Für polizeiliche Akten gewährt § 47 Abs. 1 Satz 1 PAG diesen Auskunftsanspruch. Dafür muss sich der Bürger an das Thüringer Landeskriminalamt wenden. Erst wenn von dort keine Antwort erteilt worden ist, hilft der TLfDI gern weiter.

8.21 Polizeivideo bei Facebook

Auf einer Autobahn kam es zu einem Verkehrsverstoß, indem ein in einen Stau geratener Autofahrer auf der Autobahn wendete und durch die Rettungsgasse zurück bis zur nächsten Ausfahrt fuhr. Die Polizei bat um Zeugenaussagen und verwandte zur Schilderung des Vorfalls ein von einer Privatperson gefertigtes Video, das sie bei Facebook einstellte.
Ein Bürger bezweifelte gegenüber dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) die datenschutzrechtliche Zulässigkeit des Videoeinsatzes, insbesondere hielt er ihn für unverhältnismäßig.
Der TLfDI teilte dem Bürger nach Prüfung der Angelegenheit mit, dass auf dem bei Facebook veröffentlichtem Video weder eine Per-

son noch das Kennzeichen des Fahrzeuges erkennbar waren. Damit lagen keine personenbezogenen Daten im Sinne von § 3 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) vor. Ein datenschutzrechtlicher Verstoß schied damit aus.
Da es sich darüber hinaus bei den Geschehnissen auf dem Video um eine extrem gefährliche Verhaltensweise handelte, die geeignet war, Menschen erheblichen Schaden zuzufügen, dürfte diese als Straftat „Gefährlicher Eingriff in den Straßenverkehr“ nach § 315 c) Abs. 1 Nr. 2 f) Strafgesetzbuch zu werten sein. Damit wäre auch – sofern personenbezogene Daten auf dem Video zu sehen gewesen wären – eine Datenverarbeitung für andere Zwecke gem. § 22 Abs. 1 Nr. 1 in Verbindung mit § 20 Abs. 2 Nr. 7 ThürDSG, nämlich zur Verfolgung von Straftaten, hier zulässig. Ob dagegen die Vorrausetzungen des § 23 Abs. 2 Nr. 4 ThürDSG (Wahrung eines wichtigen öffentlichen Interesses) bei der Ins-Internet-Stellung vorliegen würden, erscheint fraglich.

Die Polizei darf Fahndungsmaßnahmen ohne datenschutzrechtliche Zweifel bei Facebook platzieren, wenn hierzu keine personenbezogenen Daten verarbeitet werden.

8.22 Landrat im Zentrum der Daten

Ein Landrat wurde im Rahmen einer Besichtigung einer umgebauten Halle, die als Unterkunft für Asylbewerber diente, von einem Bewohner der Unterkunft angesprochen. Daraufhin fragte der Landrat nach dem Namen des Asylbewerbers, gab diesen in sein Tablet ein, um so eine Auflistung der gegen den Migranten bei der Polizei vorliegenden Anzeigen einsehen zu können. Nach § 87 Abs. 4 Aufenthaltsgesetz ist die Ausländerbehörde über strafrechtliche Verfahren durch die Polizei zu informieren, wodurch der Landrat die entsprechenden Kenntnisse besaß. Sekunden später zeigte der Landrat dem Mann die lange Liste der Anzeigen, die gegen ihn bei der Polizei vorlagen und fragte für die in der Unterkunft anwesenden Pressevertreter deutlich vernehmbar: „Soll ich die wirklich hier vorlesen?“
Den dargestellten Sachverhalt bewertete der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) folgendermaßen:
Nach § 4 Thüringer Datenschutzgesetz (ThürDSG) ist die Verarbeitung und Nutzung personenbezogener Daten nur zulässig, wenn

dieses Gesetz oder eine andere Rechtsvorschrift sie erlaubt oder anordnet oder soweit der Betroffene eingewilligt hat.
Der Landrat hatte im vorliegenden Sachverhalt der Öffentlichkeit, insbesondere der Presse gegenüber, zum Ausdruck gebracht, dass es zu dem betroffenen Asylbewerber strafrechtliche Einträge gab. Er hatte zwar nicht benannt, welche Einträge vorliegen, aber auch die Bekanntgabe, dass überhaupt strafrechtliche Einträge vorliegen, ist eine Übermittlung personenbezogener Daten.
Eine Einwilligung des Betroffenen bzw. die Erlaubnis durch eine spezielle Rechtsvorschrift zur Übermittlung dieser Daten lag offensichtlich nicht vor.
Zu prüfen war mithin, ob die Übermittlung nach § 22 Abs. 1 Nr. 2 ThürDSG zulässig gewesen sein könnte, was im Ergebnis zu verneinen war.
Nach § 22 Abs. 1 Nr. 2 ThürDSG ist die Datenübermittlung an Stellen außerhalb des öffentlichen Bereichs dann zulässig, wenn der Dritte, an den die Daten übermittelt werden, ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegt und der Betroffene kein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat.
Vorliegend hatte der betroffene Asylbewerber sich persönlich an den Landrat gewandt. Ausdrücklich nicht wandte sich der betroffene Asylbewerber an die anwesenden Pressevertreter, sondern der Bezug zur Presse wurde erst vom Landrat hergestellt. Ein Erfordernis dafür war für den TLfDI nicht zu erkennen. Ob spezifisch der betroffene Asylbewerber strafrechtliche Einträge hat(te), war und ist für die Öffentlichkeit nicht von Interesse. In jedem Fall aber hatte der betroffene Asylbewerber an dem Ausschluss der Übermittlung seiner personenbezogenen Daten an Dritte ein schutzwürdiges Interesse. Die öffentliche Berichterstattung über eine Straftat unter Namensnennung stellt regelmäßig eine erhebliche Beeinträchtigung des Persönlichkeitsrechts des Täters dar, weil sein Fehlverhalten – über die öffentliche Hauptverhandlung hinaus – öffentlich bekannt gemacht und seine Person in den Augen des Publikums negativ qualifiziert wird (BVerfG NJW 1973, 1226; NJW 1993, 1463/1464). Während bei schweren Straftaten regelmäßig ein Interesse der Öffentlichkeit an einer auch die Person des Täters einbeziehenden vollständigen Information über die Straftat besteht, ist bei den sonstigen Straftaten unter Berücksichtigung der jeweiligen Umstände des Einzelfalles zu entscheiden, wo die Grenze für das grundsätzlich vor-

hergehende Informationsinteresse der Öffentlichkeit an der aktuellen Berichterstattung zu ziehen ist (OLG München, Urteil vom 29. April 2008 Az. 18 U 5645/07).
Eine Interessenabwägung ließ ein Interesse der Öffentlichkeit an den Verurteilungen des Betroffenen hier nicht erkennen.
Damit bestand keine Rechtsgrundlage zur Übermittlung der Daten des betroffenen Asylbewerbers an die Presse, womit die vom Landrat vorgenommene Übermittlung datenschutzrechtlich unzulässig war.
Wegen der festgestellten Verletzung der genannten Vorschriften über den Datenschutz sprach der TLfDI eine Beanstandung nach § 39 Abs. 1 ThürDSG gegenüber dem Landrat aus.

Personenbezogene Daten, insbesondere über strafrechtliche Verurteilungen, dürfen nach der Rechtsprechung des Bundesverfassungsgerichtes zu den Grundrechten aus Art. 2 Abs. 1 in Verbindung mit Art. 1 GG in Abwägung mit Art. 5 Abs. 1 GG (Rundfunk- und Pressefreiheit, siehe Urteil „Soldatenmord in Lebach“, BVerfG, 5. Juni 1973 – 1 BvR 536/72) nur an die Presse herausgegeben werden, wenn nach einer Interessenabwägung im Einzelfall ein überwiegendes Informationsinteresse der Öffentlichkeit vorliegt und der Betroffene kein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat. Ansonsten ist die Übermittlung personenbezogener Daten gem. § 22 Abs. 1 Nr. 2 ThürDSG unzulässig.



Grunge Stempel rot VERTRAULICH – © Daniel Ernst / Fotolia.com

9. Verfassungsschutz

9.1 Stellungnahme des TLfDI gem. § 5 Abs. 2 Satz 4 Thüringer Verfassungsschutzgesetz

Das Thüringer Landesamt für Verfassungsschutz wandte sich im Berichtszeitraum in zwei Fällen an den Landesbeauftragten für den Datenschutz und für die Informationsfreiheit (TLfDI) und teilte jeweils mit, dass in den Entwürfen des Verfassungsschutzberichts für das Jahr 2014/2015 sowie für das Jahr 2016 Personennamen einzelner Extremisten erstmals Erwähnung finden sollten. Die genannten Personen seien öffentlichkeitswirksam als Anmelder bzw. Organisator extremistisch beeinflusster Versammlungen und Demonstrationen aufgetreten und nähmen darüber hinaus teilweise in den Landesverbänden bestimmter Parteien als Mitglieder des Vorstandes herausgehobene Funktionen ein. Die unveröffentlichten Berichte befänden sich derzeit in der abschließenden Hausabstimmung des Thüringer Ministeriums für Inneres und Kommunales.
Gem. § 5 Abs. 2 Satz 2 Thüringer Verfassungsschutzgesetz (ThürVerfSchG), dürfen der Öffentlichkeit personenbezogene Daten nur bekannt gegeben werden, wenn das Interesse an der Unterrichtung das schutzwürdige Interesse des Betroffenen überwiegt. Vor

einer erstmaligen Bekanntgabe personenbezogener Daten ist gem. § 5 Abs. 2 Satz 4 ThürVerfSchG dem Landesbeauftragten für den Datenschutz und für die Informationsfreiheit Gelegenheit zur Stellungnahme zu geben.
Zum Sinn des § 5 ThürVerfSchG lässt sich der Gesetzesbegründung (Seite 39 der Drucksache 5/7452), entnehmen, dass *„die Berichterstattung auch über Verdachtsfälle in bestimmten Phänomenbereichen sinnvoll" sei, „um einen vollständigen Überblick über die dort tätigen Personen und/oder Vereinigungen zu erhalten. Dies betrifft insbesondere die Verflechtungen von rechtsextremistischen Gruppierungen mit szenetypischen Musikgruppen sowie nicht offensichtlich politisch motivierten gewaltaffinen Gruppierungen. Voraussetzung ist jedoch, dass die Darstellung für das Zusammenhangsverständnis dienlich ist und tatsächliche Anhaltspunkte für verfassungsfeindliche Bestrebungen hinreichend gewichtig sind, um die Veröffentlichung etwa in Verfassungsschutzberichten auch angesichts der möglichen nachteiligen Auswirkungen auf die Betroffenen zu rechtfertigen."*
Unter Berücksichtigung der gesetzlichen Erwägungen hatte der TLfDI hinsichtlich des Verfassungsschutzberichts 2014/2015 in zwei Fällen Einwände gegen die Veröffentlichung dieser Namen, denen das Landesamt für Verfassungsschutz nachkam und von der Veröffentlichung der Namen dieser zwei Personen absah.
Für den Verfassungsschutzbericht 2016 konnte sich der TLfDI nach Abwägung der widerstreitenden Interessen damit einverstanden erklären, dass der Name einer Person erstmalig im Bericht genannt werden sollte.

Nach § 5 Abs. 2 Satz 3 Thüringer Verfassungsschutzgesetz (ThürVerfSchG) dürfen der Öffentlichkeit personenbezogene Daten nur bekannt gegeben werden, wenn das Interesse an der Unterrichtung das schutzwürdige Interesse des Betroffenen überwiegt. Abzuwägen dabei ist die Dienlichkeit der Darstellung für das Zusammenhangsverständnis und die Gewichtung der tatsächliche Anhaltspunkte für verfassungsfeindliche Bestrebungen mit den möglichen nachteiligen Auswirkungen, die die Veröffentlichung etwa in Verfassungsschutzberichten für die Betroffenen mit sich bringen kann. Der TLfDI macht sich dabei seine Aufgabe, nach § 5 Abs. 2 Satz 4 ThürVerfSchG eine Stellungnahme abzugeben, nicht leicht, fand aber mit dem Landesamt für Verfassungsschutz einvernehmliche Lösungen.

9.2 Kontrollen der Antiterrordatei beim Thüringer Landeskriminalamt und beim Amt für Verfassungsschutz

Gemäß § 1 Abs. 1 des Gesetzes zur Errichtung einer standardisierten zentralen Antiterrordatei von Polizeibehörden und Nachrichtendiensten von Bund und Ländern (Antiterrordateigesetz – ATDG) führen das Bundeskriminalamt sowie die Landeskriminalämter die Verfassungsschutzbehörden des Bundes und der Länder, der militärische Abschirmdienst, der Bundesnachrichtendienst und das Zollkriminalamt als beteiligte Behörden beim Bundeskriminalamt zur Erfüllung ihrer jeweiligen gesetzlichen Aufgaben zur Aufklärung oder Bekämpfung des internationalen Terrorismus mit Bezug zur Bundesrepublik Deutschland eine gemeinsame standardisierte zentrale Antiterrordatei.
In seinem Urteil vom 24. April 2013 (BVerfG – 1 BvR 1215/07) hatte das Bundesverfassungsgericht festgestellt, dass der Gewährleistung einer effektiven Kontrolle der Antiterrordatei eine große Bedeutung zukommen müsse und Änderungen des Datenbestandes vollständig protokolliert werden müssen (BVerfG, Urteil vom 24. April 2013, Rz. 214 f. der juris-Entscheidung). „Technische und organisatorische Maßnahmen“, so das BVerfG weiter, müssten sicherstellen, dass die Daten den Datenschutzbeauftragten in praktikabel auswertbarer Weise zur Verfügung stehen und die Protokollierung hinreichende Angaben für die Zuordnung zu dem zu kontrollierenden Vorgang enthält“ (BVerfG, Urteil vom 24. April 2013, Rz. 215 der juris-Entscheidung). Daher sieht § 10 Abs. 2 ATDG vor, dass die jeweils zuständigen Datenschutzbeauftragten des Bundes und der Länder verpflichtet sind, mindestens alle zwei Jahre die Einhaltung des Datenschutzes bei der ATD zu kontrollieren.
Deshalb kontrollierte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit im Berichtszeitraum hier sowohl die ATD beim Amt für Verfassungsschutz als auch beim Thüringer Landeskriminalamt (TLKA).
Im Fall der Kontrolle beim Landesamt für Verfassungsschutz stellte sich dabei zunächst die Schwierigkeit ein, dass nicht von vornherein für den TLfDI klar erkennbar war, warum welches Datum zu welchem Zeitpunkt verarbeitet worden war. Da das Amt für Verfassungsschutz aber die ATD nicht selbst führt, sondern dies vom Bun-

deskriminalamt besorgt wird, musste der TLfDI seine Fragen an diese Bundesbehörde weiterleiten.
Der TLfDI hat eine Vor-Ort-Kontrolle durchgeführt. Es bestand noch Rückfragebedarf. Dieser ist noch nicht abschließend bearbeitet.

Der TLfDI hat gem. § 10 Abs. 2 ATDG nun schon zum zweiten Mal die Antiterrordatei beim TLKA und Amt für Verfassungsschutz kontrolliert. Eine abschließende Bearbeitung bzw. Beurteilung war nicht möglich, da einige Fragen noch zu klären sind.



©fotomek – Euromünzemännchen – fotolia.com

10. Finanzwesen

10.1 Thüringer Verwaltung wird digital

Was beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) schon lange gelebte Praxis ist, soll nun auch für die übrigen Behörden des Freistaats Thüringen Wirklichkeit werden. Im November 2017 beschloss die Landesregierung den Entwurf eines E-Government-Gesetzes. Das Gesetz verfolgt zwei Ziele: zum einen sollen die Bürger die allermeisten Behördengänge online erledigen können. Zum anderen will das Land alle internen Verwaltungsvorgänge digitalisieren. Hierfür soll in Thüringen ein zentrales Datenmanagementsystem einführt werden. Das Kabinett bestätigte bereits im Jahr 2015 eine Grobkonzeption zur Einrichtung eines ressortübergreifenden einheitlichen Dokumentenmanagementsystems. Zur Umsetzung des Projekts wurde im Jahr 2016 ein Steuerungsgremium unter Federführung des Thüringer Finanzministeriums ins Leben gerufen, an dessen Sitzungen auch Vertreter des TLfDI teilnahmen. Im Steuerungsgremium sollten die

organisatorischen Rahmenbedingungen für die Einführung der elektronischen Akte (E-Akte) erarbeitet werden.
Die Beteiligung des TLfDI an dem Verfahren ist in zweierlei Hinsicht sachdienlich. Der TLfDI hat nach § 40 Abs. 5 Thüringer Datenschutzgesetz (ThürDSG) die Entwicklung und Nutzung der Informations- und Kommunikationstechnik, insbesondere der automatisierten Datenverarbeitung und ihrer Auswirkungen auf die Arbeitsweise und die Entscheidungsbefugnisse der öffentlichen Stellen zu beobachten. Außerdem kontrolliert der TLfDI bei allen öffentlichen Stellen die Einhaltung der Bestimmungen der Datenschutzgesetze, § 37 Abs. 1 ThürDSG. Durch eine frühzeitige Einbindung in das Verfahren ist sichergestellt, dass die gesetzlichen Vorgaben der Datenschutzgesetze eingehalten werden. Dies gilt für das geplante Verfahren umso mehr, als am 25. Mai 2018 die Datenschutz-Grundverordnung (DS-GVO) wirksam wird (siehe Punkt 3.1). Das Verfahren muss bereits im Vorfeld an den Vorgaben der DS-GVO ausgerichtet werden.
Nach Art. 35 DS-GVO muss der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durchführen, wenn bei der Verwendung neuer Technologien aufgrund der Art, des Umfangs, der Umstände und des Zwecks der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zu erwarten ist, so genannte Datenschutz-Folgenabschätzung. Nach einer ersten Einschätzung des TLfDI ist dies bei der Einführung eines Zentralen Dokumentenmanagementsystems für die Thüringer Landesverwaltung zumindest nicht von vornherein auszuschließen. Es muss daher durch die Verantwortlichen geprüft werden, ob die Voraussetzung des Art. 35 Abs. 1 DS-GVO vorliegen.
Die Art. 13 und 14 DS-GVO enthalten Anforderungen an die Informationspflicht gegenüber der betroffenen Person. Hierbei ist zu unterscheiden, ob die personenbezogenen Daten bei der betroffenen Person selbst erhoben werden (Art. 13 DS-GVO) bzw. ob sie nicht bei der betroffenen Person erhoben werden (Art. 14 DS-GVO). Es ist daher zu prüfen, nach welcher Bestimmung sich die Informationspflicht gegenüber dem Betroffenen richtet und im Folgenden sind der Inhalt und die Umsetzung der Informationspflicht zu festzulegen. Hierbei ist zudem zu berücksichtigen, dass das Land im neuen Thüringer Datenschutz weitere Regelungen zu Informationspflichten treffen kann.

Sollte das Land die Durchführung des Zentralen Dokumentenmanagementsystems mithilfe eines Auftragnehmers durchführen, bedarf es eines Vertrages zur Verarbeitung im Auftrag. Dabei ist zu beachten, dass nach Art. 28 f. DS-GVO den Auftragsverarbeiter wesentlich größere Pflichten treffen, als das nach der derzeit geltenden Regelung des § 8 ThürDSG der Fall ist. Das wird auch dadurch deutlich, dass der Auftragsverarbeiter genauso wie der Verantwortliche mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen arbeiten muss, Art. 31 DS-GVO.
Auch sind beim Abschluss eines derartigen Vertrages die Anforderungen des Art. 28 DS-GVO an die Gestaltung des Vertrages zu berücksichtigen. Nach Art. 30 DS-GVO muss jeder Verantwortliche ein Verzeichnis aller Verarbeitungstätigkeiten führen. Diese Pflicht trifft nach Absatz 2 auch den Auftragsverarbeiter. Die dort zu machenden Angaben entsprechen nicht eins zu eins den bisher im Verfahrensverzeichnis zu machenden Angaben. Nach Art. 32 DS-GVO sind sowohl der Verantwortliche als auch der Auftragsverarbeiter für die Sicherheit der Verarbeitung und die zu treffenden geeigneten technischen und organisatorischen Maßnahmen verantwortlich. Im Hinblick auf das Zentrale Dokumentenmanagementsystem ist daher zu prüfen, welchen Schutzbedarf die darin verarbeiteten Daten haben und welche Maßnahmen zu ihrem Schutz zu treffen sind.
Diese Vorgaben müssen in der Projektphase umgesetzt werden. Es ist außerdem darauf zu achten, dass nur diejenigen Stellen Zugriff auf personenbezogene Daten erhalten, die diese Daten auch für ihre Aufgabenerfüllung benötigen (Grundsatz der Erforderlichkeit). Einerseits soll es möglich sein, bestimmte Dokumente zwischen den Behörden auszutauschen, andererseits soll ein Zugriff aber nicht generell, sondern nur in begründeten Ausnahmefällen möglich sein. Hierfür sind die notwendigen technischen und organisatorischen Maßnahmen zu treffen. Für die Klärung all dieser Fragen steht der TLfDI dem Steuerungsgremium beratend zur Seite.
Außerdem wurde beim TLfDI bereits im Dezember 2010 die vollelektronische E-Akte eingeführt. Lediglich die Ordnungswidrigkeitenverfahren werden noch mit Papierakten geführt. Aufgrund dessen hat der TLfDI einen reichen Erfahrungsschatz im Umgang mit der E-Akte, an dem er das Steuerungsgremium teilhaben lässt.
Das Verfahren befindet sich derzeit in der ersten Planungsphase. Es wird den TLfDI über einen längeren Zeitraum beschäftigen und sicherlich auch Gegenstand des nächsten Tätigkeitsberichts sein.

Die digitale Entwicklung macht auch vor der Thüringer Verwaltung nicht halt. Mit dem geplanten E-Government-Gesetz soll die E-Akte für alle Thüringer Behörden verpflichtend eingeführt werden. Hierbei handelt es sich um ein Verfahren, das auch Risiken für die Rechte und Pflichten der betroffenen Personen mit sich bringt. Der TLfDI wird das Verfahren begleiten und den dafür eingerichteten Steuerungsgremium beratend zur Seite stehen.



paragraph_regen – © fotomek/ Fotolia.com

11. Justiz

11.1 „Moha“: Nur Essensgewohnheit oder doch ein Rückschluss auf das Glaubensbekenntnis

Dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) ist im Berichtszeitraum bekannt geworden, dass sich an den Haftraumtüren der Justizvollzugsanstalt

(JVA) Hohenleuben mitunter Angaben zur Anstaltskost befinden, die Rückschlüsse auf das Glaubensbekenntnis (jüdisch/muslimisch etc.) zulassen. Diese Daten gelten gem. § 4 Abs. 5 Thüringer Datenschutzgesetz (ThürDSG) als besonders geschützte personenbezogene Daten. Daneben normiert § 132 Thüringer Justizvollzugsgesetzbuch (ThürJVollzGB), dass mit Ausnahme des religiösen oder weltanschaulichen Bekenntnisses und der Daten von Gefangenen, die anlässlich ärztlicher Untersuchungen erhoben worden sind, Daten von Gefangenen in der Anstalt allgemein kenntlich gemacht werden dürfen, soweit dies für ein geordnetes Zusammenleben erforderlich ist.

Auf Nachfrage des TLfDI teilte die JVA Hohenleuben mit, dass sich in der JVA an den Haftraumtüren Schilder befänden. Dort seien die Namen, die Arbeitsstelle sowie auch die Kostform der dort untergebrachten Gefangenen angegeben. Die Hafträume seien hauptsächlich mit mehreren (bis zu sechs) Gefangenen belegt. Die Gefangenen erhielten grundsätzlich ihre Verpflegung in dem Haftraum. Eine Einnahme der Mahlzeiten in einem zentralen Speisesaal finde nicht statt. Die verschiedenen Kostformen seien grundsätzlich wie folgt in abgekürzter Form auf den Namensschildern dargestellt: „NK“ für Normalkost, „Vegi“ für vegetarische Kost und „Moha“ für Schweinefleischaustausch.

Auf Nachfrage des TLfDI räumte die JVA Hohenleuben ein, dass die Bezeichnung der Schweinefleisch-Austauschkost als ,,Moha“-Kost durchaus einen Rückschluss darauf zulässt, dass der jeweilige Gefangene, der diese Kost in Anspruch nimmt, den islamischen Glauben praktiziert. Eine direkte Verbindung zwischen dieser Kostform und einem muslimischen Glaubensbekenntnis bestehe tatsächlich jedoch nicht, denn auch konfessionslose Gefangene bzw. Gefangene, die sich zu einer anderen Religion bekennen, erhielten auf Antrag ebenfalls diese Austauschkost. Die Anstaltsküche tausche bei dieser Kostform nur Schweinefleischprodukte aus, aber bereite die Speisen nicht, wie eventuell vermutet, nach den religiösen Vorschriften des Koran (Halal) zu.

Der TLfDI teilte der JVA Hohenleuben schließlich mit, dass es keinen ersichtlichen Grund dafür gibt, weshalb die Kostform Schweinefleisch-Austausch als „Moha“ gekennzeichnet sein muss. Gerade bei dieser Abkürzung drängt sich ein Bezug zum muslimischen Glauben auf. Daher wurde seitens des TLfDI vorgeschlagen, künftig auf die Abkürzung „Moha“ zu verzichten und stattdessen beispielsweise

„SE“ für Schweinefleischersatz oder eine ähnliche Abkürzung zu verwenden.
Die JVA Hohenleuben stimmte dem Vorschlag des TLfDI zu und verwendet nunmehr die Abkürzung „SE“ für Schweinefleischersatz.

Gemäß § 4 Abs. 5 Thüringer Datenschutzgesetz (ThürDSG) ist das Verarbeiten oder Nutzen von personenbezogenen Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie von Daten über Gesundheit oder Sexualleben (besonders geschützte Daten) nur zulässig, wenn
1. eine Rechtsvorschrift dies ausdrücklich vorsieht oder zwingend voraussetzt,
2. die Betroffenen eingewilligt haben, wobei sich die Einwilligung ausdrücklich auf diese Daten beziehen muss,
3. es zum Schutz lebenswichtiger Interessen Betroffener oder Dritter erforderlich ist, sofern die Betroffenen aus physischen oder rechtlichen Gründen außerstande sind, ihre Einwilligung zu geben,
4. es sich um Daten handelt, die Betroffene offenkundig öffentlich gemacht haben,
5. es zur Abwehr erheblicher Nachteile für das Gemeinwohl oder von Gefahren für die öffentliche Sicherheit und Ordnung erforderlich ist,
6. es zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an dem Abschluss des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann,
7. es erforderlich ist, um den Rechten und Pflichten der öffentlichen Stellen auf dem Gebiet des Dienst- und Arbeitsrechts Rechnung zu tragen, oder
8. es zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich ist und die Verarbeitung dieser Daten durch ärztliches Personal oder durch sonstige Personen erfolgt, die einer entsprechenden Geheimhaltungspflicht unterliegen.
All diese Gründe lagen bei der Bekanntgabe der Kostform an den Haftraumtüren der JVA Hohenleuben nicht vor.

11.2 Datenschutzrechtliche Belange gelten auch für Bescheide der Staatsanwaltschaft

Ein Bürger zeigte seiner Ansicht nach vorliegende Straftaten bei der Staatsanwaltschaft an. Die Staatsanwaltschaft war der Ansicht, dass seine Vorwürfe gegen einen bestimmten Beschuldigten keinen Anfangsverdacht für die Einleitung eines Ermittlungsverfahrens begründeten. Die Ablehnung der Einleitung eines Ermittlungsverfahrens begründete dies ausführlich. Allerdings so ausführlich, dass so dem Bürger viele Details über den Betroffenen mitgeteilt wurden, dass sich Letzterer nunmehr in seinem Recht auf informationelle Selbstbestimmung verletzt sah.

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) vertrat in diesem Spannungsverhältnis zwischen dem Recht eines Anzeigenerstatters auf nachvollziehbare Begründung der Ablehnung seines Antrags und dem Recht des Beschuldigten auf Geheimhaltung persönlicher Daten folgende Rechtsauffassung:

Die Staatsanwaltschaft hat nach § 171 Strafprozessordnung (StPO), wenn sie einem Antrag auf Erhebung der öffentlichen Klage keine Folge leistet oder sie nach dem Abschluss der Ermittlungen verfügt, das Verfahren einzustellen, den Antragsteller unter Angabe der Gründe zu bescheiden. Wie weit diese Begründung zu gehen hat, ist in der StPO nicht geregelt. Da § 171 StPO keine spezialgesetzliche Ermächtigungsnorm zur Erhebung und Weiterleitung von Daten darstellt, ist eine Verdrängung der allgemeinen datenschutzrechtlichen Bestimmungen nicht gegeben.

Damit ist die Datenübermittlung an den Anzeigenerstatter eine Aufgabenerfüllung durch die Staatsanwaltschaft in Anwendung der Strafprozessordnung und damit nach § 22 Abs. 1 Nr. 1 in Verbindung mit § 20 Abs. 2 Nr. 7 Thüringer Datenschutzgesetz (ThürDSG) grundsätzlich zulässig, wobei allerdings das Tatbestandsmerkmal der „Erforderlichkeit“ in § 20 ThürDSG zu beachten ist.

Die Bescheidung des Anzeigenerstatters unter Angabe der relevanten Gründe muss nicht im Gegensatz zu den datenschutzrechtlichen Belangen stehen.

Die Begründung des Bescheids muss in einer dem Antragsteller verständlichen Weise die tatsächlichen und rechtlichen Gründe angeben, auf denen der Bescheid beruht.

Hier ist beim Abfassen der Begründung vom Verfasser unter Berücksichtigung des Datenschutzes auch ein Augenmerk darauf zu legen, dass persönliche Angaben über weitere Beteiligte nicht notwendigerweise immer in die Begründung einfließen müssen. Im Rahmen dieser Abwägung sollte immer geprüft werden, ob es möglich ist, die detaillierten Angaben z. B. zu den einzelnen im Ermittlungsverfahren verfolgten Handlungen der Beteiligten oder die detailreiche Schilderung der einzelnen Handlungsverläufe im Ergebnis zusammenzufassen.
Ergänzend dazu sei noch auf Nr. 89 Abs. 2 der Richtlinien für das Strafverfahren und das Bußgeldverfahren (RiStBV) hingewiesen, aus der sich ergibt, dass die Begründung der Einstellungsverfügung sich zwar nicht auf allgemeine und nichtssagende Redewendungen, z. B. „da eine Straftat nicht vorliegt oder nicht nachgewiesen ist“, beschränken darf, sondern es soll in der Regel angegeben werden, aus welchen Gründen der Verdacht einer Straftat nicht ausreichend erscheint oder weshalb sich sonst die Anklageerhebung verbietet. Die Vorschrift besagt aber eindeutig, dass es genügt, die Gründe anzuführen, die ein Eingehen auf Einzelheiten unnötig machen, z. B., dass die angezeigte Handlung unter kein Strafgesetz fällt, dass die Strafverfolgung verjährt oder aus anderen Gründen unzulässig ist oder dass kein öffentliches Interesse an der Strafverfolgung besteht.

Im konkreten Fall war die Datenübermittlung durch die Staatsanwaltschaft geschehen und konnte nicht mehr rückgängig gemacht werden. Die Staatsanwaltschaft wurde aber für künftige Fälle gebeten, das Gebot der Erforderlichkeit zu beachten.
Die Einleitung eines Ermittlungsverfahrens darf gegenüber dem Anzeigenerstatter nicht so ausführlich begründet werden, dass dieser persönliche Daten über den Beschuldigten erfährt.

11.3 Insolvent – und alle wissen es

Ausgangspunkt in diesem Fall war ein Schreiben, welches nachrichtlich auch an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und den damaligen Thüringer Justizminister gerichtet war. Darin teilte der Bundesminister der Justiz und für Verbraucherschutz mit, dass ihn die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) darauf aufmerksam gemacht hätte, dass einige Unternehmen Informationen

aus den im Internet erfolgenden öffentlichen Bekanntmachungen in Insolvenzverfahren unter Verstoß gegen den Datenschutz missbräuchlich nutzen würden. Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) habe angeregt, solchen Verstößen gegen den Datenschutz damit zu begegnen, dass der Zugriff auf die im Insolvenzregister veröffentlichten Daten für eine solche missbräuchliche Nutzung erschwert werden solle (z. B. durch technische Vorkehrungen).

Das Insolvenzportal wird unter Federführung der Landesjustizverwaltung Nordrhein-Westfalens (NRW) als ein Modul des Gemeinsamen Justizportals des Bundes und der Länder unter https://www.justiz.de betrieben.

Der TLfDI forderte das Thüringer Ministerium für Migration, Justiz und Verbraucherschutz (TMMJV) zur Stellungnahme auf, ob und wenn ja welche Art von Vorkehrungen bzw. Schutzmaßnahmen bis dato ergriffen wurden, die einen missbräuchlichen Zugriff auf die im Insolvenzregister veröffentlichten Daten verhindern bzw. erschweren.

Als Rechtsgrundlage für die öffentliche Bekanntmachung insolvenzrechtlicher Entscheidungen seitens der Insolvenzgerichte benannte das TMMJV § 9 Abs. 1 Satz 1 i. V. m. Abs. 2 Satz 2 und 3 Insolvenzordnung (InsO). Die technische und inhaltliche Ausgestaltung sowie Vorschriften zu den Löschungsfristen für die Insolvenzgerichte sind in der Verordnung zu öffentlichen Bekanntmachungen in Insolvenzverfahren im Internet (InsOBekV) geregelt. Soweit die Insolvenzordnung die öffentlichen Bekanntmachungen bestimmter Entscheidungen ausdrücklich anordnet, werden diese von den zuständigen Insolvenzgerichten auf der Internetplattform https://www.Insolvenzbekanntmachungen.de eingestellt und sind damit für jedermann abrufbar, ohne dass ein besonderes Interesse an der Einsichtnahme dargelegt werden muss. Die veröffentlichungspflichtigen Entscheidungen (z. B. Anordnungen und Aufhebungen von Sicherungsmaßnahmen, Entscheidung über die Erteilung oder Ver-

sagung der Restschuldbefreiung) sind gemäß § 3 Abs. 1 und Abs. 2 InsOBekV spätestens nach sechs Monaten zu löschen.
Das TMMJV teilte dem TLfDI mit, dass bereits adäquate Schutzmaßnahmen ergriffen worden seien. Unmittelbar nach Bekanntwerden von möglichen Versäumnissen bei der Löschung von Daten aus Insolvenzverfahren am 26. Februar 2014 hätte die Landesjustizverwaltung Nordrhein-Westfalen die Länder unverzüglich unterrichtet und um Überprüfung der Angelegenheit gebeten. Mit Erlass vom 27. Februar 2014 habe das TMMJV die Thüringer Insolvenzgerichte auf das zwingende Erfordernis der Löschung von Bekanntmachungen hingewiesen, deren Eintragungen noch abgerufen werden können, obwohl die jeweiligen Veröffentlichungen aufgrund des Ablaufs der Löschungsfristen bereits hätten gelöscht werden müssen. Ferner habe das TMMJV um Vollzug der Löschungen gebeten
Bereits im Jahr 2015 sei die Löschung der Verfahren in Thüringen weitestgehend abgeschlossen gewesen. Um künftig derartigen Konstellationen vorzubeugen, wurde länderübergreifend durch die Bund-Länder-Kommission für Informationstechnik in der Justiz (BLK) eine Prüfbitte an das Bundesministerium der Justiz und für Verbraucherschutz (BMJV) herangetragen, ob eine Änderung der entsprechenden Bundesvorschriften zum Löschen angezeigt ist.
Parallel hierzu wurden die IT-Löschroutinen innerhalb des Gemeinsamen Justizportals des Bundes und der Länder im Hinblick auf die aktuelle Thematik überarbeitet.
Eine weitere Nachfrage des TLfDI beim TMMJV im Berichtszeitraum ergab, dass die BLK durch die federführende Landesjustizverwaltung Nordrhein-Westfalen den für das bundesweite Insolvenzportal zuständigen Landesdienstleister IT.NRW mit der Durchführung der Arbeiten nach Maßgabe des aktuellen Feinkonzepts betraut habe. Hierbei orientieren sich die rechtlichen Anforderungen sowie die notwendigen technischen Anpassungen im Wesentlichen an der Vernetzung der europäischen Insolvenzregister gemäß Verordnung (EU) 201 51848 sowie den datenschutzkonformen Vorgaben gegen etwaige missbräuchliche Nutzung.
Anfang des Jahres 2017 teilte das TMMJV dem TLfDI mit, dass die Löschung der Insolvenzverfahren abgeschlossen wurde.

Die Insolvenzveröffentlichungen selbst veranlassen die jeweiligen Insolvenzgerichte der Länder in eigener Zuständigkeit und in eigener Verantwortung, denn nur sie können die korrekten Veröffentli-

chungsfristen anhand der Aktenlage ermitteln und überwachen. Die Veröffentlichungen sowie die Überwachung der Löschungsfristen erfolgen gemäß der Insolvenzordnung (InsO), u. a. § 9 lnsO, bzw. der Verordnung zu öffentlichen Bekanntmachungen in Insolvenzverfahren im Internet und sind somit originäre Aufgaben der jeweiligen Gerichte.

11.4 Sichere Telearbeitsplätze für Richter und Staatsanwälte

Seit 2006 gibt es in Thüringen eine Verordnung zum elektronischen Rechtsverkehr für Gerichte und Staatsanwaltschaften, zuletzt geändert am 14. August 2017 (GVBl.II/17, [Nr. 44]). Ziel war die Einführung der elektronischen Akte (eAkte). Im Dezember 2016 wandte sich das Thüringer Ministerium für Migration, Justiz und Verbraucherschutz (TMMJV) an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) im Rahmen seines Projektes „eJustice Thüringen“, welches zum Ziel hat, die elektronische Akte (eAkte) in der Thüringer Justiz einzuführen. Die Unabhängigkeit der Richter und deren zeitgemäße Arbeitsmodelle machten es zunehmend notwendig, technische Möglichkeiten für eine administrationsarme Bereitstellung von Heimarbeitsplätzen und mobilen Arbeitsplätzen für den sicheren Zugriff auf elektronische Akten zu prüfen.

So wurde der TLfDI gebeten, eine technische Lösung des ECOS Secure Boot Sticks, wie sie bereits in einem Pilotprojekt im Hessischen Ministerium der Justiz, für Integration und Europa Anwendung findet, hinsichtlich einer generellen Eignung zu prüfen.

Die Lösung basiert auf der Idee, per USB-Stick ein besonders gesichertes Linux-System zu starten, welches dann an jedem beliebigen Rechner unabhängig vom eigentlich installierten Betriebssystem eingesetzt werden kann.

Mit der zu prüfenden Lösung muss somit dem Rechner erlaubt werden, ein Betriebssystem von einem USB-Stick zu starten. Dies stellt ein Sicherheitsrisiko dar, da Rechner immer so konfiguriert werden sollten, dass weder von einer CD noch von einem USB-Stick ein Betriebssystem gestartet werden kann. Mit der Möglichkeit, per CD oder USB-Stick ein Betriebssystem neben dem eigentlichen Betriebssystem starten zu können ist somit ein Vollzugriff auf die gespeicherten Daten auf der Festplatte des Rechners ausführbar. Da es

vor allen Dingen Privatrechner betrifft, wäre zudem somit der Zugriff auf alle privat gespeicherten Daten des PCs möglich.
Weiterhin muss die eingesetzte Software den Sicherheits-Richtlinien der Thüringer Landesverwaltung genügen. So empfahl der TLfDI, vor Einführung der Lösung auch das zuständige Thüringer Finanzministerium, welches für die IT-Sicherheit des Landesverwaltungsnetzes zuständig ist, vorab zu kontaktieren.

Telearbeitsplätze in der Thüringer Landesverwaltung sind grundsätzlich so zu gestalten, dass nur dienstliche Geräte zum Einsatz kommen. Kann dem nicht Rechnung getragen werden, darf keinesfalls durch dienstliche Interessen der private PC einem zusätzlichen Sicherheitsrisiko ausgesetzt werden. Zudem ist bei jeder Lösung vorab das zuständige Ministerium für die IT-Sicherheit der Thüringer Landesverwaltung zu kontaktieren.

11.5 Akteneinsicht bei der Staatsanwaltschaft – aber nur mit Rücksicht auf die schutzwürdigen Interessen der Beschuldigten

Im Berichtszeitraum beschwerte sich ein Bürger beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) darüber, dass die Staatsanwaltschaft Mühlhausen im Rahmen eines Ermittlungsverfahrens dem gegnerischen Anwalt Einsicht in Kopien privater PC-Datenträger gewähren wollte. Die Kopien wurden im Rahmen einer Hausdurchsuchung beim Beschwerdeführer von der Staatsanwaltschaft Mühlhausen gefertigt. Die Staatsanwaltschaft Mühlhausen schrieb dem Beschwerdeführer hierzu lediglich, dass „davon ausgegangen wird, dass es keine Vorbehalte gegen die Einsichtnahme in die Asservate gibt“. Eine Einwilligung habe der Betroffene und Beschwerdeführer aber nicht erteilt.
Gemäß § 4 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) ist die Verarbeitung und Nutzung personenbezogener Daten nur zulässig, wenn dieses Gesetz oder eine andere Rechtsvorschrift sie erlaubt oder anordnet oder soweit der Betroffene eingewilligt hat. Die Verarbeitung umfasst auch das Übermitteln personenbezogener Daten (§ 3 Nr. 4 ThürDSG). An die Einwilligungserklärung hat der Gesetzgeber besondere Voraussetzungen geknüpft (vgl. § 4 Abs. 3 ThürDSG). Ein angenommenes Einverständnis, wie es die Staatsanwaltschaft Mühlhausen in ihrem Schreiben beschrieb, reicht indessen

nicht aus. Dadurch wäre die Datenerhebung mangels Einwilligung rechtswidrig.
In einer Stellungnahme gegenüber dem TLfDI erklärte die Staatsanwaltschaft Mühlhausen, dass Rechtsgrundlage für eine Akteneinsicht § 406e Abs. 1 Strafprozessordnung (StPO) sei. Danach kann ein Rechtsanwalt für den Verletzten die Akten, die dem Gericht vorliegen oder diesem im Falle der Erhebung der öffentlichen Klage vorzulegen wären, einsehen sowie amtlich verwahrte Beweisstücke besichtigen, soweit er hierfür ein berechtigtes Interesse darlegt.
Begrenzt wird dieses Verletzteninteresse allerdings unter anderem durch entgegenstehende schutzwürdige Interessen des Beschuldigten gemäß § 406e Abs. 2 Satz 1 StPO. Zu den schutzwürdigen Interessen des Beschuldigten zählt auch sein Interesse an der Geheimhaltung persönlicher Daten. Insoweit muss eine Abwägung der gegenläufigen Interessen von Beschuldigten und von Verletzten vorgenommen werden.
Die Staatsanwaltschaft Mühlhausen teilte dem TLfDI mit, dass im Rahmen einer Durchsuchung eine Sicherstellung von Daten auf behördeneigenen Datenträgern erfolgt sei (§ 94 StPO). Bei dieser Übertragung von Daten konnte aber nicht ausgeschlossen werden, dass eine Vielzahl von verfahrensunerheblichen Daten erfasst werden und auch andere Personen und Vorkommnisse in den Wirkungsbereich der Maßnahme miteinbezogen werden, die mit dem zu ermittelnden Sachverhalt nichts zu tun haben. Ebenso konnte nicht ausgeschlossen werden, dass Bilder oder Daten sichergestellt wurden, die den Kernbereich der privaten Lebensgestaltung betreffen.
Um dieses auszuschließen, wurde seitens der Ermittlungsbehörden eine Überprüfung der sichergestellten Daten nach ihrer Verfahrenserheblichkeit vorgenommen. Dieses erfolgte zum einen dadurch, dass anhand einer Stichwortsuche die verfahrensrelevanten Daten ermittelt wurden. Auf der anderen Seite wurde mit den vorhandenen technischen Möglichkeiten versucht, alle Daten, die den Bereich der privaten Lebensgestaltung betreffen, herauszufiltern. Nach der Eingabe des TLfDI wurde indessen eine nochmalige Überprüfung nach den zuvor genannten Kriterien vorgenommen.
Diese so reduzierten Daten wurden auf neue Datenträger übertragen. Ausschließlich mit diesen neuen Datenträgern arbeiteten dann die Ermittlungsorgane. Diese neuen Datenträger standen dann im konkreten Fall auch nur für eine Akteneinsicht zur Verfügung.

Aus datenschutzrechtlicher Sicht entsprach das Handeln der Staatsanwaltschaft Mühlhausen daher den gesetzlichen Vorschriften und war deshalb nicht zu beanstanden.

Die Rechtsgrundlage für eine Akteneinsicht im Rahmen eines staatsanwaltschaftlichen Ermittlungsverfahrens bildet § 406e Abs. 1 StPO. Etwaige schutzwürdige Interessen der Betroffenen, wie z. B. die Geheimhaltung persönlicher Daten, sind gem. § 406e Abs. 2 Satz 1 StPO gegen die Interessen der Verletzten abzuwägen. Seitens der Staatsanwaltschaft ergeht in diesem Zusammenhang auch immer der Hinweis an den Betroffenen, dass gegen die staatsanwaltschaftliche Entscheidung eine gerichtliche Entscheidung innerhalb von zwei Wochen beantragt werden kann (§ 406e Abs. 4 Satz 2 StPO).

11.6 Datenlöschung aus dem Zentralen Staatsanwaltlichen Verfahrensregister: Fehlanzeige

Ein Bürger wandte sich im Berichtszeitraum an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), weil er sich in seinem Recht auf informationelle Selbstbestimmung beeinträchtigt sah. Grund dafür waren diverse Datenlöschungen aus dem Zentralen Staatsanwaltschaftlichen Verfahrensregister (ZStV), mit denen sich auch bereits die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) befasst hatte.
Der Bürger hatte einen ZStV-Auszug beantragt und erhalten. Die BfDI hatte bei einem Abgleich dieser beiden Auszüge bereits festgestellt, dass kein neuer Eintrag hinzugekommen sei, der eine Hinausschiebung des Löschtermins begründen würde. Zudem konnte festgestellt werden, dass zu ein und demselben Verfahren in einem ZStV-Auszug ein anderes Einstellungsdatum vermerkt war, als in einem anderen Auszug. Eine Nachfrage der BfDI beim Bundesamt für Justiz, welches das ZStV führt, bezgl. der unterschiedlichen Einstellungsdaten ergab, dass die für das jeweilige Ermittlungsverfahren zuständige Staatsanwaltschaft entsprechend § 494 Abs. 2 Satz 4 Strafprozessordnung (StPO) der Registerbehörde den Eintritt der Löschungsvoraussetzungen oder den Beginn der Löschfrist mitteilt und gemäß § 494 Abs. 1 Satz 2 Halbsatz 2 StPO als zuständige Stelle die Verantwortung für die Richtigkeit und die Aktualität der Daten im ZStV trägt.

Dem Bürger wurde durch die BfDI mitgeteilt, dass „solange kein – wie auch immer gearteter – Verfahrensabschluss an das Register gemeldet worden ist, auch keine Löschung durch die registerführende Behörde erfolgen kann. Der Fehler liegt dabei aber nicht bei dem ZStV, sondern bei der (nicht) meldenden Staatsanwaltschaft bzw. dem Gericht, von denen bisher offensichtlich noch keine Meldung über einen eventuellen Verfahrensabschluss erfolgt ist."
Gemäß § 494 Abs. 2 Satz 2 StPO sind die in dem ZStV gespeicherten Daten grundsätzlich zwei Jahre nach der Erledigung des Verfahren zu löschen. Vor diesem Hintergrund begehrte der Bürger die Löschung bzw. die hierfür notwendige Meldung durch die zuständige Staatsanwaltschaft an das ZStV.
Da der TLfDI für die Kontrolle der Einhaltung datenschutzrechtlicher Vorschriften bei den Thüringer Staatsanwaltschaften zuständig ist, bat er die zuständige Staatsanwaltschaft um eingehende Stellungnahme, insbesondere zu der Frage, weshalb zu ein und demselben Verfahren unterschiedliche Einstellungsdaten an das ZStV gemeldet worden seien.
Die Staatsanwaltschaft teilte dem TLfDI mit, dass die Mitteilung über die Erledigung der Verfahren an das Bundeszentralregister erfolgte. Aus welchem Grund die Löschungen nicht fristgemäß erfolgt seien, ließe sich leider computertechnisch nicht mehr klären. Die Löschung der Verfahren wurde daher erneut veranlasst, sodass im Zentralen Staatsanwaltschaftlichen Verfahrensregister gegen den Bürger keine Verfahren der Staatsanwaltschaft mehr eingetragen blieben.
Der TLfDI konnte damit den Vorgang im Interesse des Bürgers abschließen.

Das Bundesamt für Justiz führt das Zentrale Staatsanwaltschaftliche Verfahrensregister (ZStV). Die für das jeweilige Ermittlungsverfahren zuständige Staatsanwaltschaft teilt nach § 494 Abs. 2 Satz 4 Strafprozessordnung (StPO) der Registerbehörde den Eintritt der Löschungsvoraussetzungen oder den Beginn der Löschfrist mit. Im vorliegenden Fall war es zu computertechnischen Fehlern gekommen, die durch Intervention des TLfDI beseitigt werden konnten.

11.7 Ein behördlicher Datenschutzbeauftragter für das Amtsgericht?

Im Februar 2017 erreichte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) die Anfrage eines Amtsgerichts. Hintergrund war die Frage, ob sich allein durch die Nutzung des Anwenderprogrammes HAMASYS durch die Bediensteten des Amtsgerichts die Pflicht zur Bestellung eines behördlichen Datenschutzbeauftragten ergebe.
§ 2 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) stellt klar, dass der Anwendungsbereich des ThürDSG sich auch auf Gerichte erstreckt. Ausnahmen hierzu regelt § 2 Abs. 6 ThürDSG. Hiernach gelten der § 10 (Verfahrensverzeichnis) und der § 11 (Anrufung des Landesbeauftragten für den Datenschutz) sowie der fünfte Abschnitt (Überwachung des Datenschutzes bei öffentlichen Stellen) nur, soweit die Gerichte in Verwaltungsangelegenheiten tätig werden.
Verwaltungstätigkeiten liegen dann vor, wenn die Gerichte Aufgaben erfüllen, die nicht im unmittelbaren oder mittelbaren sachlichen oder organisatorischen Zusammenhang mit der Rechtsprechung oder sonstigen Formen der individuellen Rechtspflege stehen (so Abel/Müller-Grune, Kommentar zum ThürDSG, § 2 Nr. 3). Verwaltungsaufgaben betreffen z. B. Angelegenheiten der Gebäudeverwaltung, der Personalverwaltung, die Beschaffung von Sachmitteln, die Ausübung der Dienstaufsicht oder die Verwaltung der Akten über abgeschlossene Verfahren.
Nach § 10a Abs. 1 S. 1 ThürDSG haben Daten verarbeitende Stellen, die personenbezogene Daten mithilfe automatisierter Verfahren verarbeiten oder nutzen, einen ihrer Beschäftigten zum Beauftragten für den Datenschutz schriftlich zu bestellen. Einer Bestellung eines Beauftragten für den Datenschutz bedarf es nicht, wenn in der Daten verarbeitenden Stelle ausschließlich Verfahren der in § 34 Abs. 3 ThürDSG genannten Art eingesetzt werden. Dabei handelt es sich um solche automatisierte Verfahren, die z. B. dem internen Verwaltungsablauf dienen wie Registraturverfahren.
HAMASYS ist ein Haushaltsmanagementsystem Das System unterstützt die Haushaltsplanung und -aufstellung, die Mittelverteilung und -bewirtschaftung sowie das Kassenwesen. Insoweit dient es dem internen Verwaltungsablauf und unterfällt damit § 34 Abs. 3 Nr. 1 ThürDSG, wonach allein durch die Nutzung dieses Programmes kein behördlicher Datenschutzbeauftragter zu bestellen wäre.

Die Bestellung eines Datenschutzbeauftragten empfiehlt sich jedoch auch unabhängig davon. Neben der Mitwirkung bei Freigaben automatisierter Verfahren, der Führung des Verfahrensverzeichnisses nach § 10 ThürDSG sowie der Überwachung der ordnungsgemäßen Anwendung von Datenverarbeitungsprogrammen berät der Datenschutzbeauftragte die bei der Verarbeitung oder Nutzung personenbezogener Daten tätigen Personen zu den Bestimmungen des ThürDSG sowie anderer Vorschriften über den Datenschutz (§ 10a Abs. 2 S. 3 ThürDSG). Zudem agiert er als Multiplikator für den Datenschutz und kann als Bindeglied zwischen dem TLfDI und der Behörde tätig werden. Mitunter ist der behördliche Datenschutzbeauftragte erster Ansprechpartner des TLfDI zu datenschutzrechtlichen Problematiken innerhalb der jeweiligen Behörde.

Die Pflicht zur Bestellung eines Beauftragten für den Datenschutz bei öffentlichen Stellen ergibt sich aus § 10a Abs. 1 ThürDSG. Einer Bestellung bedarf es nicht, wenn in der Daten verarbeitenden Stelle ausschließlich Verfahren der in § 34 Abs. 3 ThürDSG genannten Art eingesetzt werden. Unabhängig davon wird vom TLfDI die Bestellung eines Datenschutzbeauftragten – aufgrund seines vielseitigen Aufgabenspektrums – empfohlen.

11.8 Richterliche Unabhängigkeit für TLfDI unantastbar

Der Beklagte in einem Zivilgerichtsverfahren wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Im Wesentlichen beklagte er sich darüber, dass das Prozessgericht dem Kläger Schriftsätze von ihm übersandte, obwohl er dessen ordnungsgemäße Prozessvollmacht bezweifelte, die Klage für unzulässig hielt und somit meinte, dass Daten von ihm unzulässig übermittelt wurden.
Der TLfDI durfte hier nicht tätig werden, da die Prozessführung wie auch die Entscheidung selbst in einem gerichtlichen Verfahren in den von der Verfassung garantierten Bereich der richterlichen Unabhängigkeit fallen. Solche gerichtlichen Maßnahmen/Entscheidungen können nur mit den dafür vorgesehenen Rechtsbehelfen angegriffen werden. Das heißt, nur eine andere gerichtliche Instanz kann eine richterliche Entscheidung aufheben.
Dieses verfassungsrechtliche Prinzip der Gewaltenteilung findet seinen Ausdruck in § 2 Abs. 6 Thüringer Datenschutzgesetz.

Keine Zuständigkeit des TLfDI, wenn die richterliche Unabhängigkeit betroffen ist.

11.9 Personalakte: Übermittlungsersuchen eines Gerichts

Im vergangenen Jahr war dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) bekannt geworden, dass in einem Verwaltungsrechtsstreit gegen den Freistaat Thüringen über die Beförderung von Landes- und Kirchenbeamten ein Verwaltungsgericht die Landesfinanzdirektion (LFD) aufgefordert hatte, vollständige Verfahrensakten einschließlich Personalvorgängen zu übersenden. Daraufhin übersandte die LFD dem Gericht 35 Personalakten von Bediensteten der Thüringer Finanzämter, die sich jeweils aus vier bis acht Bänden zusammensetzten. Im Weiteren bestand nunmehr auch die Einsichtsmöglichkeit aller anwaltlich vertretenen Verfahrensbeteiligten in die Personalakten ihrer Konkurrenten.

Durch den TLfDI wurde nicht infrage gestellt, ob das Gericht die Personalunterlagen der Beteiligten benötigt. Dies war zweifelslos der Fall, sicherlich aber nicht alle Personalunterlagen, die in der Personalakte abgeheftet waren.

Nach § 99 Verwaltungsgerichtsordnung (VwGO) sind die erforderlichen Unterlagen vorzulegen. In Konkurrentenstreitigkeiten sind dies auch die Personalunterlagen des Antragstellers und der Beigeladenen / Konkurrenten, die u. a. Grundlage für die Auswahlentscheidung waren. Personalaktendaten sind in § 50 BeamtStG definiert. Die Personalakte eines Betroffenen besteht aus der Grundakte sowie aus Teilakten, Nebenakten und automatisiert geführten Dateien. Maßgeblich entscheidungsrelevant dürften die Nachweise der Qualifikation (Grundakte, Ausbildung und Fortbildung) sowie die Beurteilungen sein.

Das Gericht hat hier die vollständigen Verfahrensakten angefordert. Damit trägt das Gericht nach § 21 Abs. 2 Satz 2 Thüringer Datenschutzgesetz (ThürDSG) die datenschutzrechtliche Verantwortung. In diesen Fällen prüft die übermittelnde Stelle (d. h. die LFD) nur, ob das Übermittlungsersuchen im Rahmen der Aufgaben des Dritten liegt, es sei denn, dass besonderer Anlass zur Prüfung der Zulässigkeit der Übermittlung besteht (§ 21 Abs. 2 Satz 3 ThürDSG).

Auch wenn dies für die Betroffenen sehr unbefriedigend sein mag, hatte der TLfDI aufgrund seiner Unzuständigkeit gemäß § 2 Abs. 6 ThürDSG in diesem Falle keinen Handlungsspielraum. Daher wurde das Thüringer Ministerium für Migration, Justiz und Verbraucherschutz (TMMJV), vor dem Hintergrund der Wahrung von Persönlichkeitsrechten der Betroffenen, darum gebeten, die Gerichte im Rahmen ihrer Zuständigkeit auf den Sachverhalt sowie die Erforderlichkeit der Beiziehung umfangreicher Personalunterlagen hinzuweisen.
Das TMMJV teilte mit, dass der Hinweis des TLfDI an den Präsidenten des Thüringer Oberverwaltungsgerichts weitergeleitet und dieser gebeten wurde, seinen Geschäftsbereich entsprechend zu sensibilisieren.

Nach § 21 Abs. 2 ThürDSG trägt die Verantwortung für die Zulässigkeit der Übermittlung die übermittelnde Stelle. Erfolgt die Übermittlung auf Ersuchen des Dritten, an den die Daten übermittelt werden, trägt dieser die Verantwortung. In diesem Fall prüft die übermittelnde Stelle nur, ob das Übermittlungsersuchen im Rahmen der Aufgaben des Dritten liegt, es sei denn, dass besonderer Anlass zur Prüfung der Zulässigkeit der Übermittlung besteht. Eindeutig lag im vorliegenden Falle die Verantwortlichkeit für die Übermittlung beim Gericht. Wenn dieses im Rahmen einer Streitigkeit Unterlagen anfordert, hat die übermittelnde Stelle grundsätzlich keinen besonderen Anlass, die Übermittlungsbefugnis näher zu prüfen. Der Erforderlichkeitsgrundsatz hat auch in § 99 VwGO seinen Niederschlag gefunden.

11.10 Adressenverkauf durch das Grundbuchamt?

Im August 2016 beschwerte sich ein Bürger beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) über das Grundbuchamt der Stadt Erfurt wegen eines Verstoßes gegen datenschutzrechtliche Vorschriften. Der Beschwerdeführer legte dar, dass ein Immobilienmakler durch eine Mitteilung des Grundbuchamtes Erfurt in den Besitz von 146 Eigentümeradressen gekommen sei, darunter auch die Adresse des Beschwerdeführers. Der Immobilienmakler habe die Adressen dann für eigene Werbezwecke benutzt. Die Adressen seien im Rahmen der Aufhebung der Satzung, Sanierungsgebiet „Innere Oststadt“ im Teilbereich „Hanse-

viertel“ und der dadurch veranlassten Löschung der Eintragungen aus den Grundbüchern einem Schreiben beigefügt gewesen, das alle Eigentümer aus dem Gebiet erhalten hätten.
Zur Prüfung, ob die Verarbeitung der personenbezogenen Daten nach den geltenden datenschutzrechtlichen Vorschriften erfolgte, bat der TLfDI das Grundbuchamt der Stadt Erfurt und den angegebenen Immobilienmakler um eine Stellungnahme zum dargelegten Sachverhalt.
Der Immobilienmakler gab an, die Adressen vom Grundbuchamt erhalten zu haben. Das Grundbuchamt legte jedoch dar, dass in den vom Beschwerdeführer angegebenen Wohnungsgrundbüchern der betreffenden Eigentümergemeinschaft noch keine Löschung des Sanierungsvermerks veranlasst wurde. Somit hatte das Grundbuchamt auch noch keine Mitteilung an die Eigentümer geschickt und auch keine Adressliste.
Im Falle einer Eintragung, die alle Miteigentumsanteile eines Grundstücks betrifft – wie beispielsweise die Löschung des Sanierungsvermerks – versendet das Grundbuchamt nach eigener Darstellung eine entsprechende Mitteilung an die Eigentümer. Durch das behördenspezifische Datenverarbeitungssystem der Grundbuchämter wird dieser Mitteilung eine Liste aller Miteigentümer beigefügt mit der Bezeichnung des Grundbuchblattes, des Namens und der Anschrift. Weiterhin teilte der TLfDI dem Beschwerdeführer mit, dass diese Liste ohnehin keine Daten zu seiner Person enthielte, da der Beschwerdeführer nicht als Eigentümer der betreffenden Grundstücke im Grundbuch eingetragen war.

Im Falle einer Eintragung ins Grundbuch, die alle Miteigentumsanteile eines Grundstücks betrifft – wie beispielsweise die Löschung des Sanierungsvermerks – versendet das Grundbuchamt eine entsprechende Mitteilung an alle Eigentümer, einschließlich einer Adressliste der Miteigentümer, da dies das behördenspezifische Datenverarbeitungssystem vorsieht. Die Versendung dieser Liste an die Miteigentümer stellt somit keinen Verstoß gegen datenschutzrechtliche Vorschriften dar.



Family doctor woman. – © Kurhan / Fotolia.com

12. Gesundheits- und Sozialdatenschutz

12.1 Krebsregistergesetz – datenschutzgerecht?!

Im Jahr 2008 hat das Bundesministerium für Gesundheit den sogenannten Nationalen Krebsplan initiiert. Dessen Ziel ist die Weiterentwicklung und Verbesserung der Krebsfrüherkennung sowie die Qualitätssicherung zum Zweck einer effizienten onkologischen Behandlung von an Krebs erkrankten Menschen. Ausfluss dieses Nationalen Krebsplans ist das im Frühjahr verabschiedete „Gesetz zur Weiterentwicklung der Krebsfrüherkennung und zur Qualitätssicherung durch klinische Krebsregister“ (Krebsfrüherkennungs- und -registergesetz – KFRG). Nach dem neu in das Fünfte Buch Sozialgesetzbuch (SGB V) eingefügten Paragrafen 65c sind die Länder verpflichtet, flächendeckend klinische Krebsregister einzurichten und zu

betreiben. Damit soll eine bundesweit einheitliche und valide Datengrundlage für eine effektive Auswertung und Bewertung der onkologischen Versorgung geschaffen werden. Das Gesetz macht Vorgaben für die Länder, die auch in Thüringen umgesetzt werden müssen. Hier existieren zwar bereits seit ca. 20 Jahren fünf regionale klinische Krebsregisterstandorte in Erfurt, Gera, Jena, Nordhausen und Suhl. Künftig sind die klinischen Krebsregister allerdings nach der bundesgesetzlichen Vorgabe gehalten, eine möglichst vollzählige und vollständige Erfassung und Auswertung von personenbezogenen und medizinischen Daten von Krebspatienten zu gewährleisten. In Thüringen soll diese Vorgabe mit dem Thüringer Krebsregistergesetz (ThürKRG) umgesetzt werden. Künftig soll es ein klinisches Krebsregister Thüringen geben, in das die bewährte regionale Struktur eingebunden werden soll.

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) war bereits frühzeitig in den Prozess der Erarbeitung des Gesetzentwurfs durch das Thüringer Ministerium für Arbeit, Soziales, Gesundheit, Frauen und Familie (TMASGFF) eingebunden. Er wies im Rahmen des Beratungsverfahrens vor allem darauf hin, dass die Aufgaben der einzelnen im Gesetz vorgesehenen Akteure (zentrales klinisches Krebsregister, regionale Registerstellen, Auswertungsstelle) im Gesetz eindeutig geregelt werden müssen. Sofern private Stellen mit bestimmten Aufgaben beliehen werden sollen, muss auch diese Beleihung eindeutig und unter Nennung der konkreten Befugnisse erfolgen.

Besonders wichtig war dem TLfDI, dass im Gesetz ein Widerspruchsrecht für die betroffenen Patienten geregelt ist. Alle bekannten bereits in Kraft getretenen Gesetze der Länder sehen ein solches Widerspruchsrecht des Patienten vor. Damit das Grundrecht auf informationelle Selbstbestimmung gewahrt wird, hält der TLfDI ein derartiges Widerspruchsrecht für geboten. In der klinischen Krebsregistrierung erfolgt eine umfassende Dokumentation der Gesundheitsdaten des an Krebs erkrankten Patienten. Es muss möglich sein, dass der Patient die Entscheidung trifft, dass seine Daten nur dem jeweils behandelnden Arzt zur Verfügung stehen und nicht der zentralen klinischen Krebsregistrierung. Da jedoch der Zweck der Krebsregistrierung, nämlich die optimale onkologische Versorgung der Patienten sicherzustellen, gleichwohl gewährleistet werden soll, hielt der TLfDI es für zulässig, wenn die jeweiligen Daten des widersprechenden Patienten in anonymisierter Form in das Register einfließen.

So ist gewährleistet, dass die Daten für Thüringen flächendeckend vorliegen, jedoch im Falle eines Widerspruchs keiner bestimmten Person eindeutig zuzuordnen sind. Mit dieser Auffassung konnte sich der TLfDI durchsetzen.

Der dem Thüringer Landtag vorgelegte Gesetzentwurf der Landesregierung (Drucksache Nr. 6/4649) wurde nicht mehr wesentlich geändert. Allerdings wurde nun, wie vom TLfDI gefordert, klargestellt, welche Stellen welche Aufgaben bei der klinischen Krebsregistrierung übernehmen. Der TLfDI nahm gegenüber dem Landtag Stellung und führte aus, dass es zwar erfreulich ist, dass auf sein Drängen hin nunmehr doch ein Widerspruchsrecht des Betroffenen Eingang in den Gesetzentwurf gefunden hat. Allerdings erstreckt sich das Widerspruchsrecht nur auf die Identitätsdaten. Insoweit besteht Grund zu der Annahme, dass aus den verbleibenden klinischen Daten und meldungsbezogenen Daten in Einzelfällen die Identität des Patienten ermittelt werden kann. Aus welchem Grund sie nicht zumindest teilweise dem Widerspruchsrecht unterliegen, ist unklar. Der TLfDI teilte dem Landtag mit, dass es aus datenschutzrechtlicher Sicht wünschenswert wäre, wenn bei einem Widerspruch auch alle medizinischen Daten gelöscht bzw. tatsächlich anonymisiert würden. Dies könnte beispielsweise dadurch erreicht werden, dass bei diesen Daten nur das Geburtsjahr gespeichert wird. Moniert wurde auch, dass das Klinische Krebsregister Thüringen ermächtigt wird, Klardaten „für Auswertungen zum Zwecke der Verbesserung der Qualität der onkologischen Versorgung einschließlich regionaler Qualitätskonferenzen und für die Übermittlung von Auswertungsergebnissen an die Leistungserbringer zu verwenden“. Im Gesetz wird bereits eine Ermächtigung zur Übermittlung an mitbehandelnde Leistungserbringer formuliert. Es ist nicht ersichtlich, wozu eine weitere „Verwendung“ der Klardaten im Rahmen der Qualitätssicherung notwendig sein soll. Dies ist auch der Begründung nicht zu entnehmen. Für den genannten Zweck der Qualitätssichtung sind nach Auffassung des TLfDI pseudonymisierte bzw. angemessen aggregierte Daten ausreichend. Aufgaben der Qualitätssicherung sollten nicht mit Klardaten durchgeführt werden.

Das Gesetz soll zum Ende des Jahres in Kraft treten. Der TLfDI will im kommenden Jahr das zentrale klinische Krebsregister Thüringen, eine regionale Registerstelle und die Auswertungsstelle vor Ort aufsuchen, um zu prüfen, wie die gesetzlichen Vorgaben umgesetzt und ob die geltenden Datenschutzgesetze eingehalten werden.

Der TLfDI hat die Umsetzung des § 65c SGB V durch das Thüringer Krebsregistergesetz datenschutzrechtlich begleitet. Um das Grundrecht auf informationelle Selbstbestimmung der betroffenen Patienten zu wahren, hat er auf der Einführung eines Widerspruchsrechts im Gesetz bestanden. Der vom Gesetz verfolgte Zweck der optimalen Qualitätssicherung in der onkologischen Versorgung kann auch durch die Aufnahme anonymisierter Patientendaten gewährleistet werden.

12.2 Staatsvertrag zum epidemiologischen Krebsregister

Aus dem Nationalen Krebsregister der DDR entstand nach der deutschen Wiedervereinigung das Gemeinsame Krebsregister der Länder Berlin, Brandenburg, Mecklenburg-Vorpommern, Sachsen-Anhalt und der Freistaaten Sachsen und Thüringen (GKR). Diese Länder schlossen im Jahr 1997 einen Staatsvertrag über das Gemeinsame Krebsregister, der durch Staatsvertrag von 2006 geändert wurde. Bereits im Jahr 2012 zeigte sich, dass weitere Änderungen des Staatsvertrages zum Gemeinsamen Krebsregister erforderlich sind. Mit der Neuregelung des Bundeskrebsregisterdatengesetzes wurden den epidemiologischen Krebsregistern der Länder Aufgaben zugewiesen, die landesgesetzlicher Regelungen bedürfen. Mit dem Inkrafttreten des Krebsfrüherkennungs- und -registergesetzes am 9. April 2013 und dem neuen § 65c des Sozialgesetzbuches (SGB) Fünftes Buch (V) als gesetzlicher Grundlage für die klinische Krebsregistrierung ergeben sich auch Vorgaben für die epidemiologische Krebsregistrierung, die umgesetzt werden müssen. Zum klinischen Krebsregister wird auf den Beitrag in diesem Tätigkeitsbericht unter Nummer 12.1 verwiesen. Epidemiologische Register erfassen im Gegensatz zu klinischen Krebsregistern, wie häufig welche Art von Krebserkrankung in Deutschland an welchem Ort ist. Die klinische Krebsregistrierung dient dagegen der Optimierung der onkologischen Versorgung.
Durch die Änderung des Staatsvertrages sollen gemeinsame Strukturen im Zuge des Abgleichs mit Daten aus den Melderegistern und den Leichenschauscheinen geschaffen werden. Außerdem war der Staatsvertrag anzupassen, weil die in § 25a SGB V genannten Rahmenbedingungen zur Durchführung organisierter Früherkennungsprogramme auf überholten Richtlinien des Bundesausschusses der

Ärzte und Krankenkassen über die Früherkennung von Krebserkrankungen (Krebsfrüherkennungs-Richtlinien) beruhten. Die Erarbeitung der neuen Fassung des Staatsvertrages wird federführend von der Berliner Senatsverwaltung betreut. Alle Datenschutzbeauftragten der beteiligten Länder waren zu Stellungnahmen aufgerufen. Bei der Erarbeitung des Entwurfs ergaben sich zahlreiche datenschutzrechtliche Einzelprobleme, die diskutiert wurden. Dies betraf beispielsweise die Speicherdauer von Meldedaten beim GKR, die Voraussetzungen eines Melderegisterabgleichs, den Inhalt einer Übergangsregelung. Das für die Änderung des Staatsvertrages fachlich zuständige Thüringer Ministerium für Arbeit, Soziales, Gesundheit, Frauen und Familie (TMASGFF) beteiligte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) rege im Verfahren. Im Oktober des Jahres 2016 teilte das TMASGFF auf Nachfrage des TLfDI mit, dass die Ressortabstimmung in nächster Zeit, jedenfalls noch im Jahr 2016 erfolgen werde.
Mit der Drucksache 6/3823 wurde der Thüringer Landtag durch seinen Präsidenten nach Art. 67 Abs. 4 der Verfassung des Freistaats Thüringen über den Entwurf des 2. Staatsvertrags zur Änderung des Staatsvertrages über das Gemeinsame Krebsregister der Länder Berlin, Brandenburg, Mecklenburg-Vorpommern, Sachsen-Anhalt und der Freistaaten Sachsen und Thüringen unterrichtet. Er wurde im Ausschuss für Soziales, Arbeit und Gesundheit am 27. April 2017 in öffentlicher Sitzung beraten und zur Kenntnis genommen.

Mit der Neuregelung des Bundeskrebsregisterdatengesetzes wurden den epidemiologischen Krebsregistern der Länder Aufgaben zugewiesen, die landesgesetzlicher Regelungen bedürfen. Durch die Änderung des Staatsvertrages über das Gemeinsame Krebsregister der Länder Berlin, Brandenburg, Mecklenburg-Vorpommern, Sachsen-Anhalt und der Freistaaten Sachsen und Thüringen (GKR) wurden die notwendigen Änderungen vorgenommen. Der TLfDI war am Verfahren beteiligt.

12.3 Wearables und Gesundheits-Apps immer datenschutzkonform?

Einer repräsentativen Umfrage durch die Bitkom Research GmbH zufolge soll bereits knapp ein Drittel der Bevölkerung ab 14 Jahren sogenannte Fitness-Tracker zur Aufzeichnung von Gesundheitswer-

ten und persönlichen Verhaltensweisen nutzen. Die 91. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder hatte deshalb in ihrer Entschließung im April 2016 „Wearables und Gesundheits-Apps – Sensible Gesundheitsdaten effektiv schützen!“ ihre Vorstellungen diesbezüglich veröffentlicht.
So weist die Konferenz darauf hin, dass zahlreiche Wearables und Gesundheits-Apps die aufgezeichneten Daten an andere Personen oder Stellen weiter geben, ohne dass die betroffenen Personen hiervon wissen oder dazu eine bewusste Entscheidung treffen. Zudem müssen die Grundsätze der Datenvermeidung und Datensparsamkeit beachtet werden. Dies sieht auch Artikel 25 der ab 25. Mai 2018 wirksam werdenden Datenschutzverordnung (DS-GVO) vor.
Zudem ist die Konferenz u. A. der Meinung, dass, wer aus eigenen Geschäftsinteressen gezielt bestimmte Wearables und Gesundheits-Apps in Umlauf bringt oder ihren Vertrieb systematisch unterstützt, eine Mitverantwortlichkeit für die rechtmäßige Ausgestaltung solcher Angebote trägt. Nicht zuletzt bezweifelt sie die Rechtmäßigkeit bei Einwilligungserklärungen etwa in Beschäftigungs- und Versicherungsverhältnissen (siehe Anlage 3).

Wearables und Gesundheits-Apps erfahren derzeit einen wirtschaftlichen Aufschwung. Dennoch muss jederzeit der Datenschutz gewährleistet sein. Eine Mitverantwortlichkeit für die rechtmäßige Ausgestaltung solcher Angebote trägt auch der Entwickler und der Betreiber solcher Angebote. Deshalb ist bereits in der Planung und Entwicklung von IT-Systemen Datenschutz und Datensicherheit zu berücksichtigen (Data protection by design). Die IT-Systeme müssen zudem datenschutzfreundlich so voreingestellt sein, dass nur die personenbezogenen Daten verarbeitet werden, die für den verfolgten Zweck erforderlich sind (Data protection by default).

12.4 Arbeitsvermittlung gegen Datensammlung

Im Berichtszeitraum erhielt der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) eine Beschwerde über ein überbetriebliches Ausbildungsunternehmen, dessen Aufgabe die individuelle Integrationsbegleitung zur Wiedereingliederung in den Arbeitsmarkt ist. Die Betroffene trug vor, dass das Unternehmen wegen der Verwendung einer Schweigepflichtentbindung eine Datenschutzverletzung begangen habe. Im Zuge einer Maßnahme zur

Arbeitsvermittlung habe das Jobcenter einer Stadt den Fall der Beschwerdeführerin an das Ausbildungsunternehmen abgegeben. Dabei sei es zu einer schriftlichen Vereinbarung mit einem „Übergabeprotokoll“ gekommen, das auch eine Schweigepflichtentbindungserklärung enthielt. Die Beschwerdeführerin legte dar, man habe sie darauf hingewiesen, dass es für die Teilnahme am Projekt nötig ist, eine Schweigepflichtentbindung zu unterschreiben. Dies sollte eine regelmäßige Berichterstattung durch das Ausbildungsunternehmen an den kommunalen Eigenbetrieb legitimieren. Es folgte ein Schriftverkehr über den Datenaustausch mit dem Projektleiter im Ausbildungsbetrieb. Schließlich kam es zum Vertragsabschluss zwischen der Beschwerdeführerin und dem Betrieb. Jedoch bezog sich die Schweigepflichtentbindung auf alle personenbezogenen Daten die Beschwerdeführerin betreffend, also auch solche, die für die Tätigkeit des Ausbildungsunternehmens und des Jobcenters gar nicht erforderlich waren.

Der TLfDI bat das Unternehmen um Stellungnahme zum vorgetragenen Sachverhalt, insbesondere auch dazu, welche Daten an das Jobcenter übermittelt werden. Dieses teilte mit, dass es nach dem Schreiben des TLfDI das bisher verwendete Formular „Übergabeprotokoll“ sofort aus dem Verkehr gezogen und den Mitarbeiter/innen die Nutzung des Formulars untersagt habe. Dem Jobcenter werden zur Arbeitsvermittlung ausschließlich die Daten von Betroffenen übermittelt, die im direkten Zusammenhang mit der Begleitung und Vermittlung in relevante Berufsfelder stehen. Neben persönlichen Angaben seien dies auch gesundheitliche Sachverhalte, die für verschiedene Berufsfelder relevant sind (beispielsweise eine Seh-, Geh- oder Hörbehinderung). Aus diesem Grund werden auch für die Vermittlung relevante Daten zum Bildungsstand und zum Bildungsverlauf erhoben. Die Erhebung und Übermittlung an das Jobcenter ist notwendig, um berufliche Vermittlungsvorschläge zu unterbreiten und eine zielgerichtete Vermittlung der Betroffenen zu ermöglichen.

Der TLfDI wies das Unternehmen darauf hin, dass der/die Betroffene gemäß § 4 Abs. 1 und Abs. 2 eine wirksame Einwilligung in die Verarbeitung oder Nutzung der personenbezogenen Daten nur freiwillig erklären kann. Gemäß § 4 Abs. 3 ThürDSG ist der/die Betroffene hierbei auf den Zweck und den Umfang der Verarbeitung oder Nutzung und die voraussichtliche Dauer der Speicherung seiner Daten, auf seine Rechte auf Löschung sowie auf Verlangen auf die

Folgen der Verweigerung der Einwilligung hinzuweisen (sogenannte informierte Einwilligung).
Das Unternehmen berücksichtigte die datenschutzrechtlichen Hinweise und übersandte dem TLfDI ein neugefasstes Formular zur Schweigepflichtentbindung mit der Bitte, dies nochmals datenschutzrechtlich zu überprüfen. Das Formular sollte als Befugnis zur Datenübermittlung zwischen dem Unternehmen und dem Jobcenter dienen. Nach Durchsicht der Unterlagen empfahl der TLfDI für das Formular noch eine Präzisierung zweier Sachverhalte von personenbezogenen Daten, damit die Einwilligung auch tatsächlich „informiert“ abgegeben werden kann. Außerdem sollte das Widerrufsrecht des Betroffenen noch deutlicher gemacht werden. Für den Fall der Verweigerung der Abgabe einer Schweigepflichtentbindung sollten die hierdurch entstehenden Verzögerungen in der Bearbeitung dargelegt und begründet werden, um das Verfahren für den Betroffenen transparent zu machen. Diesen Forderungen kam das Unternehmen nach.

Nach § 4 Abs. 1 und Abs. 2 ThürDSG kann der Betroffene eine wirksame Einwilligung in die Verarbeitung oder Nutzung seiner personenbezogenen Daten nur freiwillig erklären. Im Rahmen dieser Erklärung ist der Betroffene gemäß § 4 Abs. 3 ThürDSG auf den Zweck und den Umfang der Verarbeitung oder Nutzung und die voraussichtliche Dauer der Speicherung seiner Daten, auf seine Rechte auf Löschung sowie auf Verlangen auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Nur wenn er alle notwendigen Informationen hat, kann er eine informierte Einwilligung abgeben.

12.5 Patientenportal – modern, aber datenschutzgerecht?

Ein Klinikum wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und bat um Beratung zu einem neuen Projekt. Das Krankenhaus beabsichtigte, ein Patientenportal einzurichten. Diese Maßnahme war Bestandteil des neuen Infotainmentservices des Klinikums. Das Patientenportal sollte der Information der Patienten dienen. Sie sollten die Möglichkeit haben, künftig auf diesem Weg auch eigenständig ihre Essenswünsche einzugeben oder auch sonstige Wünsche nach bestimmten Pflegedienstleistungen oder an das Servicepersonal einzugeben.

Die Mitarbeiter des TLfDI ließen sich das geplante Projekt in einer Entwurfsfassung vor Ort beschreiben. Es ist vorgesehen, dass der Patient sich an dem Portal anmeldet und er auch während des ganzen Verfahrens Herr der Daten bleibt. Das Klinikum wollte sich im Hinblick auf die zum Einsatz kommende Software eines externen Anbieters bedienen, der einen cloudbasierten Dienst anbietet, der in Deutschland betrieben wird. Deswegen war auf die Prüfung der Verschlüsselung der Transportwege und der verschlüsselten Ablage der Daten in einer Cloud besonderes Augenmerk zu richten. Nach § 27 Abs. 10 Thüringer Krankenhausgesetz hat das Krankenhaus die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich und angemessen sind, um die Beachtung der in den Absätzen eins bis neun dieser Vorschrift enthaltenen Bestimmungen zu gewährleisten.

Es war von der Projektleitung vorgesehen, dass die Daten über verschlüsselte Transportwege transportiert werden und in der Cloud automatisiert verschlüsselt abgelegt werden. Dabei werden sie in einem für den Patienten angelegten Datencontainer zwischengespeichert, der nur mithilfe des Patienten wieder entschlüsselbar ist. Entsprechend dem Schutzbedarf der eingegebenen Daten werden verschiedene Datencontainer mit verschiedenen Schutzstufen gebildet, die über verschiedene symmetrische Schlüssel verschlüsselt werden. Ein Zugriff des externen Dienstleisters wird durch diese technischen Maßnahmen ausgeschlossen. Für jeden Behandlungsfall wird im System ein neuer Container angelegt und der Patient kann selbst bestimmen, wie lange die Daten jeweils gespeichert werden.

Geplant ist, dass das Klinikum dem Patienten zunächst nach der Anmeldung seine Aufenthaltsdaten im Krankenhaus zur Verfügung stellt. Gemeint sind hiermit der genaue Zeitraum des Aufenthalts und die Angabe der Station, auf die der Patient kommt. Er erhält dann Links auf die Homepage des Klinikums, direkt auf die Stellen, die für ihn interessant sein könnten. Der Patient kann, soweit er dies wünscht, weitere Daten im System eingeben. Dies kann beispielsweise die Angabe von Angehörigen sein, die in bestimmten Fällen informiert werden sollen. Das Patientenportal soll nur innerhalb des Netzes der Klinik nutzbar sein.

Rechtliche Grundlage für den Betrieb des Portals soll die Einverständniserklärung des Patienten sein. Diesem wird vor Erteilung des Einverständnisses ein umfangreicher Informationsflyer zur Verfügung gestellt.

Der TLfDI setzte sich besonders mit der Frage der datenschutzgerechten Verschlüsselung der Daten auseinander, da es dem Patienten zum einen möglich war, selbst Gesundheitsdaten über sich im System einzugeben und andererseits bereits die Angabe des Aufenthaltsdatums ein Gesundheitsdatum ist. Es musste sichergestellt sein, dass Unbefugte auf keinen Fall auf Patientendaten Zugriff erhielten. Nach tiefgehender Prüfung teilte der TLfDI dem Klinikum mit, dass datenschutzrechtliche Bedenken gegen das geplante Vorhaben nicht bestehen.
Sofern sich das Verfahren bewährt, plant das Klinikum, möglicherweise weitere Funktionen über das Patientenportal anzubieten. Auch in diesem Fall muss geprüft werden, welchen Schutzbedarf die verarbeiteten personenbezogenen Daten haben und ob die zum jetzigen Zeitpunkt getroffenen technischen und organisatorischen Maßnahmen hierfür ausreichen. Der TLfDI hat das Klinikum gebeten, ihn in diesem Fall erneut zu kontaktieren, um eine datenschutzrechtliche Bewertung vornehmen zu können.

Ein Krankenhaus hat die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich und angemessen sind, um die datenschutzrechtlichen Bestimmungen des Thüringer Krankenhausgesetzes einzuhalten. Bei der Einrichtung eines Patientenportals in einer Cloud ist die Frage der datenschutzgerechten Verschlüsselung von großer Wichtigkeit, da nur so sichergestellt ist, dass Zugriffe unberechtigter Personen verhindert werden.

12.6 Integrierte Teilhabeplanung als App – Kontrolle vor Ort

Bereits im 11. Tätigkeitsbericht zum öffentlichen Bereich beschäftigte sich der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) mit der Problematik der Integrierten Teilhabeplanung (dort unter Nummer 16.1). Durch die Integrierte Teilhabeplanung (ITP) sollten die Ansprüche und Leistungen der Eingliederungshilfe nach den §§ 53 ff. Sozialgesetzbuch (SGB) Zwölftes Buch (XII) für Menschen mit Behinderungen besser geltend gemacht werden können. Gegenstand des ITP ist unter anderem ein Fragebogen (ITP-Bogen), in dem die Hilfebedarfe von Menschen mit Behinderungen ermittelt werden sollen. Der ITP sollte testweise von einigen Sozialämtern als sogenannte App (für Applikation) in dem Thüringer Antragssystem für Verwaltungsleistungen (ThAVEL)

betrieben werden. Wie bereits im 11. Tätigkeitsbericht unter Nr. 16.1 dargelegt, begleitete der TLfDI die Einführung der App datenschutzrechtlich. Die datenschutzrechtlichen Anforderungen an technische und organisatorische Maßnahmen nach § 9 Thüringer Datenschutzgesetz (ThürDSG) wurden in entsprechenden Konzepten festgelegt. Wichtig war, dass im System verschiedene Rollen mit verschiedenen Zugriffsrechten festgelegt wurden. Denn nicht nur der zuständige Sozialarbeiter sollte Zugriff auf das System haben, sondern auch eingeschränkt bestimmte Leistungserbringer wie Wohnheime oder Werkstätten, in denen die Betroffenen wohnten bzw. tätig waren. Der TLfDI hatte darauf gedrungen, dass nach dem Grundsatz der Erforderlichkeit die Rechte der Bearbeiter so vergeben werden, dass immer nur derjenige Zugriff auf die Daten hat, der sie für seine Aufgabenerfüllung benötigt. Wie im letzten Tätigkeitsbericht angekündigt, hat der TLfDI die Anwendung der App vor Ort geprüft.

Die ITP-App wurde im Sozialamt eines Landratsamtes im Echtzeitbetrieb in Augenschein genommen. Dort wurde festgestellt, dass ein entsprechendes Verfahrensverzeichnisblatt für die ITP-App im Landratsamt nicht vorliegt. Der TLfDI hat dies nachgefordert, weil nach § 10 ThürDSG die Daten verarbeitenden Stellen ein Verzeichnis der automatisierten Verfahren, mit denen personenbezogene Daten verarbeitet werden, führen müssen.

Im Verfahren gibt es einen ITP-Administrator, der die Rechte der übrigen Beteiligten festlegt. Er bestimmt im Sozialamt die sogenannten Leiter des Verfahrens, die Verfahren anlegen können. Wenn ein Verfahren angelegt ist, füllt der Sachbearbeiter im Sozialamt den ITP-Bogen im System elektronisch aus. Der Leiter des Verfahrens hat immer Schreibrechte an der Akte. Er kann einem sogenannten Leistungserbringer ebenfalls Schreibrechte erteilen.

Neben dem elektronischen Verfahren in ThAVEL gibt es im Sozialamt auch immer eine Handakte, es handelt sich damit um ein so genanntes hybrides Verfahren.

Der ITP Bogen kommt erst dann zur Papierakte, wenn das ITP-Verfahren abgeschlossen ist, das heißt, die Zielvereinbarung von dem Betroffenen und gegebenenfalls seinem Betreuer unterzeichnet ist. Nach der Unterzeichnung wird das ITP-Verfahren in der App beendet und nach einer gewissen Karenzzeit wird der ganze Vorgang gelöscht. Das Verfahren dient daher in erster Linie zur optimalen Erstellung des ITP-Bogens, mit dem der Hilfebedarf der Betroffenen ermittelt wird.

Auch bei einem ambulanten Pflegedienst (Leistungserbringer) wird die ITP-App angesehen, damit überprüft werden kann, welche Rechte ein Leistungserbringer hat. Bearbeitungsrechte bestehen für den Leistungserbringer nur dann, wenn ihm der Fall durch den Bearbeiter im Sozialamt freigeschaltet und er noch nicht abgeschlossen wurde. Wenn die Akte vom Leiter des Verfahrens beim Sozialamt gelöscht wird, kann auch der Leistungserbringer die Akte nicht mehr sehen. Es gibt aber die Möglichkeit, die Daten zu exportieren. Dies ist erforderlich, weil die Unterlagen nach dem Thüringer Wohn- und Teilhabegesetz 30 Jahre aufbewahrt werden müssen.
Der TLfDI stellte während der Kontrolle fest, dass die Zugriffsrechte ordnungsgemäß vergeben sind und die Rollen datenschutzgerecht eingerichtet wurden. Zu bemängeln hatte er, dass die Passwortvergabe für die Anmeldung im System nicht den Vorgaben der Maßnahmennummer 2.11 der BSI-Grundschutz-Kataloge entspricht. Außerdem enthielt das System keine komplette Historie. Es war nicht ohne Weiteres erkennbar, welcher Bearbeiter welche Änderung wann vorgenommen hat. Zu sehen waren im System nur der Bearbeiter, das Datum und die Tatsache, dass Änderungen vorgenommen wurden, nicht aber, welche Änderungen welcher Mitarbeiter vorgenommen hat. Änderungen konnten daher nur aus einem Vergleich der jeweils hinterlegten Versionen erkannt werden. Dies ist nicht von vornherein unzulässig, es muss aber durch organisatorische Maßnahmen sichergestellt sein, dass die vorgenommenen Änderungen revisionssicher erkennbar sind. Dies kann beispielsweise durch entsprechende Ablagen und Vermerke in den Handakten geschehen. Das Landratsamt wurde hierzu sowie zur Passwortvergabe um Stellungnahme gebeten. Die Fallbearbeitung dauert noch an.
Grundsätzlich ist festzustellen, dass die Einführung der ITP-App größtenteils den datenschutzrechtlichen Vorgaben entspricht. Insbesondere die Rechtevergabe wurde so vorgenommen, wie dies zwischen dem TLfDI, dem TLRZ und dem Thüringer Sozialministerium besprochen worden ist.

Ein elektronisches Antragsverfahren, auf das mehrere Stellen Zugriff haben, ist nur dann datenschutzgerecht, wenn bei den Zugriffsrechten darauf geachtet wird, dass die jeweiligen Bearbeiter nur die Angaben sehen, die für ihre Bearbeitung erforderlich sind. Ist die Bearbeitung abgeschlossen, müssen Zugriffsrechte wieder entzogen werden. Durch eine Historie im System oder entsprechende organisatori-

sche Maßnahmen ist sicherzustellen, dass nachvollziehbar ist, wer in welcher Rolle wann welche Änderungen im System vorgenommen hat.

12.7 Biete medizinische Werbung, suche ärztliche Daten …

Im September 2016 bat die Landeszahnärztekammer Thüringen (LZÄKTh) den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) um Auskunft darüber, ob bzw. inwiefern die Übermittlung von Mitgliederdaten an die Bundeszahnärztekammer (BZÄK) datenschutzrechtlich zulässig ist.
Die LZÄKTh ist Mitglied der Bundeszahnärztekammer (BZÄK). Gemeinsam mit der Kassenzahnärztlichen Bundesvereinigung gibt die BZÄK bundesweit 14-tägig die Zeitschrift „Zahnmedizinische Mitteilungen“ (zm) heraus. Zum Zweck der Verteilung dieser Zeitschrift an die Zahnärzte in Thüringen übermittelt die Landeszahnärztekammer die Adressen ihrer Mitglieder (Name, Anschrift, Geschlecht) an den Bundesverband. Herausgegeben und vertrieben wird die Zeitschrift von einem privaten Verlag; finanziert wird dies zum größten Teil über den Erlös aus Werbeanzeigen. Die Werbenden beabsichtigen, das Anzeigengeschäft zukünftig stärker auf die Beworbenen zuzuschneiden, sodass Werbebeilagen gezielt diejenigen Empfänger der Zeitschrift erreichen, die tatsächlich mit der Werbung angesprochen werden sollen. Daher bat die BZÄK die Landesverbände, das heißt die LZÄKTh, weitere Daten ihrer Mitglieder preiszugeben, unter anderem Approbationsdaten, mit denen zwischen berufstätigen und nicht mehr berufstätigen Zahnärzten unterschieden werden kann, sowie Angaben über Praxisgründer und Berufseinsteiger und Daten zum beruflichen Status als selbstständiger oder angestellter Zahnarzt. Die Landeszahnärztekammer Thüringen hielt diese Datenübermittlung an die Bundeszahnärztekammer e. V. für datenschutzrechtlich bedenklich.
Aufgrund eigener Bedenken zur Datenübermittlung hatte die BZÄK bereits ein Rechtsgutachten zur Datenübermittlung erstellen lassen. Der TLfDI ist der Auffassung, dass die Verwendung von Mitgliederdaten zum Zweck der zielgerichteten Ausstattung der „Zahnärztlichen Mitteilungen“ mit Werbung rechtlich nicht zulässig ist und begründet dies folgendermaßen:
Zunächst muss man zwischen der Datenerhebung durch die Landeszahnärztekammer an die Bundeszahnärztekammer und sodann der

Datenübermittlung durch letztere an eine nicht-öffentliche Stelle – den privaten Verlag – unterscheiden. Als Körperschaft des öffentlichen Rechts richtet sich das gesamte Handeln der LZÄKTh nach dem öffentlichen Recht. Das Thüringer Datenschutzgesetz (ThürDSG) kann die Datenübermittlung der Landesärztekammer nicht rechtfertigen, da im Datenschutzrecht ein sogenanntes Verbot mit Erlaubnisvorbehalt gilt. Das bedeutet, dass die Verarbeitung von Daten gemäß § 4 Abs. 1 ThürDSG nur zulässig ist, sofern eine Rechtsvorschrift sie erlaubt bzw. der Betroffene selbst eingewilligt hat.
Rechtsgrundlage für die Arbeit der LZÄKTh ist das Thüringer Heilberufegesetz (ThürHeilBG). Jedoch ist der Umgang mit personenbezogenen Daten hier nicht abschließend geregelt. Daher muss ergänzend das ThürDSG herangezogen werden (§ 2 Abs. 3 Satz 1). Nach § 19 Abs. 1 ThürDSG ist das Erheben personenbezogener Daten zulässig, wenn ihre Kenntnis zur Erfüllung der Aufgaben der erhebenden Stelle erforderlich ist. Ob beziehungsweise inwiefern die Erhebung der o. g. ergänzenden Daten zum Zwecke zielgerichteter Werbung für die Aufgabenerfüllung der LZÄKTh erforderlich ist, muss die LZÄKTh fachlich begründen. Sofern diese Daten für die Aufgabenerfüllung nach § 5 des ThürHeilBG nicht erforderlich sind, dürfen diese Daten nicht erhoben werden. Vor diesem Hintergrund hielt die LZÄKTh bereits die Erhebung dieser Daten für datenschutzrechtlich bedenklich.
Die Frage der Datenübermittlung an den privaten Verlag als nicht-öffentliche Stelle ist in § 22 ThürDSG geregelt. Diese Datenübermittlung ist nur zulässig, wenn sie zur Aufgabenerfüllung der LZÄKTh erforderlich ist und wenn die Voraussetzungen vorliegen, die eine Nutzung nach § 20 ThürDSG zulassen würden.
Nach Auffassung des TLfDI ist die Übermittlung der bisherigen Daten (Name und Anschrift der Ärzte) an die Bundeszahnärztekammer e. V. zur Erfüllung der Aufgaben, die der LZÄKTh obliegen, erforderlich. Denn diese Angaben sind notwendig, um die gemeinsam vertriebene Zeitung „Zahnärztliche Mitteilungen“ an die Mitglieder zu vertreiben. Diese Erforderlichkeit besteht jedoch nach Darlegung der LZÄKTh nicht in Bezug auf weitere Daten, da die bessere Bewerbung von Mitgliedern mit Anzeigen nicht zu den gesetzlichen Aufgaben der LZÄKTh gehört. Somit ist diese Übermittlung unzulässig, die Rechtsgrundlage fehlt, worauf der TLfDI die LZÄkTh hinwies. Gleichzeitig teilte er mit, dass eine Datenübermitt-

lung jedoch zulässig sei, wenn sich die Mitglieder der LZÄKTh mit der Erhebung dieser Daten und der Übermittlung an die BZÄK schriftlich einverstanden erklärten. Diese Einwilligung muss den Voraussetzungen des § 4 Abs. 2 und 3 ThürDSG entsprechen, das heißt in der regelmäßig schriftlichen Einwilligungserklärung muss deutlich gemacht werden, welche Daten zu welchem Zweck erhoben werden und an welche Stelle sie zu welchem Zweck übermittelt werden. Mit dieser Auskunft zeigte sich die LZÄkTh zufrieden.

Die Übermittlung von personenbezogenen Daten der Mitglieder der LZÄKTh zur gezielten Versendung von Werbebeilagen in einer Verbandszeitschrift ist nicht für die originären Aufgaben des Verbandes erforderlich. Für einen derartigen Zweck dürfen Daten nur an Dritte übermittelt werden, wenn sich die Mitglieder der LZÄKTh schriftlich damit einverstanden erklären und vorher detailliert dargelegt wird, welche Daten zu welchem Zweck erhoben und an welche Stelle übermittelt werden dürfen.

12.8 Wenn das Amt die Miete zahlt – der Vermieter erfährt alles, oder?

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) ist zuständige Kontrollbehörde für die Bundesagentur für Arbeit. In dieser Funktion hat die BfDI die Landesbeauftragten für den Datenschutz auf ein Datenschutzproblem im Zusammenhang mit der Abtretung von Rückzahlungsansprüchen bei Mietkautionsdarlehen aufmerksam gemacht. Auf der Grundlage der bereits 2004 in Kraft getretenen Verordnung zur Zulassung von kommunalen Trägern als Träger der Grundsicherung für Arbeitsuchende wurden in Thüringen vier sogenannte Optionskommunen bestimmt, die seit 2012 die Aufgaben der Grundsicherung für Arbeitsuchende in Eigenregie übernommen haben. Als Thüringer kommunale Stellen unterliegen diese der Kontrollzuständigkeit des TLfDI nach § 37 Thüringer Datenschutzgesetz (ThürDSG). Den Hinweis der BfDI hat der TLfDI zum Anlass genommen, die Praxis der seiner Kontrolle unterliegenden Jobcenter der Landkreise Eichsfeld, Schmalkalden-Meiningen und Greiz sowie der kreisfreien Stadt Jena zu hinterfragen. Das datenschutzrechtliche Problem gestaltete sich folgendermaßen: Die kommunalen Träger der gemeinsamen Einrichtungen sind befugt, Weisungen zu erlassen, durch die das Verfahren zur Gewäh-

rung von Mietkautionsdarlehen (§ 22 Absatz 6 SGB II) geregelt wird. Durch die Weisung kann zwingend bei der Gewährung eines Mietkautionsdarlehens die Abtretung des Rückzahlungsanspruchs der Mietkaution an das Jobcenter vorausgesetzt werden. Die Abtretung wird aber nur dann zum gesicherten Anspruch des Jobcenters, wenn dieser Anspruch dem Vermieter bekannt gegeben wird, ansonsten besteht unter Umständen die Gefahr, dass dieser die Kaution an den Mieter auszahlt und das Geld dann weg ist. Mit der Information über den Abtretungsanspruch wird aber dem Vermieter der staatliche Leistungsbezug des betroffenen Mieters bekannt gegeben. Eine Rechtsgrundlage für diese Datenübermittlung besteht jedoch nicht. Im Sozialgesetzbuch (SGB) Zweites Buch (II) ist die Absicherung des Mietkautionsdarlehens nicht vorgesehen. Jedoch stellt die Zusicherung des Jobcenters, dass es die Mietkaution übernimmt, nach § 22 Abs. 6 SGB II gleichzeitig eine Anspruchsvoraussetzung für die spätere Übernahme dieser Kosten dar (vgl. BSG, Urteil v. 7. November 2006 – Az. B 7b 10/06).
Nach Ansicht des TLfDI ist eine Abtretung des Rückzahlungsanspruchs als Voraussetzung für den Erhalt der Mietkaution nur in begrenzten Einzelfällen zulässig. Dies ist dann der Fall, wenn das Jobcenter objektiv darlegen kann, dass aufgrund der Umstände des Einzelfalles die Rückzahlung des Darlehens angezweifelt wird und die Sicherung des Darlehens nicht bereits auf andere Weise sichergestellt werden kann, beispielsweise durch die monatliche Aufrechnung in Form des anteiligen Einbehalts eines Betrages bei der Auszahlung der Sozialleistung an den Empfänger der Grundsicherung. § 42a SGB II sieht ausdrücklich die Aufrechnungsmöglichkeit vor. Auf die Nachfrage des TLfDI, wie dieser Sachverhalt im Zuständigkeitsbereich der vier Thüringer Jobcenter geregelt ist, teilten diese mit, dass sie die Abtretung des Rückzahlungsanspruchs der Mietkaution zum Zwecke der Sicherung eines möglichen Darlehensrückzahlungsanspruches gegenüber dem Leistungsempfänger nicht fordern. Verstöße gegen datenschutzrechtliche Vorschriften waren somit nicht festzustellen.

Vier Kommunen in Thüringen leisten Aufgaben der Grundsicherung für Arbeitsuchende in Eigenregie. Diese Kommunen haben eigene Regelungen zur Abtretung von Rückzahlungsansprüchen bei Mietkautionsdarlehen gemäß SGB II erlassen, um die Rückzahlung der

Darlehen abzusichern. Gegen die einzelnen Regelungen hatte der TLfDI keine datenschutzrechtlichen Bedenken.

12.9 Reha-Entlassungsbericht: Daten an den MDK?

Das Thüringer Ministerium für Arbeit, Soziales, Gesundheit, Frauen und Familie (TMASGFF) ist Aufsichtsbehörde für den Medizinischen Dienst der Krankenkassen (MDK).
Im Januar 2017 bat das TMASGFF den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) um eine Stellungnahme, ob bzw. inwiefern die Übermittlung von Reha-Entlassungsberichten an den MDK einer Einwilligung der betroffenen Patienten bedarf.
Reha-Entlassungsberichte enthalten sensible medizinische Daten, das heißt besonders schutzwürdige Sozialdaten. Als gesetzliche Grundlage für eine Übermittlung an den MDK durch den Träger der Rentenversicherung kommt § 69 Abs. 1 Sozialgesetzbuch (SGB) Zehntes Buch (X) in Verbindung mit § 76 SGB X infrage. Eine Übermittlung ohne Einwilligung setzt nach § 76 Abs. 2 Nr. 1 SGB X voraus, dass der Reha-Entlassungsbericht eine „Begutachtung wegen der Erbringung von Sozialleistungen“ darstellt. Nach Ansicht der Rentenversicherungsträger stellt der Entlassungsbericht jedoch keine derartige Begutachtung dar, sodass er nicht nach § 76 Abs. 2 SGB X weitergeleitet werden könne. Daher sei eine Schweigepflichtentbindung entsprechend § 76 Abs. 1 SGB X zwingend erforderlich.
Zu dieser Frage bestehen unterschiedliche Rechtsauffassungen. Die Mehrheit der Aufsichtsbehörden ist der Ansicht, dass die Einwilligung der Betroffenen zwingend erforderlich ist. Andere hingegen sehen für die Einwilligung keine Notwendigkeit.
Nach Prüfung des dargelegten Sachverhalts gelangte auch der TLfDI zu der Auffassung, dass die vollständige Übermittlung von Reha-Entlassungsberichten an den Medizinischen Dienst der Krankenkassen nicht zulässig ist und die betroffenen Patienten in die Übermittlung einwilligen müssen. Weiterhin wies der TLfDI das TMASGFF darauf hin, dass nach SGB Fünftes Buch (V) in Fällen der teilweisen Übermittlung jeweils eine Einzelprüfung erforderlich sei, inwiefern der Bericht für die Arbeit des MDK erforderlich ist. Diese Fälle sind abschließend im SGB V geregelt.

Betroffene Patienten müssen einer Übermittlung von Reha-Entlassungsberichten an den Medizinischen Dienst der Krankenkassen grundsätzlich zustimmen.

12.10 Löschungsresistente Daten im Gesundheitsamt – Teil 2

In seinem 11. Tätigkeitsbericht zum nicht-öffentlichen Bereich informierte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) unter Nummer 11.29 über „Löschungsresistente Daten im Gesundheitsamt“. Dabei ging es um ein Softwareprogramm, das in Thüringer Gesundheitsämtern beispielsweise im Rahmen von Einschulungsuntersuchungen zum Einsatz kommt. Problematisiert wurde, dass bei diesem System keine Löschung von hochsensiblen Patientendaten erfolgt. Auch seien Zugriffe auf eine sogenannte Zentralkartei uneingeschränkt möglich. Bereits im vergangenen Berichtszeitraum hatte der TLfDI versucht, auf einen datenschutzgerechten Einsatz hinzuwirken, wobei sich die Gesundheitsämter demgegenüber sehr aufgeschlossen zeigten. Festgestellt wurde, dass insgesamt eine große Unsicherheit in Bezug auf die Notwendigkeit des Löschens von Daten im Gesundheitsamt besteht.
Nach § 16 Thüringer Datenschutzgesetz (ThürDSG) sind personenbezogene Daten zu löschen, wenn ihre Speicherung unzulässig ist oder ihre Kenntnis bei der Daten verarbeitenden Stelle zur Erfüllung ihrer Aufgaben nicht mehr erforderlich ist. Stehen einer Löschung entweder schutzwürdige Interessen des Betroffenen oder gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegen, sind die Dateien zu sperren. Das bedeutet, dass sie derart gekennzeichnet werden müssen, dass eine weitere Verarbeitung oder Nutzung nur sehr eingeschränkt möglich ist, § 3 Abs. 3 Nr. 5 ThürDSG. Für das Gesundheitsamt würde dies bedeuten, dass die Daten in diesem Fall unter Verschluss genommen werden, bevor sie vor der Löschung nach den geltenden archivrechtlichen Vorschriften dem zuständigen Archiv angeboten werden.
Wie der TLfDI in seinem Tätigkeitsbericht angekündigt hat, hat er in diesem Berichtszeitraum die Datenverarbeitung von einem Gesundheitsamt eines Landratsamtes vor Ort geprüft. Dort wurden zunächst alle Aufgaben eruiert, die das Gesundheitsamt mit diesem Programm wahrnimmt:

Die Betreuungsbehörde des Gesundheitsamtes beschäftigt sich mit dem Betreuungsverfahren. Aufgabe des Gesundheitsamtes ist dabei vor allem, Sachberichte für das Gericht in Betreuungsverfahren zu erstellen. Im Verfahren ist kein Arzt beteiligt, es befinden sich aber ärztliche Befunde in den Fachakten für die Vorlage an das Gericht, das über die Betreuung entscheidet. Weiterhin gibt es den sozialpsychiatrischen Dienst, in dem Sozialarbeiter und Ärzte beschäftigt sind. Diese werden auf Anregung Dritter (Privatpersonen oder Behörden) tätig, um beispielsweise Unterbringungsverfahren einzuleiten, die Nachsorge nach einer Unterbringung zu betreuen bzw. um eine erste Hilfe in prekären Lebenssituationen zu geben. Der Bereich „Hygiene“ beschäftigt sich mit dem Infektionsschutz. Ärzte sowie Gemeinschaftsunterkünfte wie Schulen und Kindergärten sind nach dem Infektionsschutzgesetz verpflichtet, bestimmte Krankheiten an das Gesundheitsamt zu melden. In diesen Fällen wird das Gesundheitsamt beratend tätig, spricht gegebenenfalls ein Tätigkeitsverbot aus und gibt allgemeine Hinweise. Ärzte sind in dem Verfahren in der Regel nicht tätig. Im amtsärztlichen Dienst sind Ärzte tätig, sie begutachten Beamte, führen Drogenscreenings und Vaterschaftstests durch, machen HIV-Tests und sind für die Betreuung von Asylbewerbern im Rahmen der erforderlichen Impfungen zuständig. Dieses Sachgebiet arbeitet nicht mit dem in Rede stehenden Programm. Schließlich gibt es noch den Kinder- und Jugendärztlichen Dienst/Zahnärztlichen Dienst. Dieser führt Reihenuntersuchungen an den Schulen und Kindergärten sowie die Schuleingangsuntersuchungen durch.

Festgestellt wurde zunächst, dass es mittlerweile bei der Arbeit mit dem geprüften Programm möglich ist, Daten zu löschen. Auch wird die sogenannte Zentralkartei inzwischen datenschutzgerecht genutzt. Es ist nicht möglich, zentral alle Adressen im System einzusehen.

Es gibt eine Archivordnung des Landratsamtes, an dem das Gesundheitsamt angesiedelt ist. Für bestimme Daten gibt es im Landratsamt einen internen Aufbewahrungsraum sowie eine Zwischenlagerung im Gesundheitsamt. Aus der Darstellung der verschiedenen Sachgebiete wird deutlich, dass im Gesundheitsamt die unterschiedlichsten Arten von Daten zu den vielfältigen Zwecken geführt und aufbewahrt werden. Der TLfDI ist nun dabei, aus den erhobenen Informationen eine Handreichung zu Löschfristen im Gesundheitsamt unter Berücksichtigung der verschiedenen Aufbewahrungsfristen für die unterschiedlichen Kategorien von Daten zu erarbeiten. Hierzu wird

er sich auch mit dem fachlich zuständigen Thüringer Ministerium für Arbeit, Soziales, Gesundheit, Frauen und Familie ins Benehmen setzen.

Personenbezogene Daten sind zu löschen, wenn ihre Speicherung unzulässig oder ihre Kenntnis für die Daten verarbeitende Stelle zur Erfüllung ihrer Aufgaben nicht mehr erforderlich ist, § 16 ThürDSG. Wenn noch Aufbewahrungsfristen bestehen, sind die Daten nicht zu löschen sondern zunächst zu sperren. Werden in einer Daten verarbeitenden Stelle verschiedene Kategorien von Daten verarbeitet, ist es oft nicht einfach, allerdings notwendig, festzustellen, für welche Arten von Daten welche Aufbewahrungsfristen gelten.

12.11 Alte Arztstempel – die Lizenz zur Rezeptausstellung?

Die Landesapothekerkammer Thüringen wurde von der Kassenärztlichen Vereinigung über einen für ungültig erklärten ärztlichen Abrechnungsstempel informiert und beabsichtigte, diese Information an die Apotheken weiterzuleiten, um die Einlösung entsprechender Rezepte zu verhindern. Mit der Weiterleitung würden jedoch auch die Daten des betreffenden Arztes weitergegeben. Daher bat die Apothekerkammer den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) um Auskunft, inwieweit und unter welchen Bedingungen Informationen über Rezeptfälschungen und ungültige Abrechnungsstempel an die Apotheken weitergeleitet werden können.
Gemäß § 2 Abs. 2 gilt das Thüringer Datenschutzgesetz (ThürDSG) sowohl für die Kassenzahnärztliche Vereinigung Thüringen als auch für die Landesapothekerkammer, da beide Körperschaften des öffentlichen Rechts sind. Die Information von Apotheken durch die Apothekerkammer ist jedoch eine Datenübermittlung an Stellen außerhalb des öffentlichen Bereichs, denn Apotheken sind private Unternehmen. Die Zulässigkeit einer derartigen Datenübermittlung ist in § 22 ThürDSG geregelt.
Voraussetzung für die Weitergabe dieser Information ist zunächst, dass deren Übermittlung notwendig ist, damit die Apothekerkammer die ihr obliegenden Aufgaben ordnungsgemäß erfüllen kann. Außerdem müssen die Voraussetzungen des § 20 ThürDSG vorliegen. Die Daten müssen danach grundsätzlich für den Zweck der Übermittlung erhoben worden sein. Die Daten über den ungültigen Zahn-

arztstempel wurden vermutlich nicht zu dem Zweck erhoben, die Apotheken über die Ungültigkeit des Stempels zu informieren. Daher muss ein Fall der zulässigen Zweckänderung nach § 20 Abs. 2 ThürDSG vorliegen.
Nach § 20 Abs. 2 Nr. 6 ThürDSG können die Daten für einen anderen Zweck verwandt werden, wenn dies zur Abwehr erheblicher Nachteile für das Allgemeinwohl oder einer sonst unmittelbar drohenden Gefahr für die öffentliche Sicherheit erforderlich ist. Das Gesundheitssystem, dem auch die Apotheken angehören, soll nicht nur das missbräuchliche Erlangen und Verwenden von Medikamenten verhindern, sondern es soll auch die Versicherungsgemeinschaft vor unzulässigen Belastungen schützen. Diese Aufgabe können die Apotheken als Ausgabestellen für Medikamente nur dann erfüllen, wenn die Gültigkeit eines Rezeptes eindeutig belegt ist. Ein gültiger Arztstempel ist Voraussetzung für ein gültiges Rezept. Daher kann die Übermittlung der Information über ungültige ärztliche Abrechnungsstempel als erforderlich im Sinne des § 20 Abs. 2 Nr. 6 ThürDSG angesehen werden. Darüber informierte der TLfDI die Apothekerkammer Thüringen.

Die Landesapothekerkammer kann die Apotheken über ungültige (zahn-)ärztliche Abrechnungsstempel informieren, da die Weitergabe dieser Information im Sinne des § 20 Abs. 2 Nr. 6 ThürDSG für die Abwehr erheblicher Nachteile für das Allgemeinwohl oder einer sonst unmittelbar drohenden Gefahr für die öffentliche Sicherheit erforderlich ist.

12.12 Urkundenverifikationsdienst Approbationsurkunden

Bereits im 11. Tätigkeitsbericht berichtete der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) über den Einsatz einer Technik zur Verifikation von Approbationsurkunden von Ärzten und Fachkräften in Pflegeberufen. Es ging dabei darum, dass Patienten die Echtheit einer Approbationsurkunde eines Arztes prüfen können, ohne sich an die Landesärztekammer Thüringen wenden zu müssen. Das Verfahren läuft wie folgt ab: Seit 2016 stellt das Thüringer Landesverwaltungsamt Approbationsurkunden mit einen QR-Code versehen aus. Ein QR-Code (von Quick Response) ist ein zweidimensionales Bild, in dem bestimmte Informationen hinterlegt sind. Diese können mithilfe eines sogenann-

ten QR-Code-Scanners abgerufen werden, der beispielsweise als App auf das Smartphone geladen werden kann. Besitzer eines Smartphones können den QR-Code auf diesen „neuen“ Urkunden scannen, der einen 64-stelligen Code (Buchstaben und Zahlen) enthält, mit welchem jede Person mit Internetzugang auf dem Portal https://www.kammerservice.de unter Eingabe dieses Codes die Echtheit der Urkunde prüfen kann.



Bereits im letzten Tätigkeitbericht wurde berichtet, dass das Verfahren zur Generierung des 64-stelligen Codes den Datenschutzanforderungen entspricht. Im aktuellen Berichtszeitraum hatte der TLfDI weiterhin geprüft, wer Zugriff auf die Daten der Urkunden hat und wie diese vor Veränderung geschützt sind. Da die Landesärztekammer Thüringen, welche das Verifikationsportal mit anderen Ärztekammern in Deutschland betreibt, nicht die Stelle ist, die Urkunden selbst ausstellt, werden nur digitale Kopien des Urkundeninhalts bereitgestellt.

Wichtig aus datenschutzrechtlicher Sicht war, dass bei Übertragung der Kopien keine Datenveränderung durch Unbefugte (Hacker, böswillige Angestellte) stattfinden kann und das zum zweiten eine Sicherung der Daten gegen Zerstörung (auch hier durch Hacker bzw. technisches Versagen der Rechentechnik) gegeben ist.

Zum ersten Punkt der Sicherstellung der Integrität der Daten hat der TLfDI eine Lösung mit dem Thüringer Landesverwaltungsamt und der Landesärztekammer Thüringen abgestimmt und Verbesserungsvorschläge eingebracht, wie die zu übermittelnden Daten zusätzlich zum Übertragungsweg sicher verschlüsselt werden können. Zum zweiten Punkt (Schutz vor Datenverlust) trägt das Thüringer Landesverwaltungsamt die Verantwortung für die Richtigkeit der Urkundendaten. Hier muss dem TLfDI zurzeit noch ein schlüssiges Konzept zur Datensicherung nachwiesen werden.

Jede öffentliche Stelle bzw. nicht-öffentliche Stelle ist verpflichtet, beim Umgang mit personenbezogenen Daten in technischen Systemen die Daten vor unerlaubter Manipulation und vor Datenverlust zu schützen. Dabei kann es je nach Schutzbedarf der betroffenen Daten erforderlich sein, nicht nur den Übertragungsweg bei einer Übermittlung zu verschlüsseln, sondern auch die Daten selbst.

12.13 Qualität versus Datenschutz im Gesundheitswesen?

Die Landesgeschäftsstelle für Qualitätssicherung (LQS) ist eine Einrichtung des Landes Thüringen und handelt in dessen Auftrag. Sie nimmt auf Landesebene die Aufgaben ihrer Vertragspartner (Landeskrankenhausgesellschaft und Verbände der Krankenkassen) wahr zur Umsetzung der externen stationären Qualitätssicherung. Die LQS hat ihren Sitz bei der Landesärztekammer Thüringen, ist jedoch organisatorisch, fachlich und finanziell unabhängig. Ihre Mitarbeiterinnen und Mitarbeiter stehen in einem dienstrechtlichen Verhältnis mit der Landesärztekammer und sind somit Angestellte der Kammer. Die Umsetzung des Verfahrens zur externen stationären Qualitätssicherung wird in der Richtlinie über Maßnahmen der Qualitätssicherung in Krankenhäusern (QSKH-RL) geregelt.
Die LQS bat den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) um eine fachliche datenschutzrechtliche Einschätzung zu folgendem Sachverhalt:
Auf der Grundlage des § 136 Absatz I SGB V i. V. mit § 136c Absatz I und Absatz 2 SGB V hatte der Gemeinsame Bundesausschuss (G-BA) im Dezember 2016 die Richtlinie zu planungsrelevanten Qualitätsindikatoren (PlanQI-RL) beschlossen. Nach § 9 Abs. 5 dieser Richtlinie werden die Landesgeschäftsstellen für Qualitätssicherung damit beauftragt, die durch die Krankenhäuser im Verfahren gemäß QSKH-RL dokumentierten Qualitätssicherungsdaten zu validieren. Diese Validierung sollte durch direkte Akteneinsicht erfolgen. Somit erhalte die LQS Einsicht in Patientenunterlagen, obwohl sie ausschließlich patientenanonymisierte Daten zur Qualitätssicherung erhebt und überprüft.
Die LQS vertrat die Auffassung, dass die geforderte Validierung nicht gegen bestehende datenschutzrechtliche Normen verstoße. Sie berief sich hierfür auf § 2 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG). Danach sei die LQS eindeutig als öffentliche Stelle zu definieren, sodass sie personenbezogene Daten gemäß §§ 19 Abs. 1 und 2 sowie 20 Abs. 1 ThürDSG nutzen dürfe. Öffentliche Stellen dürfen personenbezogene Daten nutzen, wenn eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt, die Nutzung dieser Daten zur Erfüllung der festgelegten Aufgabe erforderlich ist und für die Zwecke erfolgt, für die die Daten erhoben worden sind – im Falle der LQS für die Qualitätssicherung. Weiterhin sei die Validierung

durch das Thüringer Krankenhausgesetz (ThürKHG) gedeckt. Gemäß § 27 Abs. 6 Nr. 4 ThürKHG ist die Übermittlung von Patientendaten an Personen außerhalb des Krankenhauses zur Durchführung von qualitätssichernden Maßnahmen in der Krankenversorgung legitim, wenn bei der beabsichtigten Maßnahme das Interesse der Allgemeinheit größer ist als die schutzwürdigen Belange der Patienten. Somit sah die LQS sowohl in ihrem Bereich als auch das Krankenhaus betreffend alle Voraussetzungen erfüllt, um das Datenvalidierungsverfahren gemäß PlanQI-RL durchzuführen. Zur Bestätigung ihrer Sichtweise bat die LQS den TLfDI jedoch um eine datenschutzrechtliche Einschätzung.

Der TLfDI bestätigte der LQS ihren juristischen Status als öffentliche Stelle gemäß § 2 Abs. 2 Satz 1 ThürDSG. Jedoch konnte der TLfDI anhand der Darlegungen der LQS keine Einschätzung darüber abgeben, inwiefern nach § 27 Abs. 2 Nr. 4 ThürKHG die Voraussetzungen für die Übermittlung von Patientendaten gegeben sind und deren Erhebung tatsächlich für die von der LQS wahrgenommenen Aufgaben erforderlich ist. Weiterhin gab der TLfDI zu bedenken, dass fraglich sei, warum für die beabsichtigte Validierung das Interesse der Allgemeinheit die schutzwürdigen Belange der betroffenen Patienten erheblich überwiegt. Nach Ansicht des TLfDI kann dies nicht grundsätzlich für alle qualitätssichernden Maßnahmen gelten, sonst hätte der Gesetzgeber die Aufgaben der Qualitätssicherung nicht unter den Vorbehalt dieser Rechtsgüterabwägung gestellt. Daher muss in jedem Einzelfall dargelegt werden, warum gerade diese Durchführung von qualitätssichernden Maßnahmen die Voraussetzungen des § 27 Abs. 5 Nr. 4 ThürKHG erfüllt. Ob die Voraussetzung eines erheblichen Interesses der Allgemeinheit nach § 27 Abs. 2 Nr. 4 ThürKHG gegeben ist, muss fachlich entschieden werden. Zur Klärung dieser Frage empfahl der TLfDI der LQS, sich mit dem Thüringer Ministerium für Arbeit, Soziales, Gesundheit, Frauen und Familie (TMASGFF) in Verbindung zu setzen.

Weiterhin wies der TLfDI die LQS darauf hin, dass auch unter den Voraussetzungen des § 27 Abs. 2 Nr. 4 ThürKHG nur in möglichst geringem Maße in die Rechte der Betroffenen eingegriffen werden darf. Dies muss durch technische und organisatorische Maßnahmen sichergestellt werden. In diesem Zusammenhang sollten die betroffenen Krankenhäuser vorab gefragt werden, ob auch die Möglichkeit besteht, anonymisierte Patientenunterlagen einzusehen. Weiterhin müssen die Personen, die vor Ort die Patientenunterlagen

tatsächlich einsehen, nach § 6 ThürDSG auf das Datengeheimnis verpflichtet werden. Darüber hinaus muss sichergestellt werden, dass die beauftragten Personen nur anonymisierte Patientendaten an die für die Validierung zuständigen Stellen weitergeben.

Für die Frage, ob die Einsichtnahme in Patientenakten im Krankenhaus zu Zwecken der Qualitätssicherung zulässig ist, ist in Thüringen § 27 Abs. 2 Nr. 4 des Thüringer Krankenhausgesetzes (ThürKHG) einschlägig. Danach ist eine Einsichtnahme in Patientendaten nur zulässig, wenn sie für qualitätssichernde Maßnahmen in der Krankenversorgung erforderlich ist und wenn für diese Maßnahmen das Interesse der Allgemeinheit die schutzwürdigen Belange der Betroffenen erheblich überwiegt.

12.14 Telemedizin: Datenschützer begleiten Nutzung der Gesundheitskarte für elektronische Patientenakte

Das Thüringer Ministerium für Arbeit, Soziales, Gesundheit, Frauen und Familie (TMASGFF) informierte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) darüber, dass im Rahmen der Zusammenarbeit mit dem Thüringer Ministerium für Wirtschaft, Wissenschaft und digitale Gesellschaft (TMWWDG) ein großes Projekt zur Telemedizin geplant sei. Hierfür sollte eine interministerielle Arbeitsgruppe gebildet werden und eine entsprechende „Kickoff"-Veranstaltung stattfinden. Das TMASGFF bat den TLfDI um fachliche Unterstützung bei datenschutzrechtlichen Fragen im Rahmen der Erarbeitung des Projekts „Errichtung eines telemedizinischen Zentrums". Der TLfDI sicherte dem TMASGFF seine Unterstützung zu.
Unter Beteiligung des TLfDI initiierte das TMASGFF die Gründung einer Arbeitsgruppe zur Entwicklung und Einführung telemedizinischer Projekte in Thüringen. Im Rahmen eines entsprechenden Informationsaustauschs übersandte das TMASGFF dem TLfDI auch Anmerkungen zur elektronischen Patientenakte und bat um eine datenschutzrechtliche Bewertung im Hinblick auf die Patientensicherheit. Gemäß § 9 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) haben „öffentliche Stellen, die (…) personenbezogene Daten verarbeiten, (…) die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Bestimmungen [des ThürDSG] zu gewährleisten."

In seiner datenschutzrechtlichen Prüfung legte der TLfDI dar, dass die Gesellschaft für Telematikanwendungen der Gesundheitskarte (gematik) nach § 291a Abs. 5c Sozialgesetzbuch (SGB) Fünftes Buch (V) bis zum 31. Dezember 2018 die erforderlichen Voraussetzungen dafür schaffen muss, dass Daten über den Patienten in einer elektronischen Patientenakte nach § 291a Abs. 3 Satz 1 Nr. 4 SGB V dieser Vorschrift bereitgestellt werden können. Danach soll die elektronische Patientenakte Befunde, Diagnosen, Therapiemaßnahmen, Behandlungsberichte und Impfdaten enthalten, die für eine fall- und einrichtungsübergreifende Dokumentation über den Patienten genutzt werden. § 291a Abs. 5 SGB V legt fest, dass das Erheben, Verarbeiten und Nutzen von Daten mittels der elektronischen Gesundheitskarte in der Regel nur mit dem Einverständnis des Versicherten zulässig ist. Durch technische Vorkehrungen muss gewährleistet werden, dass der Zugriff nur durch die Autorisierung der Versicherten möglich ist. Nach § 291a Abs. 5c Satz 2 müssen die technischen und organisatorischen Verfahren geeignet sein, diese Daten entsprechend verfügbar zu machen.
Der Zugriff auf diese Daten mittels elektronischer Gesundheitskarte darf nur in Verbindung mit einem elektronischen Heilberufsausweis erfolgen. Der Ausweis muss über die Möglichkeit zur sicheren Authentifizierung und über eine qualifizierte elektronische Signatur verfügen.
Der TLfDI legte dar, dass sich der Gesetzgeber bewusst dafür entschieden habe, einen Zugriff für Versicherte nur für die Daten zuzulassen, die sie selbst dort einstellen können. In der Gesetzesbegründung wird dazu ausgeführt: „Das Patientenfach bietet (…) den Versicherten die Möglichkeit, für sie bestimmte Datensammlungen, (…) beispielsweise Daten über durchgeführte Impfungen oder Daten des (…) Mutterpasses, im Sinne eines elektronischen Impf- oder Mutterpasses dort einstellen zu lassen.“ Nach den derzeitigen Regelungen ist der Zugriff nur zusammen mit einem elektronischen Heilberufsausweis z. B. an einem Terminal in der Arztpraxis oder mittels einer eigenen Signaturkarte des Versicherten mit qualifizierter elektronischer Signatur zulässig. In der Regel verfügen Versicherte jedoch nicht über entsprechende Signaturkarten und andererseits gibt es andere technische Verfahren zur sicheren Authentifizierung. Im Hinblick darauf soll die Zugriffsmöglichkeit der Versicherten auf das Patientenfach durch geeignete technische Verfahren zur Authentifizierung verbessert werden (Bundestagsdrucksache 18/5293 Seite 45,

Gesetz für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen sowie zur Änderung weiterer Gesetze vom 1. Dezember 2015 – E-Health-Gesetz).

Im Juni 2017 veröffentlichte die gematik ein sogenanntes Interoperabilitätsverzeichnis im Internet (https://www.vesta-gematik.de). Das Verzeichnis soll die dringend notwendige Zusammenarbeit und Kompatibilität zwischen unterschiedlichen, im Gesundheitswesen verwendeten IT-Systemen verbessern. Das Verzeichnis mit dem Namen „vesta“ etabliert bundeseinheitliche Standards, Profile und Leitfäden für Informations- und Kommunikationstechnologien im deutschen Gesundheitswesen. Vesta ist verbindlich für alle Unternehmen, die technische Lösungen für Telemedizin oder Gesundheits-IT auf den Markt bringen wollen; sie können die Aufnahme eines IT-Standards in das Verzeichnis beantragen. Der gesetzliche Auftrag zum Aufbau eines solchen Verzeichnisses und des zugehörigen Informationsportals ist im § 291e Abs. 1 SGB V festgeschrieben.

Auch das TMASGFF stand Forderungen, die Zugriffsrechte auf die personenbezogenen medizinischen Daten der Gesundheitskarte noch mehr im Sinne der Patientinnen und Patienten zu regeln, positiv gegenüber und beabsichtigt, eine Machbarkeitsstudie für den Aufbau eines Telemedizinischen Zentrums in Thüringen zu erstellen. Hierfür wurde durch das TMASGFF eine Arbeitsgruppe eingerichtet, der der TLfDI ebenfalls angehört.

Die medizinischen Daten auf der elektronischen Gesundheitskarte sind besonders sensible personenbezogene Daten. Gemäß § 9 Abs. 1 ThürDSG haben „öffentliche Stellen, die (…) personenbezogene Daten verarbeiten, (…) die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Bestimmungen [des ThürDSG] zu gewährleisten.“ Dies gilt nach dem E-Health-Gesetz umso mehr für die Entwicklung und Nutzung einer elektronischen Patientenakte mit umfassenden medizinischen Daten zu Befunden, Impfungen und Diagnosen. Unter der Federführung des TMASGFF wurde in Thüringen eine Arbeitsgruppe gebildet, die mit der Erstellung einer Machbarkeitsstudie für den Aufbau eines Telemedizinischen Zentrums in Thüringen befasst ist. Eine

wesentliche Rolle hierbei spielt der Umgang mit der elektronischen Patientenakte. Der TLfDI ist Mitglied der Arbeitsgruppe und begleitet das Projekt aus datenschutzrechtlicher Sicht.

12.15 Wenn die Konfession für die stationäre Aufnahme im Klinikum entscheidend ist

Ein Patient beschwerte sich beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) über ein Thüringer Klinikum in öffentlicher Hand. Der Beschwerdeführer legte dar, dass bei seiner stationären Aufnahme in einem Thüringer Klinikum neben der Abfrage von persönlichen Daten, auch die Auskunft über den Familienstand, die Konfessionszugehörigkeit und Vornamen des Ehepartners verlangt wurden. Dem Patienten wurde mitgeteilt, das Erfassungsprogramm verlange zwingend die Informationen, ansonsten sei keine weitere Eingabe und Erfassung der Daten möglich.
Gemäß § 37 Thüringer Datenschutzgesetz (ThürDSG) kontrolliert der TLfDI bei allen öffentlichen Stellen die Einhaltung der Bestimmungen über den Datenschutz. Daher bat der TLfDI das Klinikum um eine Stellungnahme zum Sachverhalt. Nach § 27 Abs. 3 Nr. 1 Thüringer Krankenhausgesetz (ThürKHG) dürfen Patientendaten „nur erhoben, gespeichert, verändert oder sonst genutzt werden, soweit dies zur Erfüllung der Aufgaben des Krankenhauses oder im Rahmen des krankenhausärztlichen Behandlungsverhältnisses erforderlich ist …“. Dem TLfDI war nicht ersichtlich, inwiefern u. a. die Konfessionszugehörigkeit für die Behandlung im Krankenhaus von Bedeutung ist.
Das Klinikum teilte mit, dass für die stationäre Aufnahme von Patienten mittels Erfassungsprogramm die Eingabe des Familienstandes, der Konfessionszugehörigkeit und vom Vornamen des Ehepartners nicht zwingend erforderlich sind. Die aufnehmende Mitarbeiterin des Klinikums habe diese Angaben versehentlich für zwingend erforderlich gehalten. Die Leiterin der stationären Aufnahme habe sich daher bereits bei dem betroffenen Patienten und Beschwerdeführer entschuldigt. Im Anschluss an das Gespräch mit der Aufnahmeleiterin stimmte der betroffene Patient der Angabe einer Kontaktperson zu, für deren Identifikation auch die Angabe des Vornamens erforderlich ist.

Weiterhin teilte das Klinikum mit, dass im Zusammenhang mit der Beschwerde des Patienten die Abläufe in der stationären Aufnahme im Hinblick auf die Einhaltung des Datenschutzes nochmals überprüft und die Mitarbeiter hierüber aufgeklärt und belehrt wurden. Dies begrüßte der TLfDI ausdrücklich und betrachtete die Angelegenheit damit datenschutzrechtlich als erledigt.
Dem Beschwerdeführer teilte der TLfDI mit, dass die Abläufe in der stationären Aufnahme des Klinikums im Hinblick auf die Einhaltung des Datenschutzes nochmals überprüft und die Mitarbeiter entsprechend belehrt worden seien, um derartige Fehlinformationen in Zukunft zu vermeiden. Da es sich um die Fehleinschätzung einer einzelnen Person handelte und das Krankenhaus sofort tätig wurde, sah der TLfDI von einer Beanstandung ab.

Nach § 27 Abs. 3 Nr. 1 Thüringer Krankenhausgesetz (ThürKHG) dürfen Patientendaten „nur erhoben, gespeichert, verändert oder sonst genutzt werden, soweit dies zur Erfüllung der Aufgaben des Krankenhauses oder im Rahmen des krankenhausärztlichen Behandlungsverhältnisses erforderlich ist …“. Naturgemäß sind für die fachliche medizinische Behandlung Daten über die Konfessionszugehörigkeit, den Vornamen des Ehepartners und den Familienstand nicht erforderlich.

12.16 Auch wenn sich alle Beteiligten kennen: Datenschutz nicht vergessen!

Wenn sich die Beteiligten in einem Verwaltungsverfahren dienstlich und/oder privat kennen, muss dennoch den datenschutzrechtlichen Vorschriften Rechnung getragen werden. Welche Konsequenzen eine Vermischung von Dienstlichem und Privatem haben kann, zeigt folgender Fall:
Die Beschwerdeführerin, eine Bedienstete eines Landratsamtes war von einem Familienangehörigen bevollmächtigt, dessen Angelegenheiten im Zusammenhang mit der Schwerbehinderung wahrzunehmen. Für die Schwerbehindertenangelegenheiten war eine andere Kommune zuständig, gegen die die Beschwerdeführerin in Wahrnehmung ihrer Bevollmächtigung eine Dienstaufsichtsbeschwerde eingereicht hatte. Sie wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), weil sie von ihrer Dienstvorgesetzten auf die Angelegenheit ange-

sprochen wurde. Das konnte sie sich nur damit erklären, dass das sie beschäftigende Landratsamt von der die Schwerbehindertenangelegenheiten wahrnehmenden Kommune Informationen über sie, den Schwerbehinderten und die eingereichte Dienstaufsichtsbeschwerde erhalten haben musste. Die Übermittlung personenbezogener Daten ist nach § 21 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) zulässig, wenn sie zur Erfüllung der in der Zuständigkeit der übermittelten Stelle oder des Dritten liegenden Aufgaben erforderlich ist und die Voraussetzungen vorliegen, die eine § 20 ThürDSG zulassen würden. Zu klären war daher, ob eine Übermittlung der Tatsachen, dass ein Familienangehöriger schwerbehindert ist, von der Beschwerdeführerin erfolgte und diese eine Dienstaufsichtsbeschwerde eingereicht hatte.

Auf Anfrage des TLfDI teilte die für Schwerbehindertenangelegenheiten zuständige Kommune dem TLfDI mit, die Beschwerdeführerin habe einen Antrag auf Einsicht in die Schwerbehindertenakte ihres Familienangehörigen gestellt, mit der Maßgabe, dass die Akte zum Zweck der Einsicht zu ihrer Beschäftigungsbehörde übersandt werde. Damit habe sie zumindest konkludent ihr Einverständnis erteilt, sowohl den Namen des schwerbehinderten Familienangehörigen als auch ihren eigenen ihrer Beschäftigungsbehörde bekanntzugeben, denn anders wäre eine Akteneinsichtnahme dort nicht möglich. Angesichts dessen, dass die Beschwerdeführerin aufgrund ihrer Zuständigkeit in ihrer Beschäftigungsbehörde den Mitarbeitern in der für Schwerbehindertenangelegenheiten ihres Familienangehörigen zuständigen Verwaltung bekannt sei, hätten sich die jeweiligen Leiter zur Klärung der beantragten Akteneinsicht telefonisch verständigt. Der Austausch der personenbezogenen Daten, dass die Beschwerdeführerin Einsicht in die Akte XY in der Beschäftigungsbehörde begehrte, war auch aus Sicht des TLfDI zur Aufgabenerfüllung der beteiligten Behörden erforderlich und zulässig. Die für Schwerbehindertenangelegenheiten zuständige Behörde räumte allerdings ein, man habe bei diesem Datenaustausch „nicht so sehr“ zwischen dienstlichen und persönlichen Angelegenheiten getrennt, da sich ja alle Beteiligten kannten. Möglicherweise sei es dann zum Austausch von Informationen gekommen, deren Weitergabe im Rahmen des Verfahrens nicht erforderlich war. Über die eingereichte Dienstaufsichtsbeschwerde habe man sich jedoch nicht unterhalten. Man habe dies zum Anlass genommen, die Angelegenheit auszuwerten und eine Sensibilisierung zur Einhaltung der gesetzlichen Vor-

schriften zur Weitergabe und Verarbeitung von personenbezogenen Daten vorgenommen. Es werde alles getan, um zukünftig den gesetzlichen Vorschriften Rechnung zu tragen. Das dargelegte Vorgehen bewertete der TLfDI als geeignete Maßnahmen, um für die Zukunft die Einhaltung der datenschutzrechtlichen Vorschriften zur Übermittlung von Daten Betroffener sicherzustellen. Von einer Beanstandung wegen unzulässiger Datenübermittlung konnte daher nach § 39 Abs. 3 ThürDSG abgesehen werden.
Um zu klären, weshalb die Beschwerdeführerin von ihrer Beschäftigungsbehörde zu der gegen die andere Kommune eingereichten Dienstaufsichtsbeschwerde befragt wurde, obwohl die für Schwerbehindertenangelegenheiten zuständige Behörde nach deren Angaben der Beschäftigungsbehörde nichts mitgeteilt hatte, wandte sich der TLfDI auch an die Beschäftigungsbehörde. Diese teilte mit, die Beschwerdeführerin selbst habe in einem informellen Gespräch mit ihrer Vorgesetzten die Dienstaufsichtsbeschwerde erwähnt. Konkrete Inhalte zu der Dienstaufsichtsbeschwerde lägen der Dienststelle jedoch nicht vor. Daher finde auch eine Verarbeitung von Inhalten zur Beschwerde keineswegs statt. Da aber weder aus dem Vortrag der Kommune noch aus dem Vorbringen der Beschwerdeführerin konkrete Anhaltspunkte dafür zu entnehmen waren, dass sie nicht den Tatsachen entsprachen und weitergehende Mittel zur Sachaufklärung nicht ersichtlich waren, war diesbezüglich ein datenschutzrechtlicher Verstoß nicht feststellbar.

Auch wenn sich die in einem Verwaltungsverfahren beteiligten Bediensteten verschiedener oder gleicher Behörden persönlich kennen, dürfen nur die für die konkrete Aufgabenerfüllung erforderlichen personenbezogenen Daten und Informationen in Wahrnehmung der konkreten Aufgabe ausgetauscht werden.

12.17 Auskunft der Einkommens- und Vermögenverhältnisse gegenüber unterhaltspflichtigen Geschwistern bei Unterhaltsforderungen

Einem Landkreis stellte sich als Sozialhilfeträger ein datenschutzrechtliches Problem, weswegen er sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) wandte. Der Landkreis leistete einer Frau, die sich im Pflegeheim befindet, vorab Unterhalt nach dem Sozialgesetzbuch (SGB) Zwölf-

tes Buch (XII). Die Frau hat drei unterhaltspflichtige Kinder, denen die Kosten in Rechnung gestellt werden sollten. Der Landkreis hatte bereits die Einkommens- und Vermögensverhältnisse der Kinder geprüft. Danach ergab sich nach §§ 94 Abs. 1 SGB XII, 1606 Abs. 3 Nr. 1 und 1603 Bürgerliches Gesetzbuch (BGB), dass eines der Kinder nichts zu zahlen hat und die Forderung unter den anderen Kinder im Verhältnis von 30 zu 70 Prozent aufzuteilen ist. Das Kind mit der höheren Unterhaltsquote weigerte sich jedoch, die Unterhaltsforderung zu zahlen, solange kein Beweis der Einkommens- und Vermögensverhältnisse der Geschwister vorliege.

Dadurch ergab sich für den Landkreis ein Konflikt, denn unterhaltspflichtige Kinder besitzen gegenseitig Anspruch auf Mitteilung ihrer Einkommens- und Vermögensverhältnisse nach § 242 BGB. Dagegen hat das Sozialamt § 35 SGB Erstes Buch (I) zu beachten; dieser beinhaltet die Wahrung des Sozialgeheimnisses, das heißt konkret, dass die Einkommens- und Vermögensverhältnisse der Kinder nicht ohne Weiteres an Dritte weitergegeben werden dürfen. Dasjenige Kind, welches nichts zu zahlen hat, gestattete dem Landkreis seine Einkommens- und Vermögensverhältnisse seinen Geschwistern mitzuteilen. Dagegen hat das Kind mit der Unterhaltsquote von 30 Prozent untersagt, seine Einkommens- und Vermögensverhältnisse gegenüber seinen Geschwistern offenzulegen.

Der § 69 Abs. 1 SGB Zehntes Buch (X) sollte dem Landkreis als Ermächtigungsgrundlage dienen; danach ist eine Übermittlung der Sozialdaten dann zulässig, soweit dies für die Erfüllung des Zweckes, für den sie erhoben wurden, erforderlich ist. Allerdings war der Landkreis nicht sicher, ob die Bestimmung für diesen Fall einschlägig ist.

Nach § 69 Abs. 1 Nr. 1 SGB X bestehen keine Anforderungen in Bezug auf den Dritten, an den die Daten übermittelt werden. Insoweit können Sozialdaten nicht nur an andere in § 35 SGB I genannte Stellen übermittelt werden, sondern auch an Private, insbesondere Unterhaltspflichtige (§ 98 SGB X). Einer Einwilligung der Betreffenden bedarf es nicht.

Dies ergibt sich auch aus der Kommentierung (Hauck/Noftz) zu § 94 SGB XII. Dort wird unter Randnummer 216 ausgeführt, dass im Rahmen der Geltendmachung der Erstattungsansprüche der Träger der Sozialhilfe verpflichtet ist, im gerichtlichen Verfahren zumindest die ihm bekannten Tatsachen im Unterhaltsrechtsstreit auch dann vorzutragen, wenn sich daraus aus den Unterhaltspflichten günstige

Rechtsfolgen herleiten lassen. Begründet ist dies damit, dass der im vorprozessualen Verwaltungsverfahren geltende Untersuchungsgrundsatz nicht ins Leere läuft. Gerade das wäre aber der Fall, wenn ein Unterhaltsverpflichteter geltend machen könnte, dass die ihn betreffenden, von der Sozialbehörde erhobenen Einkommensdaten anderen möglichen Unterhaltspflichtigen nicht zur Kenntnis gelangen dürften und er damit einen Erstattungsanspruch des Sozialhilfeträgers verhindert. Den Unterhaltspflichtigen steht untereinander ein Anspruch auf Mitteilung ihrer Einkommens- und Vermögensverhältnisse zu. Wird ein Unterhaltspflichtiger im Verwaltungsverfahren auf Unterhalt in Anspruch genommen, wäre es jedoch nicht zu rechtfertigen, ihn auf seinen Auskunftsanspruch den anderen Unterhaltspflichtigen gegenüber und im Übrigen darauf hinzuweisen, dass er die Berechnungsgrundlagen erst im gerichtlichen Verfahren erhalten könne. Der Landkreis ist daher befugt, den unterhaltspflichtigen Kindern die Einkommens- und Vermögensverhältnisse ihrer Geschwister, soweit sie als Berechnungsgrundlage des zu leistenden Unterhalts herangezogen wurden, im Hinblick auf mögliche gerichtliche Verfahren offenzulegen, wobei sich die Darlegung auf die erforderlichen Angaben zur Berechnung beschränken muss.

Gemäß § 69 Abs. 1 SGB X kann durch den Sozialträger die Auskunft der Einkommens- und Vermögensverhältnisse gegenüber Unterhaltspflichtigen erteilt werden, wenn sie für die Erfüllung der Durchsetzung der Unterhaltsansprüche erforderlich sind.

12.18 Auch das Sozialamt verlangt Daten

Ein Ehepaar wandte sich hilfesuchend an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Das Ehepaar hatte eine erwachsene Tochter, die aufgrund ihrer Behinderung erwerbsunfähig war. Sie hatte daher beim zuständigen Sozialamt Sozialhilfe nach dem Sozialgesetzbuch (SGB) Zwölftes (XII) Buch gestellt. Um zu klären, ob die grundsätzlich unterhaltspflichtigen Eltern leistungsfähig sind, wandte sich das Sozialamt mit einem Auskunftsersuchen an sie. Beide erhielten gesonderte Anschreiben mit einem Selbstauskunftsbogen, auf dem sie über ihre Einkünfte und auch die des Ehepartners bzw. Lebenspartners Angaben machen sollten. Außerdem sollten Kontoauszüge der letzten drei

Monate vorgelegt werden. Die Eltern baten den TLfDI um Überprüfung der Zulässigkeit dieses Auskunftsersuchens.
Auf Nachfrage des TLfDI teilte das Sozialamt mit, dass die Ehegatten jeweils gesondert angeschrieben worden waren und auch gesondert Angaben zu machen haben. Die Nachfrage nach dem Ehepartner bzw. Lebenspartner beziehe sich nur auf einen neuen Ehe- bzw. Lebenspartner, der zwar selbst nicht unterhaltspflichtig, jedoch auskunftspflichtig im Sinne der unterhaltsrechtlichen Regelung ist. Dies ergab sich aber keinesfalls aus den vom Sozialamt verwendeten Antragsunterlagen. Dieses wurde daher gebeten, im Antragsformular für Klarstellung zu sorgen, damit nicht fälschlicherweise jeder Unterhaltsverpflichtete auch Angaben zu dem Lebenspartner bzw. Ehegatten macht, der selbst auch unterhaltsverpflichtet ist.
Im Hinblick auf die Kontoauszüge teilte das Sozialamt mit, dass nach der Rechtsprechung des Bundessozialgerichtes Kopien von Kontoauszügen als Beweismittel im Sinne von § 16 Abs. 1 Nr. 3 SGB Erstes (I) Buch gelten. Dies ist zwar richtig, gleichwohl sind Kontoauszüge nur dann vorzulegen, soweit dies für die Aufgabenerfüllung der Sozialbehörde erforderlich ist. Dies ergibt sich auch aus der Regelung des § 117 SGB XII, der die Auskunftspflicht der unterhaltspflichtigen Personen regelt. Das Sozialamt wurde darauf hingewiesen, dass den Betroffenen in gewissen Fällen Schwärzungen der Kontoauszüge ermöglicht werden müssen, beispielsweise wenn es sich um besonders geschützte Daten nach § 4 Abs. 5 Thüringer Datenschutzgesetz (ThürDSG) handelt, wie Daten über religiöse Überzeugungen oder Gewerkschaftszugehörigkeit. Auch bedeutet die Vorlagepflicht nicht, dass alle Kontoauszüge zur Akte genommen werden dürfen. Dies ist nur zulässig, soweit es sich um anspruchsbegründende Unterlagen handelt. Das Sozialamt wurde daher aufgefordert darzulegen, wie mit den eingereichten Kopien von Kontoauszügen dort weiter verfahren wird. Eine Antwort des Sozialamts steht noch aus.

Werden von Betroffenen Daten erhoben, so muss sich eindeutig ergeben, welche Daten angegeben werden sollen. Dies gilt insbesondere dann, wenn es sich um Daten von Dritten handelt. Bei Kopien von Kontoauszügen handelt es sich zwar um Beweismittel im Sinne des § 60 Abs. 1 Nr. 3 SGB I, sie dürfen aber nur erhoben und gespeichert werden, soweit dies zur Aufgabenerfüllung der Behörde erforderlich ist.

12.19 Sozialamt – Agentur für Arbeit – Jobcenter – Optionskommune: Datenschutz-Dschungelbuch

Ein Bürger hoffte, dass ihm der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) dabei helfen könne zu klären, wo maßgebliche Vorgänge bei dem für ihn zuständigen Sozialamt gespeichert sind und welche Daten in diesen Vorgängen erhoben und übermittelt wurden. Er selbst habe bereits gemäß § 83 Sozialgesetzbuch (SGB) Zehntes Buch (X) eine Auskunft vom Sozialamt verlangt, auf seine Anfrage sei jedoch nicht eingegangen worden. Nach Durchsicht der zahlreichen der Beschwerde beigefügten Unterlagen stellte sich heraus, dass sich der Beschwerdeführer gegen die Vorgehensweise des dortigen Jobcenters wandte. Der betreffende Landkreis zählte nicht zu den sogenannten Optionskommunen, denen die Aufgabenerfüllung nach dem Sozialgesetzbuch (SGB) Zweites Buch (II) in eigener Zuständigkeit übertragen wurde. Im gesetzlichen Regelfall sind die Bundesagentur für Arbeit und die jeweilige Kommune Leistungsträger der Grundsicherungsleistungen nach dem SGB II. Die sogenannten Optionskommunen (siehe dazu Beitrag 12.8) sind auf ihren Antrag zugelassene kommunale Träger der Grundsicherung für Arbeitsuchende. Sie bilden dazu ein Jobcenter, für dessen datenschutzrechtliche Kontrolle der jeweiligen Landesbeauftragte für den Datenschutz zuständig ist.
Da es sich hier nicht um eine Optionskommune handelte, erklärte der TLfDI, dass nicht er, sondern nach § 50 Abs. 4 Satz 3 SGB II die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) für die Datenschutzkontrolle des Jobcenters zuständig ist. Aus den Ausführungen und Anlagen, die der Beschwerdeführer dem TLfDI zugesandt hatte, konnte der TLfDI entnehmen, dass sich die BfDI bereits ausführlich mit der Beschwerde auseinandergesetzt und dahingehend bereits Feststellungen getroffen hatte. Es war weder eine Zuständigkeit des TLfDI gegeben noch war dem etwas hinzuzufügen, da die Angelegenheit umfassend geklärt war.

Der TLfDI kontrolliert als Kontrollbehörde die Einhaltung der datenschutzrechtlichen Vorschriften im Zusammenhang mit der Gewährung von Leistungen nach dem SGB II bei den Jobcentern der sogenannten Optionskommunen des Landes. Für die Jobcenter der Agentur für Arbeit ist die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit zuständig.

12.20 Datenschutzrechtliche Skepsis bei der Sepsis?

Die Qualitätsverbesserung in der Krankenversorgung ist den Krankenhäusern ein wichtiges Anliegen. Es gibt daher zahlreiche Forschungsvorhaben, die sich damit beschäftigen, welche Faktoren auf den Verlauf einer Krankheit Einfluss haben. Zur Durchführung derartiger Studien ist auch immer die Erhebung von Patientendaten erforderlich. Damit dies datenschutzgerecht geschieht, wenden sich etliche Krankenhäuser mit der Bitte um Beratung an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). So bat auch das Universitätsklinikum Jena um datenschutzrechtliche Bewertung einer geplanten Studie zur Qualitätsverbesserung der Behandlung von Sepsiserkrankungen. Dazu übersandte es Unterlagen, in denen das Verfahren beschrieben wurde. Ziel der Studie war es, die Behandlungsqualität bei Patienten mit Sepsis in den kooperierenden Krankenhäusern zu verbessern sowie die damit einhergehenden Veränderungsprozesse wissenschaftlich zu begleiten. In die Studie sollten die Daten aller Patienten, die ab einem gewissen Zeitpunkt in den teilnehmenden Kliniken vollstationär behandelt wurden, einbezogen werden. Die fallbezogenen Daten sollten durch die Vergabe von Codenummern pseudonymisiert werden. Die Schlüsseltabellen zur Aufhebung der Pseudonymisierung verbleiben dabei in den jeweiligen Krankenhäusern. Die pseudonymisierten Daten gehen zu einem Unternehmen, das die Daten auswertet und Qualitätsberichte erstellt. Damit wertet es personenbeziehbare Daten im Auftrag aus. Die Stelle, die dann wissenschaftlich Analysen durchführt, erhält von der Auswertungsfirma vollständig anonymisierte Daten.

Auch wenn die Daten an das Auswertungsunternehmen in pseudonymisierter Form übermittelt werden, handelt es sich dabei nach § 3 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) um personenbezogene Daten, jedenfalls im Hinblick auf das Krankenhaus. Da der Schlüssel für die Aufhebung der Pseudonymisierung im Krankenhaus verbleibt, waren die Daten für das Auswertungsunternehmen anonymisiert im Sinne von § 3 Abs. 9 ThürDSG, da dieses nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft die Daten einer bestimmten Person hätte zuordnen können. Gleichwohl prüfte der TLfDI den zwischen dem Krankenhaus und dem Auswertungsunternehmen geschlossenen Auftragsdatenverar-

beitungsvertrag sorgfältig, damit sichergestellt war, dass das Krankenhaus die technischen und organisatorischen Maßnahmen getroffen hat, die erforderlich sind, um datenschutzrechtliche Anforderungen einzuhalten, § 27a Abs. 10 Thüringer Krankenhausgesetz. Der TLfDI forderte insbesondere, dass so konkret wie möglich dargestellt werden soll, welche Daten in welcher Form übermittelt werden und welche Aufgaben das Auswertungsunternehmen damit wahrnehmen soll. Auch die Umstände der Verschlüsselung der Projektdaten sollten konkreter angegeben werden. Nachdem das Universitätsklinikum alle Anregungen des TLfDI umgesetzt hatte, bestanden keine datenschutzrechtlichen Bedenken an der Durchführung des Projektes mehr.

Für die Qualitätsverbesserung in der Krankenversorgung ist es notwendig, fallbezogen mit Patientendaten zu arbeiten. Eine Auswertung und wissenschaftliche Bewertung durch dritte Stellen erfordert es in der Regel nicht, die Daten bestimmten Personen zuordnen können. Es ist durch technische und organisatorische Maßnahmen sicherzustellen, dass die Voraussetzungen an die Anonymisierung eingehalten werden.

12.21 Sozialdaten – Schweigepflicht besteht auch gegenüber dem Landrat

Ein Mitarbeiter des Sozialpsychiatrischen Dienstes eines Gesundheitsamtes im Landratsamt wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und bat um Information darüber, welche Angaben aus seiner dienstlichen Tätigkeit er gegenüber anderen Stellen des Landratsamtes unter welchen Voraussetzungen offenbaren dürfe. Der Mitarbeiter legte folgenden Sachverhalt dar: Ein Bürger hatte die Beratung des Sozialpsychiatrischen Dienstes in Anspruch genommen. Unabhängig davon war es mit einem Mitarbeiter des Landratesamtes zu einem Streit wegen des Entzugs des Führerscheines gekommen. Dabei kam es zu Beschimpfungen und verbalen Bedrohungen. Der Sozialpsychiatrische Dienst wurde im Rahmen der Beratung aufgefordert, diese Vorfälle zu prüfen. Wiederholte Abklärungen über einen Zeitraum von circa zwei Jahren ergaben keinerlei Anhaltspunkte für die Unterbringung des Bürgers in einer psychiatrischen Fachklinik gegen dessen Willen. Nunmehr verlangt das Landratsamt als Dienst-

herr des betroffenen Mitarbeiters Einsicht in die Akte beim Sozialpsychiatrischen Dienst. Der Sozialpsychiatrische Dienst bat um Auskunft darüber, wie das Landratsamt bei seiner Fürsorgepflicht unterstützt werden kann, ohne dass datenschutzrechtliche Vorschriften verletzt werden. Parallel zur Anfrage des Mitarbeiters vom Sozialpsychiatrischen Dienst erhielt der TLfDI auch eine Anfrage vom Thüringer Landeverwaltungsamt (TLVwA) zum entsprechenden Sachverhalt.
Der TLfDI beriet beide Stellen wie folgt:
Die personenbezogenen Angaben des Bürgers unterliegen dem Sozialdatenschutz, da es sich beim Sozialpsychiatrischen Dienst des Landkreises um eine Sozialbehörde im Sinne des Sozialgesetzbuches handelt. Die Weitergabe personenbezogener Daten richtet sich auch innerhalb einer öffentlichen Stelle nach den Übermittlungsvorschriften, wenn datenschutzrechtlich zwei verschiedene verantwortliche Stellen betroffen sind. Eine Übermittlung von Sozialdaten ist nur zulässig, wenn eine gesetzliche Übermittlungsbefugnis nach dem Sozialgesetzbuch Zehntes Buch (SGB X) gemäß § 67d Abs. 1 vorliegt. Eine Übermittlungsbefugnis an die Behördenleitung – das Landratsamt – aus Gründen der Fürsorgepflicht für den betroffenen Mitarbeiter ergibt sich nach Auffassung des TLfDI aus SGB X nicht. Daher kann der Sozialpsychiatrische Dienst der Behördenleitung als Prüfungsergebnis mitteilen, dass die erforderlichen Voraussetzungen für weitere Maßnahmen gegenüber dem Bürger nicht vorliegen. Dabei darf der Mitarbeiter des Sozialpsychiatrischen Dienstes aber nicht auf Einzelheiten eingehen, da diese nach Auffassung des TLfDI der Schweigepflicht unterliegen. Eine Verletzung der Schweigepflicht wäre nach § 203 Strafgesetzbuch strafbar, wenn keine Rechtfertigungsgründe bestehen und die Datenübermittlung somit unbefugt erfolgen würde. Eine Übermittlungsbefugnis liegt für den angestrebten Zweck der Fürsorge für eine Mitarbeiterin nach den Vorschriften des SGB nicht vor.

Eine Übermittlung von Sozialdaten ist nur zulässig, soweit eine gesetzliche Übermittlungsbefugnis nach dem Sozialgesetzbuch Zehntes Buch (SGB X) vorliegt, § 67d Abs. 1 SGB X. Aus den Regelungen des SGB X ergibt sich keine Übermittlungsbefugnis zu beim Sozialpsychiatrischen Dienst gespeicherten Daten eines Bürgers an die Behördenleitung aus Fürsorgezwecken, wenn dieser zur Auffassung gelangt ist, dass eine Unterbringung des Betroffenen geboten ist.

12.22 Schwärzungen bei Kontoauszügen

Eine Bürgerin wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), weil gegen sie eine Forderung des Jobcenters besteht, für welche im Rahmen einer Schuldenregulierung versucht wird, eine Stundung zu erreichen. In Zuge dessen verlangte der Sachbearbeiter des Forderungsmanagements des Jobcenters ungeschwärzte Kontoauszüge der letzten drei Monate. Das hielt der Schuldenberater der Beschwerdeführerin für nicht zulässig, daher bat sie den TLfDI, die Zulässigkeit zu prüfen.

Der Anfrage an den TLfDI war ein Schreiben ihres Schuldenberaters an das Jobcenter beigefügt, in dem auf das Urteil vom 19. September 2008, Az.: B 14 AS 45/07 R des Bundessozialgerichts Bezug genommen wird. Dieses Urteil enthält eine richtungsweisende Entscheidung zur Vorlagepflicht von Kontoauszügen und deren Beschränkungen. Demnach ist der Antragsteller verpflichtet, seine Hilfsbedürftigkeit nachzuweisen, denn der Leistungsträger muss in der Lage sein, anhand nachweisbarer Kriterien über den Antrag entscheiden zu können. Um sowohl dem Recht auf informationelle Selbstbestimmung des Antragstellers als auch den Interessen der Sozialleistungsträger angemessen Rechnung tragen zu können, gibt das Bundessozialgericht für eine datenschutzgerechte Verfahrensweise bei der Anforderung von Kontoauszügen folgende Vorgaben: Schwärzen von einzelnen Buchungen kann dem Antragsteller nicht vornherein verwehrt werden. Eine Mitwirkung des Antragstellers kann lediglich im Rahmen des Verhältnismäßigkeitsgrundsatzes verlangt werden. Die Mitwirkung muss danach erforderlich und angemessen sein. Die Betroffenen müssen auf die Möglichkeit des Schwärzens einzelner Buchungen bereits bei der Anforderung der Kontoauszüge hingewiesen werden.

Insbesondere bei Soll-Buchungen über geringe Beträge (regelmäßig bis 50 Euro) kann der Antragsteller die zu den Einzelbuchungen aufgeführten Texte in der Regel schwärzen. Der Betrag selbst muss sichtbar bleiben. Über die Angabe der Beträge bzw. durch den Vergleich der Kontostände lässt sich die Einkommens- bzw. Vermögenssituation weiterhin lückenlos feststellen.

Allerdings ist darauf hinzuweisen, dass jeweils die Besonderheiten des Einzelfalles zu beachten sind. So können zum Beispiel regelmä-

ßige Zahlungen von Beiträgen für Kapital bildende Lebensversicherungen, Ausbildungsversicherungen oder Bausparverträge durchaus entscheidungsrelevant sein. Insoweit wäre eine Schwärzung auch bei geringeren Beträgen nicht zulässig. Jedoch hat hier der Sachbearbeiter, wenn er die Schwärzung für unzulässig erachtet, dem Betroffenen gegenüber den Grund zu erläutern. Ein möglicher Lösungsansatz für strittige Einzelfälle könnte zum Beispiel sein, dass dem Betroffenen eine Teilschwärzung der Buchungstexte ermöglicht wird. Beispielsweise könnte der Name der betreffenden Organisation oder die Versicherungsnummer geschwärzt werden.

Inwieweit das Schwärzen von Texten bei einzelnen Soll-Buchungen über größere Beträge (über 50 Euro) zur Wahrung schutzwürdiger Belange von Antragstellern zulässig ist, hängt von der Gestaltung des Einzelfalls ab.

Schwärzungen können unabhängig vom Betrag grundsätzlich dann vorgenommen werden, wenn die Buchungstexte Angaben über besonders geschützte Daten im Sinne des § 67 Abs. 12 Sozialgesetzbuch (SGB) Zehntes Buch (X) enthalten. Dazu zählen Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben. Beispielsweise kann bei Überweisungen von Mitgliedsbeiträgen an eine Partei beziehungsweise eine Gewerkschaft oder bei Zahlungen an eine Religionsgemeinschaft die Bezeichnung der Organisation geschwärzt werden. Der Text „Mitgliedsbeitrag“ oder „Spende“ sollte lesbar bleiben, um Missverständnisse zu vermeiden.

Da es in diesem Fall nicht um die Entscheidung der Hilfsbedürftigkeit nach dem SGB Zweites Buch (II), sondern um die Prüfung einer beantragten Ratenzahlung ging, ist das Jobcenter von den Anforderungen der Rechtsprechung, die eine Schwärzung besonders zu schützender personenbezogener Daten als zulässig festgestellt hat, abgewichen. Das Jobcenter ging davon aus, im Rahmen der Stundung könne dem Schuldner zugemutet werden, dass er alle zur Beurteilung der persönlichen und sachlichen Stundungsgründe maßgebenden Umstände preisgebe, ähnlich wie bei der Mitwirkungspflicht bei Anträgen auf Sozialleistungen. In zukünftigen Fällen will das Jobcenter jedoch analog der Verfahrensweise zur Feststellung der Hilfebedürftigkeit nach dem SGB II auch bei Stundungsanträgen auf die Schutzwürdigkeit personenbezogener Daten nach dem SGB X und dass diese geschwärzt werden können hinweisen.

Der TLfDI hält die neue Vorgehensweise des Jobcenters für datenschutzkonform.

Nach § 67 Abs. 12 SGB X können Schwärzungen unabhängig vom Betrag grundsätzlich dann vorgenommen werden, wenn die Buchungstexte Angaben über besonders geschützte Daten enthalten. Damit den datenschutzrechtlichen Belangen nachgekommen werden kann, sollte auf Vorlage vollständig ungeschwärzter Kontoauszüge verzichtet und Schwärzungen auch im Rahmen von Stundungsbearbeitung akzeptiert werden. Darauf sollte bereits bei der Anforderung der Kontoauszüge hingewiesen werden.

12.23 Einwilligung im Rahmen der Unfallversicherung?

Ein Bürger wandte sich mit folgendem Anliegen an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI): Er habe im Berichtszeitraum einen Arbeitsunfall erlitten, daher habe sein Arbeitgeber an die Berufsgenossenschaft eine entsprechende Unfallmeldung gemacht. Von dieser erhielt der Betroffene einen Unfallbogen, dem eine „Erklärung zum Datenschutz“ sowie eine „Information zum Datenschutz“ beigefügt waren. Die „Erklärung zum Datenschutz“ war so gestaltet, dass vom Betroffenen quasi eine Einwilligung für die Datenerhebung durch die Berufsgenossenschaft bei verschiedenen Stellen erteilt wird. Nach § 119 Abs. 1 Sozialgesetzbuch (SGB) Siebtes Buch (VII) dürfen die Unfallversicherungsträger Sozialdaten nur erheben und speichern, soweit sie zur Erfüllung ihrer gesetzlich vorgeschriebenen oder zugelassenen Aufgaben erforderlich sind. Diese Übermittlungsbefugnis wird in § 200 Abs. 1 SGB VII durch den Verweis auf § 76 Abs. 2 Nr. 1 SGB Zehntes Buch (X) eingeschränkt. Nach § 76 Abs. 2 Nr. 1 SGB X gilt das in Abs. 1 zur Bestimmung ausgesprochene Verbot zur Übermittlung nicht für Sozialdaten, die im Zusammenhang mit einer Begutachtung wegen der Erbringung von Sozialleistung oder wegen der Ausstellung einer Bescheinigung übermittelt worden sind, es sei denn, dass der Betroffene der Übermittlung widerspricht. Der Betroffene ist dabei von der verantwortlichen Stelle zu Beginn des Verwaltungsverfahrens in allgemeiner Form schriftlich auf das Widerspruchsrecht hinzuweisen. Die Kasse teilte in der „Information zum Datenschutz“ mit, dass sie durch die „Einwilligung“ im Rahmen des Ver-

fahrens sicherstellen will, dass die anderen beteiligten Stellen wissen, dass das Widerrufsrecht nicht ausgeübt wird.
Der TLfDI wandte sich an die Berufsgenossenschaft und wies darauf hin, dass zum einen zu Beginn des Verfahrens auf das Widerspruchsrecht hinzuweisen ist, § 76 Abs. 2 Nr. 1 letzter Halbsatz SGB X. Und außerdem ist es zum andern das Wesen des Widerspruchsrechts, dass es jederzeit wahrgenommen werden kann. Das bedeutet, dass auch eine Einwilligung zu jeder Zeit des Verfahrens zurückgenommen werden kann. Die beabsichtigte Verfahrensbeschleunigung kann daher gar nicht eintreten. Außerdem ist der TLfDI der Auffassung, dass neben den gesetzlichen Erhebungs- und Übermittlungsbefugnissen für eine Einwilligung im Rahmen des SGB VII kein Platz ist.
Die Berufsgenossenschaft teilte dem TLfDI daraufhin mit, dass es sich bei ihr um eine bundesunmittelbare Körperschaft des öffentlichen Rechts handle, die von der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit kontrolliert wird. Diese habe allerdings in den vergangenen Jahren ebenfalls Bedenken hinsichtlich der Einwilligungserklärungen zu Datenerhebungen und -übermittlungen in der gesetzlichen Unfallversicherung geäußert. Derzeit werde gemeinsam daran gearbeitet, die erforderlichen Informationen und Befugnisse zur Datenerhebung mit einer transparent gehaltenen Formulargestaltung zu verbessern. Hierüber setzte der TLfDI den Betroffenen in Kenntnis.

Nach § 119 Abs. 1 SGB VII dürfen die Unfallversicherungsträger Sozialdaten nur erheben und speichern, soweit dies zur Erfüllung ihrer gesetzlich vorgeschriebenen oder zugelassenen Aufgaben erforderlich ist. Neben den gesetzlichen Erhebungs- und Übermittlungsbefugnissen des SGB VII ist für eine Einwilligung grundsätzlich kein Raum. Ein gesetzlich bestehendes Widerspruchsrecht kann nur dann wirksam ausgeübt werden, wenn der Betroffene zu Beginn des Verfahrens darauf hingewiesen wird.

12.24 Welche Daten darf die Krankenkasse bei Renteneintritt erheben?

Ein Bürger beschwerte sich beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) darüber, dass seine Krankenkasse (KK) im Zusammenhang mit seinem Eintritt in die Altersrente personenbezogene Daten erhob, u. a. die Höhe seiner

Brutto-Rente. Als Beleg übersandte der Beschwerdeführer den entsprechenden Fragebogen seiner KK an den TLfDI. Der Beschwerdeführer kritisierte, dass die KK den Kassenbeitrag von der Rentenstelle überwiesen bekäme und insofern für die Datenerhebung keine Notwendigkeit bestünde. Dementsprechend stimmte der Beschwerdeführer der im Fragebogen ausgewiesenen Datenübermittlung nach § 10 Abs. 2a Einkommenssteuergesetz (EstG) auch nicht zu. Der Beschwerdeführer wollte vom TLfDI wissen, ob er verpflichtet sei, den Fragebogen der KK auszufüllen.

Der TLfDI teilte dem Beschwerdeführer mit, dass die KK nach Auffassung des TLfDI die erbetenen Angaben benötigt, um den vom Beschwerdeführer zu zahlenden Krankenversicherungsbeitrag zu berechnen. Dieser Beitrag richtet sich nach den Einnahmen des Versicherungspflichtigen. Gemäß § 237 Sozialgesetzbuch Fünftes Buch (SGB V, Gesetzliche Krankenversicherung) werden bei der Beitragsbemessung von versicherungspflichtigen Rentnern folgende Einnahmen vollständig zugrunde gelegt: der Zahlbetrag der Rente von der gesetzlichen Rentenversicherung, der Zahlbetrag vergleichbarer Einnahmen und das Arbeitseinkommen (sofern vorhanden).

Nach § 206 SGB V muss der Versicherungspflichtige auf Verlangen der KK über alle Tatsachen Auskunft erteilen, die für die Feststellung der Versicherungs- und Beitragspflicht erforderlich sind und die die KK zur Durchführung der ihr übertragenen Aufgaben benötigt. Nach erster Einschätzung des TLfDI wurden mit dem Fragebogen der KK jedoch keine Daten erhoben, die für die Aufgabenerfüllung der KK nicht erforderlich gewesen wären. Dennoch bot der TLfDI dem Beschwerdeführer an, sich an die KK zu wenden und die erbetenen Angaben im Einzelnen auf ihre Erforderlichkeit für die Aufgabenerfüllung der KK zu prüfen.

Im Hinblick auf die Zustimmung zur Datenübermittlung nach § 10 Abs. 2a EStG legte der TLfDI gegenüber dem Beschwerdeführer dar, dass die Krankenkassenbeiträge zu den sogenannten Vorsorgeaufwendungen gehören und die KK beabsichtigt, der Steuerbehörde die Höhe dieser Beiträge mitzuteilen. Durch die Höhe dieser Beiträge kann sich unter Umständen die Höhe der Einkommenssteuer des Beschwerdeführers verringern. Der Beschwerdeführer muss dieser Datenübermittlung an die Steuerbehörde jedoch nicht zustimmen. Allerdings muss er in diesem Falle die betreffenden Angaben gegenüber seiner zuständigen Steuerbehörde selbst nachweisen.

Da sich der Beschwerdeführer nicht mehr meldete, schien ihm die erteilte Auskunft ausreichend zu sein.

Gemäß § 206 SGB V muss der Versicherungspflichtige auf Verlangen seiner Krankenkasse über alle Tatsachen Auskunft erteilen, die für die Feststellung der Versicherungs- und Beitragspflicht erforderlich sind und die die Krankenkasse zur Durchführung der ihr übertragenen Aufgaben benötigt. Sofern der Versicherungsnehmer einer Datenübermittlung der Krankenkasse an die Steuerbehörde gemäß § 10 Abs. 2a Einkommensteuergesetz nicht zustimmt, muss er die entsprechenden Angaben gegenüber seiner Steuerbehörde selbst nachweisen.

12.25 Wenn alle Behörden Fragen haben

Ein Bürger wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), war sich aber nicht sicher, ob dieser für sein Problem zuständig sei. Er sei berufstätig und Vater zweier unehelicher Kinder, gegenüber denen er unterhaltspflichtig sei. Ständig werde er von verschiedenen Behörden aufgefordert, Unterlagen vorzulegen. Dies wiederhole sich aus seiner Sicht in einem recht kurzen Zeitraum immer wieder. So wolle das Jugendamt Auskünfte von ihm, auch das Grundsicherungsamt fordere Unterlagen an. Jetzt habe er ein Formular mit 46 Seiten Umfang erhalten und müsse ungeschwärzte Kontoauszüge der letzten vier Wochen nachreichen. Der Vater fragte an, warum er immer alle Unterlagen vorlegen müsse, auch Einkommensnachweise der letzten 12 Monate sowie seine letzte Steuererklärung. Er verstehe nicht, warum das Jugendamt für die Prüfung des Kindesunterhalts verantwortlich sei. Auch als die Kostenübernahme für eine Tagesmutter beantragt worden sei, mussten alle Unterlagen wieder erneut eingereicht werden. Er sehe nicht, dass dies erforderlich sei, da die Grunddaten doch bei den Behörden grundsätzlich vorhanden seien. Aus seiner Sicht wäre es besser, wenn die Daten miteinander verknüpft werden, sodass nicht immer neue Antragsunterlagen eingereicht werden müssen.
Da der Beschwerdeführer den Sachverhalt nur sehr allgemein angerissen hatte, konnte der TLfDI ihm auch nur eine allgemein gehaltene Antwort geben. Er wurde zunächst darauf hingewiesen, dass der TLfDI alle öffentlichen Stellen in Thüringen hinsichtlich der Einhal-

tung datenschutzrechtlicher Vorschriften kontrolliert, § 37 Thüringer Datenschutzgesetz. Die vom Beschwerdeführer genannten Stellen (Grundsicherungsamt, Jugendamt und Jobcenter) können personenbezogene Daten nicht ohne Weiteres untereinander austauschen. Hierzu bedarf es einer gesetzlichen Grundlage im Sozialgesetzbuch (SGB), die im Einzelfall gegeben sein kann. Ob dies im konkreten Fall gegeben war, konnte nicht festgestellt werden, weil der Sachverhalt dafür nicht hinreichend bekannt war.

Nimmt eine Person staatliche Leistungen in Anspruch, muss sie grundsätzlich nachweisen, dass die Anspruchsvoraussetzungen für den Erhalt der begehrten Leistungen vorliegen. Deswegen gibt es im SGB auch eine Mitwirkungspflicht des Antragstellers gegenüber den Behörden, § 60 SGB Erstes Buch. Allerdings dürfen die Behörden nur personenbezogene Daten anfordern/erheben, soweit dies zu ihrer Aufgabenerfüllung erforderlich ist. Bei Einkommensnachweisen sind beispielsweise regelmäßige Überprüfungen unter Umständen notwendig, sodass in zeitlichen Abständen erneute Nachweise angefordert werden können. Dabei ist auch zu berücksichtigen, dass nach der jeweils zugrundeliegenden rechtlichen Regelung der Einkommensbegriff im Steuerrecht sich von demjenigen im Sozialrecht unterscheidet. Daher kann nicht ohne Weiteres die Steuererklärung allein für die Berechnung eines Bedarfs herangezogen werden. Außerdem gilt im Datenschutzrecht der Grundsatz der Zweckgebundenheit. Das bedeutet, dass Daten grundsätzlich nur für den Zweck verarbeitet werden, für den sie erhoben werden. Ein Datenaustausch zwischen Behörden ist nur zulässig, wenn es eine gesetzliche Ermächtigungsgrundlage hierzu gibt, § 67d SGB Zwölftes Buch.

Ob diese Voraussetzungen im konkreten Einzelfall erfüllt sind, kann der TLfDI nur überprüfen, wenn konkrete Angaben gemacht werden, gegen welche Stelle sich aus welchem Anlass die Beschwerde richtet. Dies gilt auch für die Forderung der Einreichung von ungeschwärzten Kontoauszügen. Hier ist auch entscheidend, ob die Kontoauszüge nach der Prüfung zu den Akten genommen werden oder, falls sich aus ihnen keine Besonderheiten ergeben, diese vernichtet werden (siehe Punkt 12.26).

Dem Beschwerdeführer wurde mitgeteilt, dass der TLfDI sich gerne an die Stelle wendet, durch deren Verhalten der Beschwerdeführer bei der Verarbeitung oder Nutzung seiner personenbezogenen Daten in seinen schutzwürdigen Belangen beeinträchtigt sei, § 11 Abs. 1

Thüringer Datenschutzgesetz. Da der Beschwerdeführer sich nicht mehr meldete, war eine weitere Prüfung nicht möglich.

Im Datenschutzrecht gilt der Grundsatz der Zweckgebundenheit. Das bedeutet, dass Daten grundsätzlich nur für den Zweck verarbeitet werden dürfen, für den sie erhoben wurden. Ein Datenaustausch zwischen Behörden ist nur zulässig, wenn es eine gesetzliche Ermächtigungsgrundlage hierzu gibt.

12.26 Kontoauszüge für das Jobcenter

Arbeitsuchende erhalten nach den Bestimmungen des Sozialgesetzbuches (SGB) Zweites (II) Buch eine Grundsicherung von den Jobcentern. Hierzu gehört auch das Arbeitslosengeld II, dessen Träger im Regelfall die Agenturen für Arbeit und die kreisfreien Städte oder Landkreise sind. Diese Träger heißen nach § 6d SGB II Jobcenter. Sie sind in aller Regel eine gemeinsame Einrichtung der Bundesagentur für Arbeit und eines kommunalen Trägers. Für diese Jobcenter besitzt der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) keine Kontrollzuständigkeit (vergleiche Punkt 12.19). Außerdem gibt es aber noch die Möglichkeit, dass eine Kommune (Landkreis oder kreisfreie Stadt) die alleinige Trägerschaft der Leistungen nach dem SGB II besitzt. In Thüringen gibt es vier dieser sogenannten Optionskommunen als zugelassene Träger der Grundsicherung für Arbeitsuchende: die Landkreise Eichsfeld, Greiz, Schmalkalden-Meiningen und die Stadt Jena. Für diese Jobcenter hat der TLfDI nach § 37 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) die Kontrolle über die Einhaltung der datenschutzrechtlichen Vorschriften.
Den TLfDI erreichen seit geraumer Zeit gehäuft Anfragen und Beschwerden Betroffener, die vom jeweils zuständigen Jobcenter der Thüringer Optionskommunen aufgefordert werden, die Kontoauszüge der letzten drei bis sechs Monate vorzulegen, wobei Schwärzungen nur in sehr geringem Umfang akzeptiert werden. Die vorgelegten Kontoauszüge werden in der Regel in Kopie komplett zu den Leistungsakten genommen. Zwar obliegt dem Antragsteller bei der Beantragung von Sozialleistungen eine Mitwirkungspflicht. Gemäß § 60 Abs. 1 SGB Erstes (I) Buch hat, wer Sozialleistungen beantragt oder erhält, alle Tatsachen anzugeben, die für die Leistungen erheblich sind und auf Verlangen des zuständigen Leistungsträgers Be-

weisurkunden vorzulegen oder ihrer Vorlage zuzustimmen. Klare gesetzliche Vorgaben, ob und in welchem Umfang der Leistungsträger bei der Beantragung von Sozialleistungen die Vorlage von Kontoauszügen verlangen darf, welche Angaben ggf. geschwärzt und welche Beweisurkunden dauerhaft in den Akten gespeichert werden dürfen, gibt es leider nicht. Bei der Beantragung von laufenden Leistungen nach dem SGB II ist die Anforderung von Kontoauszügen der letzten ein bis drei Monate nicht grundsätzlich unzulässig. Das Gesetz sieht aber nur die Vorlage dieser Unterlagen vor, nicht die dauerhafte Speicherung. In Einzelfällen kann die Vorlage der Kontoauszüge auch über einen Zeitraum von drei Monaten hinaus erforderlich sein, wenn konkrete Anhaltspunkte vorliegen, die den Verdacht auf Missbrauch von Sozialleistungen begründen. Das Schwärzen von einzelnen Buchungen kann dem Antragsteller nicht grundsätzlich verwehrt werden. Insbesondere Buchungen, die besonders geschützte Daten, wie politische Meinungen, religiöse Überzeugungen, Gewerkschaftszugehörigkeiten oder aber auch Daten über die Gesundheit betreffen, § 4 Abs. 5 ThürDSG, können geschwärzt werden.

Die Kontoauszüge dürfen vom Leistungsträger eingesehen werden, allerdings stellt aus Sicht des TLfDI die Bestimmung des § 60 SGB I keine Befugnis zur Speicherung dieser Daten dar. Gemäß § 67c Abs. 1 Satz 1 SGB Zehntes (X) Buch ist das Speichern, Verändern oder Nutzen von Sozialdaten durch die in § 35 Abs. 1 SGB I genannten Stellen zulässig, wenn es zur Erfüllung der in der Zuständigkeit der verantwortlichen Stelle liegenden gesetzlichen Aufgaben erforderlich ist. Da in aller Regel die Kontoauszüge eines Zeitraums von ein bis zwei oder gar sechs Monaten eine Vielzahl von Kontobewegungen enthalten, die für die Feststellung des Bedarfs der Hilfebedürftigen nicht relevant sind, ist eine komplette Speicherung dieser Daten regelmäßig unzulässig. Sie dürfen nur dann gespeichert werden, wenn die Daten zur Aufgabenerfüllung im Einzelfall erforderlich sind. In aller Regel sollte es genügen, wenn der Sachbearbeiter einen Vermerk in der Akte fertigt, in welchem er darlegt, aus welchem Zeitraum ihm Kontoauszüge vorgelegen haben und dass keine für den Leistungsanspruch relevanten Daten ermittelt wurden.

In diesem Zusammenhang ist jedoch auch der Grundsatz der ordnungsgemäßen Aktenführung zu beachten. Der TLfDI befragte daher den Thüringer Rechnungshof, welche Angaben sich seiner Auffassung nach in den Akten der Jobcenter befinden müssen, damit die Leistungsgewährung ordnungsgemäß dokumentiert wird. Der Rech-

nungshof machte deutlich, dass bei einem Erstantrag eine umfassende Vermögensprüfung durchzuführen ist. Im Rahmen dieser Vermögensprüfung können auch kleinere Beträge Hinweise auf weitere Vermögenspositionen enthalten. Datenabgleiche erfolgen erst regelmäßig mit mehreren Monaten Zeitverzug. Ordnungsgemäße Aktenbearbeitung setzte nach Ansicht des Rechnungshofes voraus, dass leistungsrelevante Nachweise in den Verwaltungsakten vollständig vorliegen bzw. deren leistungsrechtliche Bewertung durch die zuständigen Bearbeiter aktenkundig ist.

Auch mit einer Thüringer Optionskommune wurde ein Gespräch geführt, um zu einer datenschutzgerechten Lösung zu gelangen. Das Jobcenter der Optionskommune legte dar, dass es den Bearbeitern am Sprechtag nicht möglich sei, alle vorgelegten Unterlagen zu prüfen, diese müssten zunächst zum Vorgang genommen werden und dann zu einem späteren Zeitpunkt im Detail geprüft werden. Es sei im Rahmen der normalen Sprechzeiten nicht möglich, alle vorgelegten Unterlagen im Detail zu prüfen und daraufhin zu filtern, welche Angaben für die Entscheidung über die Leistungsgewährung tatsächlich erforderlich sind.

Der TLfDI machte dem Jobcenter folgenden Vorschlag zur Vorgehensweise: Das Jobcenter soll zunächst die Kontoauszüge entgegennehmen und für einen noch näher zu bestimmenden Prüfungszeitraum aufbewahren. Nach Vornahme dieser Prüfung dürfen allerdings nur die Kontoauszüge bzw. die Buchungen zur Akte genommen werden, die tatsächlich Nachweis-Charakter haben. Alle anderen Kopien von Kontoauszügen sind zu löschen, das heißt zu vernichten. Eine Stellungnahme des Jobcenters zu dem Vorschlag des TLfDI steht noch aus.

Nach § 67c Abs. 1 Satz 1 SGB X ist das Speichern, Verändern oder Nutzen von Sozialdaten zulässig, wenn es zur Erfüllung der in der Zuständigkeit der verantwortlichen Stelle liegenden gesetzlichen Aufgaben erforderlich ist. Im Rahmen der Beantragung von Arbeitslosengeld II ist es nach Auffassung des TLfDI nicht erforderlich, sämtliche Kontobewegungen von Antragstellern über einen längeren Zeitraum in den Leistungsakten zu speichern. Nach einer Prüfung über die Leistungsrelevanz sind die Daten zu löschen, die für die Gewährung der Leistung unerheblich sind.

12.27 Immer wieder Kontoauszüge

Ein Bürger wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) mit der Bitte, ihm bei der Aushändigung seiner Kontoauszüge bei einem Jobcenter behilflich zu sein. Er trug vor, dass die zur Vorlage beim Jobcenter eingereichten Kontoauszüge im Original nicht zurückgegeben worden seien. Er habe ein Schreiben des Jobcenters erhalten, in dem ihm mitgeteilt wurde, dass eine Rücksendung der im Original eingereichten Unterlagen nicht möglich sei. Es könnten nur Ausdrucke aus der elektronischen Akte übersandt werden.
Das Jobcenter wurde um Stellungnahme zum Sachverhalt gebeten. Zur datenschutzrechtlichen Prüfung bat der TLfDI das Jobcenter weiterhin um Mitteilung, ob die Betroffenen allgemein oder im Besonderen darauf hingewiesen werden, dass keine Originale einzureichen sind, weil diese nicht zurückgegeben werden.
Das Jobcenter teilte dem TLfDI die Festlegung der Verfahrensweise für die Entgegennahme von Poststücken mit: Die Antragsteller können zur Abgabe ihrer Unterlagen beim zuständigen Sachbearbeiter vorab einen Termin durch die Mitarbeiter der Servicestelle erhalten. Zum Termin werden die Originalunterlagen gesichtet und soweit erforderlich, eingescannt und in der elektronischen Akte abgelegt. Die Originalunterlagen werden dann zurückgegeben. Werden Antragsunterlagen oder andere Schriftstücke postalisch eingereicht, werden diese durch eine zentrale Stelle im Jobcenter gescannt und an die entsprechenden elektronischen Postkörbe der Mitarbeiter zur weiteren Bearbeitung weitergeleitet. Die Originalunterlagen werden für 30 Kalendertage zwischengelagert und danach unter Beachtung der Datenschutzbestimmungen vernichtet (gelöscht). Über dieses Prozedere werden alle Antragsteller im Rahmen der Erstberatung und/oder Antragstellung informiert. Um den Verwaltungsaufwand und die damit verbundenen Kosten zu begrenzen, werden nur die Poststücke zurückgesandt, welche vom Antragsteller speziell gewünscht oder bei denen ein Vermerk zur Rückgabe angebracht ist. Kontoauszüge, welche durch den Kontoausdrucker der Kreditinstitute gefertigt werden, werden generell zurückgesandt. Ebenfalls werden Originalbelege (soweit als solche erkennbar), welche postalisch eingehen, von den verantwortlichen Mitarbeitern an die Kunden zurückgesandt. Die Rückgabe wird listenmäßig dokumentiert.

Das Jobcenter teilte auch mit, dass der Beschwerdeführer das Angebot, einen Termin zu vereinbaren, um da die geforderten Unterlagen vorzulegen, nicht wahrgenommen hat. Auch seien die in Rede stehenden Kontoauszüge über das Onlinebanking ausgedruckt zur Verfügung gestellt worden, ein erneuter Ausdruck ist dem Beschwerdeführer somit jederzeit möglich, und es bestand aus Sicht des Jobcenters keine Erforderlichkeit der Rücksendung der Kontoauszüge. Man habe sie wie Kopien von Kontoauszügen behandelt und gelöscht.
Gegen das vom Jobcenter durchgeführte Verfahren ist nach datenschutzrechtlicher Prüfung nichts einzuwenden und es konnte kein Datenschutzverstoß festgestellt werden. Dies wurde dem Beschwerdeführer mitgeteilt.

Bei der Antragstellung im Jobcenter sollten Originalunterlagen nur bei einem Termin beim zuständigen Sachbearbeiter zur Durchsicht vorgelegt werden, der dann relevante Dokumente eingescannt in den Vorgang nehmen kann. Wenn Originalunterlagen auf dem Postweg versandt werden, sollte deutlich gemacht werden, dass eine Rücksendung gewünscht wird.

12.28 Weitergabe von Sozialdaten zur Rechnungsprüfung: kein Verstoß gegen den Datenschutz

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) wurde um Auskunft zur Zulässigkeit der Weitergabe und Verwendung von personenbezogenen Daten durch das Jobcenter einer Optionskommune in Thüringen gebeten. Das Jobcenter nimmt ungeachtet seiner Rechtsform als Eigenbetrieb die Gewährung der Grundsicherung für Arbeitsuchende nach dem Sozialgesetzbuch Zweites Buch (SGB II) für die Kommune wahr. Zur Rechnungsprüfung des Eigenbetriebes hatte das von der Kommune mit der Prüfung beauftragte Unternehmen vollständige Einblicke in Akten von Leistungsempfängern erhalten, ohne dass zuvor (personenbezogene) Daten der Akten anonymisiert wurden. Der TLfDI bewertete den Sachverhalt datenschutzrechtlich und teilte dem Fragesteller mit, das Jobcenter erfülle für die Optionskommune die Grundsicherung für Arbeitsuchende und sei damit Sozialbehörde nach § 35 Sozialgesetzbuch (SGB) Erstes Buch (I). Die Erfüllung der Aufgaben decke sich mit den entsprechenden Aufgaben der Bundesagentur für Arbeit und unterliege somit dem Sozialdaten-

schutz. Dieser ist insbesondere im SGB Zehntes Buch (X) geregelt (§§ 67 ff. SGB X).
Die personenbezogenen Daten der Betroffenen (Leistungsempfänger) dürfen als Sozialdaten grundsätzlich nur für den Zweck verarbeitet werden, für den sie erhoben wurden, sofern nicht eine Verarbeitung auch für andere Zwecke zulässig ist (vgl. § 67c Absätze 1 und 2 SGB X). Im vorliegenden Fall dürfen die Daten primär für die Gewährung der Grundsicherung verarbeitet werden. Nach § 67c Abs. 3 SGB X dürfen diese Daten jedoch auch gespeichert, verändert und genutzt werden, wenn dies für die Wahrnehmung von Aufsichts-, Kontroll- und Disziplinarbefugnissen, der Rechnungsprüfung oder der Durchführung von Organisationsuntersuchungen für die verantwortliche Stelle erforderlich ist. Dies entspricht auch den allgemeinen datenschutzrechtlichen Vorgaben des § 14 Abs. 3 Bundesdatenschutzgesetz (BDSG) für öffentliche Stellen des Bundes und § 20 Abs. 3 Thüringer Datenschutzgesetz (ThürDSG) für öffentliche Stellen des Landes.
Das mit der Prüfung beauftragte Unternehmen führt offensichtlich die Rechnungsprüfung für die Optionskommune durch. Im Rahmen der Rechnungsprüfung müssen grundsätzlich konkrete Akten zugrunde gelegt werden. Inwiefern im vorliegenden Fall eine Beschränkung der Einsicht aufgrund des Prüfungsauftrags möglich gewesen wäre, konnte der TLfDI nicht einschätzen. Jedoch stellt allein die Einsichtnahme in Leistungsakten nach SGB II zum Zweck der Rechnungsprüfung keine unzulässige Datenverarbeitung oder eine unzulässige Kenntnisnahme durch Dritte dar.
Die Verarbeitung der Sozialdaten durch die Mitarbeiter des Rechnungsprüfungsunternehmens unterliegt jedoch der strengen Zweckbindung, d. h., die zum Zweck der Rechnungsprüfung erhaltenen personenbezogenen Daten dürfen auch nur für diesen Zweck genutzt werden.

Nach § 67c Abs. 3 SGB X dürfen (personenbezogene) Sozialdaten auch gespeichert, verändert und genutzt werden, wenn dies für die Wahrnehmung von Aufsichts-, Kontroll- und Disziplinarbefugnissen, der Rechnungsprüfung oder der Durchführung von Organisationsuntersuchungen für die verantwortliche Stelle erforderlich ist.

12.29 Qualitätssicherung versus Datenschutz?

Ein Arzt wandte sich hilfesuchend an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Er teilte mit, dass die Kassenärztliche Vereinigung (KV) Thüringen ihn, wie möglicherweise andere Kollegen auch, aufgefordert habe, die Sonografiebilder und dazugehörige Krankenblatteinträge von fünf Patienten zur Qualitätskontrolle einzureichen. Er kam der Aufforderung nach, ohne das Einverständnis der Betroffenen einzuholen und bat nachträglich um Klärung, ob das Vorgehen der KV Thüringen rechtskonform ist.
Der TLfDI bat die KV Thüringen um Stellungnahme zu dem Vorwurf. Sie teilte mit, dass die Rechtsgrundlage für die in Rede stehenden Daten Sozialgesetzbuch (SGB) Fünftes Buch (V) sei. Nach § 92 Abs. 1 Satz 2 Nr. 13 SGB V beschließt der Gemeinsame Bundesausschuss die zur Sicherung der ärztlichen Versorgung erforderlichen Richtlinien über die Gewährung einer ausreichenden, zweckmäßigen und wirtschaftlichen Versorgung der Versicherten, insbesondere zur Qualitätssicherung. Zu diesem Zwecke seien gemäß § 299 SGB V die an der vertragsärztlichen Versorgung teilnehmenden Ärzte befugt und verpflichtet, personen- oder einrichtungsbezogene Daten der Versicherten zu erheben, zu verarbeiten oder zu nutzen.
Dem entgegnete der TLfDI, dass nach § 299 Abs. 1 Satz 4 Nr. 1 SGB V die von der KV Thüringen erwähnten Richtlinien sicherzustellen haben, dass die versichertenbezogenen Daten pseudonymisiert werden. Pseudonymisieren ist nach § 67 Abs. 8a SGB Zehntes Buch (X) das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren. Der TLfDI bat daher um erneute Stellungnahme, warum die Stichproben im vorliegenden Fall nicht pseudonymisiert worden waren. Die KV Thüringen berief sich auf § 299 Abs. 1 Satz 5 Nr. 2 SGB V. Danach können abweichend von § 299 Abs. 1 Satz 4 Nr. 1 SGB V die Richtlinien auch vorsehen, dass von einer Pseudonymisierung der versichertenbezogenen Daten abgesehen werden kann, wenn für die Qualitätssicherung die Überprüfung der ärztlichen Behandlungsdokumentation fachlich oder methodisch erforderlich ist und die technische Beschaffenheit des die versichertenbezogenen Daten speichernden Datenträgers eine Pseudonymisierung nicht zulässt. Außerdem muss die Anfertigung einer Kopie des speichernden Datenträgers,

um auf dieser die versichertenbezogenen Daten zu pseudonymisieren, mit für die Qualitätssicherung nicht hinnehmbaren Qualitätsverlusten verbunden sein. Die korrekte Beschriftung von Aufnahmen aus bildgebenden Verfahren mit patientenidentifizierbaren Daten sei Teil der Qualitätssicherung und Qualitätsprüfung.
Der TLfDI wies die KV nach diesem Vorbringen darauf hin, dass nach § 299 Abs. 1 Satz 5 Nr. 2, letzter Halbsatz SGB V die Gründe nach § 299 Abs. 1 Satz 5 Nr. 2 SGB V in den Richtlinien darzulegen sind. Eine derartige Darlegung konnte der von der KV übermittelten Vereinbarung nicht entnommen werden. Hierzu wurde die KV erneut um Stellungnahme gebeten. Daraufhin stellte die KV Thüringen klar, dass sich die von ihr durchgeführte Qualitätssicherungsmaßnahme nicht auf § 299 SGB V, sondern auf die Durchführung eines Qualitätssicherungsverfahrens nach § 135a Abs. 2 SGB V beziehe. Danach sind die Leistungserbringer zur Sicherung und Weiterentwicklung der Qualität der von ihnen erbrachten Leistungen verpflichtet. Vertragsärzte sind nach § 135a Abs. 2 SGB V verpflichtet, sich an einrichtungsübergreifenden Maßnahmen zur Qualitätssicherung zu beteiligen, die zum Ziel haben, die Ergebnisqualität zu verbessern. Die Qualitätsvereinbarungen nach § 135a Abs. 2 SGB V werden von der Regelung des § 299 SGB V nicht erfasst.
Die KV Thüringen legte die Vereinbarung von Qualitätssicherungsmaßnahmen nach § 135a Abs. 2 SGB V zur Ultraschalldiagnostik (Ultraschall-Vereinbarung) vom 31. Juli 2008 vor. Nach deren § 11 fordert die KV Thüringen jährlich von mindestens drei Prozent der Ärzte, denen eine Genehmigung zur Ausführung und Abrechnung sonografischer Leistungen in der vertragsärztlichen Versorgung erteilt worden ist, die Dokumentation zu fünf abgerechneten Ultraschalluntersuchungen an. Die Auswahl des Arztes und die Auswahl der Dokumentationen erfolgt gemäß der Ultraschallvereinbarung nach dem Zufallsprinzip unter Angabe des Patientennamens und des Untersuchungsdatums. Damit erfolgte die Anforderung der fünf Dokumentationen von dem Arzt auf einer Rechtsgrundlage. Dies wurde dem Beschwerdeführer mitgeteilt und das Verfahren gegenüber der KV Thüringen für erledigt erklärt.

Im Bereich der kassenärztlichen Versorgung gibt es vielfältige Maßnahmen zur Qualitätssicherung. Hierzu ist in manchen Fällen die Anforderung von Patientendaten durch die kassenärztliche Vereinigung erforderlich, in anderen Fällen genügt die Anforderung von

pseudonymisierten Daten. Es ist in jedem Einzelfall sehr sorgfältig zu prüfen, aufgrund welcher Rechtsgrundlage Unterlagen von einem Arzt angefordert werden können.

12.30 Übermittlung von Sozialdaten

Im Berichtszeitraum erhielt der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) die Information, dass das Bundesministerium für Familie, Senioren, Frauen und Jugend (BMFSFJ) zur Erstellung des nach § 25 Bundeselterngeld- und Elternzeitgesetz (BEEG) geforderten Berichts über die Auswirkung der Regelung zum Elterngeld Plus und zum Partnerschaftsbonus ein Institut beauftragt hat. Hierfür solle eine Befragung von Bezieherinnen und Beziehern des Elterngeldes Plus und/oder des Partnerschaftsbonusses durchgeführt werden. Für die Befragung wurden die Namen, Anschriften und Telefonnummern von Beziehern benötigt, die in Thüringen nach Stand für den Februar 2017 Elterngeld Plus oder den Partnerschaftsbonus beantragt hatten und in deren Anträgen eine Telefonnummer angegeben wurde. Für die Befragung war zudem die Information notwendig, für wie viele Monate das Elterngeld Plus und/oder der Partnerschaftsbonus jeweils beantragt wurde. Das BMFSFJ und das Institut stützen sich diesbezüglich auf §§ 14 und 16 Bundesdatenschutzgesetz (BDSG). Demnach ist die Übermittlung personenbezogener Daten an nicht-öffentliche Stellen zulässig, wenn sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgaben erforderlich ist und die Voraussetzungen vorliegen, die eine Nutzung nach § 14 BDSG zulassen würden.
Der TLfDI vertritt die Auffassung, dass es sich bei den Leistungen nach dem BEEG um Sozialleistungen nach § 25 Sozialgesetzbuch (SGB) Erstes Buch (I) handelt, d. h. die zu übermittelnden Daten sind Sozialdaten im Sinne des § 67 Abs. 1 Satz 1 SGB Zehntes Buch (X). Für Sozialdaten gilt nach § 35 Abs. 1 Satz 1 SGB I das Sozialgeheimnis. Eine Erhebung, Verarbeitung und Nutzung von Sozialdaten ist nur unter den Voraussetzungen des 2. Kapitels des SGB X zulässig. Nach § 67d Abs. 1 SGB X ist eine Übermittlung von Sozialdaten nur zulässig, soweit eine gesetzliche Übermittlungsbefugnis nach den §§ 68 bis 77 oder nach einer anderen Rechtsvorschrift in diesem Gesetzbuch vorliegt. Hier wäre der § 75 SGB X anzuwenden. Demnach wäre eine Übermittlung zulässig, soweit diese erforderlich für ein bestimmtes Vorhaben der wissenschaftlichen Forschung im

Sozialleistungsbereich oder der wissenschaftlichen Arbeitsmarkt- und Berufsforschung oder der Planung im Sozialleistungsbereich durch eine öffentliche Stelle im Rahmen ihrer Aufgaben ist und schutzwürdige Interessen des Betroffenen nicht beeinträchtigt werden oder das öffentliche Interesse an der Forschung oder Planung das Geheimhaltungsinteresse des Betroffenen erheblich überwiegt. Im Hinblick auf die in § 25 BEEG geregelte Berichtspflicht dürften insoweit die Voraussetzungen des § 75 Abs. 1 Satz 1 SGB X als erfüllt betrachtet werden. Nach § 75 Abs. 1 S. 3 SGB X dürfen neben Angaben über den Familien- und Vornamen, die Anschrift und die Telefonnummer auch die für die Einleitung eines Vorhabens nach Satz 1 zwingend erforderlichen Strukturmerkmale der Betroffenen für Befragungen ohne Einwilligungen übermittelt werden.
Das Thüringer Ministerium für Arbeit, Soziales, Gesundheit, Frauen und Familie (TMASGFF) bestätigte auf Nachfrage, dass das Anschreiben einen Hinweis auf die Freiwilligkeit enthält und damit keine datenschutzrechtlichen Bedenken bestehen dürften. Der TLfDI teilt aus den oben gennannten Gründen diese Auffassung.

Für die Übermittlung von personenbezogenen Daten und speziell für Sozialdaten gelten besondere datenschutzrechtliche Bestimmungen. So muss nach § 67d SGB X eine Übermittlungsbefugnis vorliegen. Nach § 75 SGB X ist eine Übermittlung zulässig, soweit sie für ein bestimmtes Vorhaben der wissenschaftlichen Forschung im Sozialleistungsbereich oder der wissenschaftlichen Arbeitsmarkt- und Berufsforschung oder der Planung im Sozialleistungsbereich durch eine öffentliche Stelle im Rahmen ihrer Aufgaben erforderlich ist und schutzwürdige Interessen des Betroffenen nicht beeinträchtigt werden oder das öffentliche Interesse an der Forschung oder Planung das Geheimhaltungsinteresse des Betroffenen erheblich überwiegt.

12.31 Silver Economy

Der demografische Wandel schreitet voran: Immer mehr ältere Menschen leben allein in ihren Häusern und Wohnungen, teilweise fernab von städtischen Strukturen. Um weiterhin selbstbestimmt leben zu können, brauchen sie Ansprechpartner bei Fragen und Hilfestellungen im Alltag. Die Unternehmen und die wissenschaftlichen Einrichtungen der „Silver Economy“ haben bereits eine Vielzahl von Produkten und altersgerechten Assistenz-Systemen für ein selbstbe-

stimmtes Leben entwickelt. Ein Thüringer Unternehmen will sich diesen Herausforderungen stellen, in einem Innovationsforum Ideen generieren und im Rahmen eines entstehenden Netzwerkes die Realisierung von derartigen Produkten auf den Weg bringen. Für die dafür notwendige Netzwerkbildung erhält das Unternehmen Fördermittel des Bundesministeriums für Bildung und Forschung (BMBF). Im Laufe der Umsetzung des Projekts wurde festgestellt, dass möglicherweise auch die Erhebung, Speicherung und Übermittlung von Patientendaten eine Rolle spielen kann. Viele Hilfestellungen für ältere Personen erfordern eine Kommunikation auch zu medizinischen oder sozialen Dienstleistungen der älteren Bevölkerung. Das Unternehmen bat daher den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) um Beratung.
Während eines Termins beim TLfDI stellte die Initiative ihr Projekt näher vor. Bislang wurden nur erste Vorüberlegungen angestellt. Zunächst sollen Senioren an die Technik herangeführt und eine Kommunikationsplattform eingeführt werden, auf der sich ältere Menschen anmelden können. In einem zweiten Schritt sollen den Menschen gewisse technische Produkte angeboten werden. Die Einbindung von sogenannten Smart-Home-Produkten soll möglich sein. In einem dritten Schritt soll es schließlich auch eine telemedizinische Anwendung zwischen Hausarzt, Pflegedienst und Patienten geben.
Der TLfDI wies darauf hin, dass eine Datenerhebung, Speicherung und auch eine Übermittlung an Dritte nur dann zulässig ist, wenn es hierfür eine Rechtsgrundlage bzw. eine informierte Einwilligung in die Datenverarbeitung durch die Betroffenen gibt, § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG). Außerdem müssen die Vorgaben des § 9 BDSG an die erforderlichen technischen und organisatorischen Maßnahmen eingehalten werden. Der Initiative wurde deutlich gemacht, dass bei einer Einbeziehung einer Cloudlösung hohe Anforderungen an die technischen und organisatorischen Maßnahmen zu stellen sind. Hier ist insbesondere darauf zu achten, dass der Zugriff durch Unberechtigte verhindert wird und das Unternehmen als verantwortliche Stelle nach wie vor Herr der Daten bleibt.
Grundsätzlich sind derartige Projekte möglich, wenn mit den Betroffenen, die sich auf der Plattform anmelden, ein entsprechender Vertrag geschlossen wird, der dann Rechtsgrundlage für die Verarbeitung ist, § 28 Abs. 1 Nr. 1 BDSG. In technischer und organisatorischer Hinsicht sind umso strengere Maßstäbe anzulegen, je höher der Schutzbedarf der Daten ist. Jedenfalls ab dem Moment, ab dem

auch besondere Kategorien von Daten, wie beispielsweise Gesundheitsdaten nach § 3 Abs. 9 BDSG, ins Spiel kommen, muss die Kommunikation auf sicher verschlüsselten Kommunikationswegen erfolgen und die Daten müssen verschlüsselt und sicher vor dem Zugriff Dritter abgelegt werden. Der TLfDI sicherte zu, das Projekt weiterhin datenschutzrechtlich zu begleiten.

Der demografische Wandel bringt es mit sich, dass neue Lösungen für die Versorgung von lebensälteren Personen und ihre Möglichkeit zur gesellschaftlichen Teilhabe geschaffen werden. Ein wichtiges Hilfsmittel stellt dabei die digitale Kommunikation sowohl mittels technischer Geräte (Smart Home) als auch digitaler Assistenzsysteme dar. Der datenschutzgerechte Gebrauch setzt voraus, dass durch technische und organisatorische Maßnahmen ausgeschlossen werden kann, dass Unberechtigte auf die Daten der Betroffenen zugreifen. Der TLfDI wird die Initiierung solcher Projekte in Thüringen datenschutzrechtlich gern begleiten.

12.32 Besonders zu schützende Daten Dritter als Zugabe

Eine beihilfeberechtigte Beamtin hatte bei der Beihilfestelle einen Heil- und Kostenplan für eine zahnärztliche Behandlung eingereicht, um zu erfahren, mit welcher Kostenerstattung sie rechnen könne. Die Beihilfestelle teilte ihr schriftlich mit, nach der Thüringer Beihilfeverordnung sei die Vorlage eines Heil- und Kostenplans zur zahnärztlichen Behandlung nicht erforderlich. Bei der Auskunft über die voraussichtliche Höhe der Beihilfe zu eingereichten Heil- und Kostenplänen handele es sich um eine freiwillige Serviceleistung, welche die Beihilfestelle nicht mehr erbringen könne. Was sie letztendlich erstattet erhalte, werde erst nach Vorlage der Rechnung entschieden. Dem Schreiben fügte die Beihilfestelle den von der Beamtin eingereichten Heil- und Kostenplan und einen weiteren für eine ihr völlig fremde Person erstellten Heil- und Kostenplan bei. Sie wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), weil sie nicht wissen wollte, was die Zähne anderer Leute kosten sollten und sich unschlüssig war, was sie denn mit dem fremden Heil- und Kostenplan unternehmen sollte. Außerdem machte sie sich Sorgen, weil die andere Person ja dann gar nicht erfahre, was diese erstattet erhalten könnte.

Der TLfDI forderte die Beihilfestelle auf, die konkrete Angelegenheit zur Übersendung eines falschen Heil- und Kostenplans an den Beschwerdeführer zu prüfen. Da mit dem falschen Heil- und Kostenplan besonders zu schützende Daten (§ 4 Abs. 5 Thüringer Datenschutzgesetz) einer unbefugten Personen zur Kenntnis gelangt waren, mussten auch unverzüglich die erforderlichen Maßnahmen getroffen werden, nämlich die dritte Person hierüber zu informieren. Diese Pflicht zur Information resultiert aus § 5 Abs. 1 Nr. 6 ThürDSG, nach dem Betroffene über rechtmäßige Übermittlungen zu informieren sind. Bei unrechtmäßigen Übermittlungen muss dies daher erst recht gelten.
Der TLfDI prüfte in diesem Zusammenhang auch die aktuellen im Intranet veröffentlichten Hinweise der Beihilfestelle. Diese informierten darüber, dass die Vorlage eines Heil- und Kostenplanes vor Beginn einer zahnärztlichen Behandlung grundsätzlich nicht erforderlich sei, da die Beihilfevorschriften auch bei umfangreichen zahnärztlichen Maßnahmen kein Voranerkennungsverfahren vorsehen. Ausnahmen bestünden nur bei kieferorthopädischen Behandlungen. Die Formulierung im Schreiben der Beihilfestelle an die Beschwerdeführerin ließ die Vermutung zu, dass offenbar in der Vergangenheit zu eingereichten Heil- und Kostenplänen die zu erwartende Kostenerstattung berechnet worden war, sodass sich die Betroffenen auf eine eventuelle eigene finanzielle Belastung einstellen konnten. Da dies aber nun nicht mehr der Fall sein sollte und die Formulierung der Hinweise im Intranet etwas kryptisch erschien, war nicht auszuschließen, dass nicht erforderliche personenbezogene Daten in Form von Heil- und Kostenplänen wegen zahnärztlicher Behandlung an die Beihilfestelle übersandt werden, zu denen letztendlich keine Bearbeitung erfolgt.
Der TLfDI bat daher die Beihilfestelle um Mitteilung, welche geeigneten Maßnahmen von dort aus getroffen werden können, um zukünftig die unnötige Übersendung von Heil- und Kostenplänen wegen zahnärztlicher Behandlung zu unterbinden bzw. einzuschränken, wenn eine Auskunft als freiwillige Serviceleistung nicht erbracht werden kann.
Die Beihilfestelle teilte mit, sie habe die betroffene andere Person darauf hingewiesen, dass jemand anderes durch unbefugte Weitergabe ihrer Daten Kenntnis von ihrem Heil- und Kostenplan erhalten habe. Weiterhin hat die Beihilfestelle in ihrem Internetauftritt den Hinweis zur Behandlung des allgemeinen Heil- und Kostenplans

dahingehend geändert, dass eine Vorabauskunft über die voraussichtliche Höhe der Beihilfe zu einem Heil- und Kostenplan vor Beginn einer zahnärztlichen Behandlung grundsätzlich nicht mehr erfolge. Dies könne nur noch in besonders begründeten Einzelfällen geschehen, an die ein strenger Maßstab anzulegen ist.

Erhält eine unbeteiligte Person besonders zu schützende Gesundheitsdaten unzulässigerweise zur Kenntnis, ist die betroffene Person hiervon zu unterrichten (§ 5 Abs. 1 Nr. 6 ThürDSG). Um zu vermeiden, dass letztendlich nicht erforderliche personenbezogene Daten von Beihilfeberechtigten übersandt werden, sollten sie im Wege allgemeiner Hinweise korrekt aufgeklärt werden.

12.33 Kamera an bei psychiatrischer Begutachtung?

Ein Arzt wandte sich mit der Bitte um Beratung an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Er habe sich in der Vergangenheit in einem Rechtsstreit mit der Landesärztekammer Thüringen befunden, bei der es um die Aberkennung seiner Approbation gegangen sei. Im Rahmen dieses Verfahrens sei er von einem Psychiater als Sachverständigen begutachtet worden. Dabei hätte es entgegen seinem ausdrücklichen Wunsch keine Dokumentation des Gesprächs mit einer Kamera gegeben. Er hätte es bevorzugt, wenn bei einem derartigen Verfahren seine Begutachtung aus Beweisgründen durch eine Videoaufzeichnung mit Tonaufnahmen dokumentiert worden wäre.
Aus datenschutzrechtlicher Sicht müssen hier zwei Interessen gegeneinander abgewogen werden. Zum einen dienen die nach dem Datenschutzrecht zu treffenden technischen und organisatorischen Maßnahmen der Integrität der erhobenen personenbezogenen Daten während der Verarbeitung, § 9 Abs. 2 Nr. 2 Thüringer Datenschutzgesetz (ThürDSG). Andererseits hat der begutachtende Psychiater auch ein schützenswertes Interesse daran, keinerlei Leistungskontrolle im Hinblick auf seine Arbeit zu unterliegen. Es muss daher in einem derartigen Fall eine Abwägung geben zwischen dem Interesse des Betroffenen an einer angemessenen Dokumentation der Datenverarbeitung einerseits und dem Interesse des begutachtenden Arztes andererseits. Möglicherweise kann eine hinreichende Dokumentation auch schriftlich oder durch reine Tonaufzeichnung erfolgen.

Die Landesärztekammer Thüringen wurde um Stellungnahme dazu gebeten, was aus fachlicher Sicht dagegen spricht, wenn derartige Begutachtungen, bei denen es um existentielle Fragen wie beispielsweise die Geschäftsfähigkeit einer Person geht, auf ausdrücklichen Wunsch des zu Begutachtenden durch Kameraaufnahmen dokumentiert würden. Die Landesärztekammer teilte mit, dass hierzu fachliche Expertise eingeholt werden müsse und daher eine abschließende Stellungnahme noch nicht möglich sei. Der TLfDI wies die Landesärztekammer auf ihre Pflicht zur Unterstützung nach § 38 Abs. 1 ThürDSG hin, nach der dem TLfDI unverzüglich Auskunft zu seinen Fragen gegeben werden muss.
Die Landesärztekammer teilte daraufhin mit, dass die Forderung, gutachterliche Untersuchungen durch Videoaufnahmen zu begleiten, immer wieder gestellt werde. Berufsrechtlich gäbe es keine entsprechende ausdrücklich geregelte Pflicht für die begutachtenden Ärzte. Auch aus der Rechtsprechung sei nicht bekannt, dass bei der Begutachtung des Gesundheitszustandes eines Patienten zur Feststellung der Geeignetheit für einen Beruf eine Videodokumentation zur ordnungsgemäßen Begutachtung gefordert werde. Insofern liege es in der Entscheidung des Arztes zu beurteilen, ob dies sinnvoll ist. Dabei kann nicht nur das Interesse des Patienten eine Rolle spielen, sondern es müsste dieses gegen die Persönlichkeitsinteressen des Arztes abgewogen werden. Mitunter kann eine filmische Dokumentation auch für die Gesundheit des Patienten kontraproduktiv sein. Der Vorwurf einer Falschbegutachtung könne bei Bedarf durch ein entsprechendes Gegengutachten überprüft werden. Diese Auffassung teilt der TLfDI und unterrichtete den Beschwerdeführer entsprechend.

Datenschutzrechtlich muss das Interesse des einen Betroffenen an einer ordnungsgemäßen Dokumentation der Datenerhebung und -verarbeitung gegen das Interesse des anderen Betroffenen daran, keiner Leistungskontrolle unterzogen zu werden, abgewogen werden. Geht es für den einen Betroffenen um existentielle Fragen, wie beispielsweise den Verlust der Geschäftsfähigkeit, muss möglicherweise das Interesse des anderen Betroffenen zurücktreten.

12.34 Unerlaubter Datenaustausch zwischen Krankenkasse und MDK?

Ein Elternpaar wandte sich Hilfe suchend an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Ihr Sohn sei volljährig und schwerbehindert, ihm wurde eine Pflegestufe zuerkannt. In diesem Zusammenhang hätte es eine unzulässige Datenübermittlung zwischen seiner Krankenkasse und dem Medizinischen Dienst der Krankenkasse (MDK) gegeben. Im Vorfeld sei in diesem Zusammenhang die Begutachtung des Sohnes seitens des MDK in einem anderen Bundesland durchgeführt worden.

Sie hätten dann zu einem späteren Zeitpunkt die Mitteilung der Krankenkasse ihres Sohnes erhalten, dass ein Begutachtungsauftrag an den MDK in Thüringen gegangen sei und sie noch ärztliche Unterlagen vorlegen bzw. beibringen sollten. Gleichzeitig wurde die Reha-Klinik benannt, in der der Sohn behandelt werden sollte. Dabei hätten sie der Krankenkasse keine Einwilligung in die Datenübermittlung gegeben. Eine Woche später habe sie die Pflegekasse darüber unterrichtet, dass die Gutachterin eine Rehabilitationsmaßnahme empfohlen habe und legte Antragsunterlagen bei. Damit habe die Krankenkasse bzw. Pflegekasse unerlaubt Daten an den MDK in Thüringen übermittelt.

Nach § 11 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) kann sich jedermann mit dem Vorbringen an den Landesbeauftragten für den Datenschutz wenden, durch öffentliche Stellen in Thüringen seien seine schutzwürdigen Belange beeinträchtigt. Da sich der betroffene Sohn nicht selbst an den TLFDI wandte, konnten die Eltern seine Beschwerde nur wirksam vorbringen, weil sie eine entsprechende Vollmacht vorlegten. Da die Pflege- und Krankenkasse des Sohnes ihren Sitz in einem anderen Bundesland hatte, gab der TLfDI die Beschwerde dorthin ab. Zuständig ist der TLfDI allerdings für den MDK. Dieser wurde zu dem Vorgang um Stellungnahme gebeten. Liegt eine Datenübermittlung vor, sind immer zwei Seiten zu betrachten: die Stelle, die die personenbezogenen Daten übermittelt und diejenige, die sie erhält. Wenn diese Stelle die Daten speichert, handelt es sich nach § 67 Abs. 6 Sozialgesetzbuch (SGB) Zehntes Buch (X) um eine Verarbeitung von Daten, die einer gesetzlichen Ermächtigung bedarf, § 67b SGB X.

Der MDK teilte mit, dass bei ihm keine personenbezogenen Daten des Betroffenen gespeichert sind. Eine Gutachterin des MDK habe eine sozialmedizinische Fallberatung in den Geschäftsräumen der Krankenkasse in Erfurt durchgeführt. Dabei wurden die fallbezogenen Unterlagen eingesehen und verblieben bei der Krankenkasse. Für statistische Zwecke wurden die Frage des Auftraggebers sowie das Ergebnis erfasst. Aber es erfolgte keine Speicherung personenbezogener Daten seitens des MDK Thüringen. Da der MDK folglich ihm möglicherweise unzulässig übermittelte Daten nicht gespeichert hatte, sah der TLfDI die Angelegenheit als erledigt an.

Liegt eine Datenübermittlung vor, sind aus datenschutzrechtlicher Sicht immer zwei Seiten zu betrachten: die Stelle, die die personenbezogenen Daten übermittelt und diejenige, die sie erhält. Nur wenn Letztere diese Daten auch speichert, liegt eine Datenverarbeitung vor, die einer gesetzlichen Ermächtigungsgrundlage bedarf.

12.35 Informationsflyer zum Neugeborenen-Sreening

Das Thüringer Ministerium für Arbeit, Soziales, Gesundheit, Frauen und Familie (TMASGFF) wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und bat um datenschutzrechtliche Prüfung eines Informationsflyers zum sogenannten Neugeborenen-Sreening. Das Neugeborenen-Screening ist eine Reihenuntersuchung von Neugeborenen, um angeborene Stoffwechselerkrankungen und Hormonstörungen frühzeitig zu erkennen.
Bereits vor rund zehn Jahren war ein Flyer vom damaligen Thüringer Sozialministerium und dem Versorgungszentrum für Kinder im Thüringer Landesamt für Verbraucherschutz (TLV) mit dem TLfD abgestimmt worden. Aufgrund der Einführung des Mukoviszidose-Screenings war jetzt eine Aktualisierung des Flyers erforderlich. Insbesondere wurde der TLfDI hierbei gebeten, die im Flyer enthaltene Einverständniserklärung zur Untersuchung der Neugeborenen datenschutzrechtlich zu bewerten.
In der geplanten Langversion des Flyers werden die Gründe für die Übermittlung der personenbezogenen Daten konkretisiert. In der vorliegenden, vom TLfDI zu prüfenden Kurzversion des Informationsflyers wird dargelegt: „Früherkennung und Frühbehandlung für betroffene Neugeborene sind nur möglich, wenn alle Beteiligten –

Eltern, Klinik bzw. Kinderarzt, Screening-Labor und Stoffwechselzentrum – ohne Zeitverlust zusammenarbeiten, damit die Untersuchungsergebnisse rechtzeitig erhoben und kontrolliert werden."
Nach Prüfung teilte der TLfDI dem TMASGFF mit, dass der Informationsflyer die Betroffenen verständlich und umfassend über die Früherkennungsuntersuchung und deren Verfahrensweise aufklärt. Der TLfDI wies jedoch darauf hin, dass in den Text noch eine Information über die bestehenden Rechtsgrundlagen der Durchführung des Screenings aufgenommen werden sollte. Dies sind hier insbesondere §§ 8, 9 des Gesetzes über genetische Untersuchungen bei Menschen (Gendiagnostikgesetz – GenDG), nach einem positiven Befund auch § 10 GenDG sowie die „Richtlinie des Gemeinsamen Bundesausschusses über die Früherkennung von Krankheiten bei Kindern bis zur Vollendung des 6. Lebensjahres" (Kinder-Richtlinie). Außerdem wies der TLfDI darauf hin, dass für Dritte nicht unmittelbar einsichtig ist, aus welchen Gründen personenbezogene Daten der Betroffenen und deren Neugeborenen an die im Flyer genannten drei Stellen übermittelt werden (Screening-Labor Leipzig, Stoffwechselzentrum Thüringen der Uniklinik Jena und an das Thüringer Vorsorgezentrum für Kinder). Hier sollte noch dargelegt werden, wer welche Daten zu welchen Zwecken wie lange benötigt.
Nach Informationen des mit der Untersuchungsorganisation befassten Universitätsklinikums sollte der Informationsflyer kurzfristig in Druck gehen. Aufgrund der Eilbedürftigkeit schlug das Klinikum in Abstimmung mit dem TMASGFF vor, zunächst nur 3000 Exemplare zu drucken und zwischenzeitlich die Änderungen in die 2. Druckauflage einzuarbeiten. Im Hinblick auf die medizinische Eilbedürftigkeit teilte der TLfDI dem TMASGFF mit, dass er aus datenschutzrechtlicher Sicht diesem Vorschlag zustimmt. Gleichzeitig bat der TLfDI darum, ihm den überarbeiteten Entwurf des Flyers zur erneuten Prüfung zuzusenden.
Nach Freigabe übersandte das Klinikum die PDF-Version des Informationsflyers an das Screening-Labor Leipzig sowie an das TLV/Vorsorgezentrum und an das Stoffwechselzentrum Thüringen zur Veröffentlichung auf den jeweiligen Homepages.

Im Rahmen des Neugeborenen-Screenings zur Feststellung von Stoffwechselerkrankungen werden notwendigerweise aus medizinischen Gründen auch personenbezogene Daten erhoben. Rechtsgrundlage hierfür bildet das Gendiagnostikgesetz, §§ 8 und 9 und –

im Falle eines positiven Befundes – § 10 sowie die Richtlinie des Gemeinsamen Bundesausschusses über die Früherkennung von Krankheiten bei Kindern bis zur Vollendung des 6. Lebensjahres (Kinder-Richtlinie).

12.36 Zentralregister für Gesundheitsberufe zum Abgleich von Mehrfachantragsstellungen

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichte aus dem Kreise der Datenschutzbeauftragten des Bundes und der Länder der Hinweis, dass die Einrichtung eines Zentralregisters zur Bewertung eines Berufsabschlusses im Ausland in einem Gesundheitsberuf geplant sei. Das einzurichtende Zentralregister soll der Vermeidung von Doppel- oder Mehrfacharbeit dienen, da gelegentlich Antragsteller in mehreren Bundesländern vorstellig werden, um ihre Chancen zu erhöhen. Die Länderbehörden sollen nach bisheriger Konzeption über eine verschlüsselte Verbindung auf einen Server der Gutachtenstelle zugreifen können. Liegt bereits ein Antrag der Person vor, erfolgt die Rückmeldung einschließlich des Hinweises auf die Behörde, Eingabedatum und Ansprechpartner. Erfolgt keine Rückmeldung des Registers, werden die Anfragedaten der Landesbehörde inhaltlich und mit Hinweis auf die anfragende Behörde für eventuelle künftige Abgleiche gespeichert.
Die Durchführung der Bewertung des ausländischen Berufsabschlusses durch die gemeinsame Gutachtenstelle und der Abgleich mit einem Register zur Erleichterung der Arbeit dürften mangels spezifischer Grundlage auf Basis der Landesdatenschutzgesetze unzulässig sein. Die Übermittlung der Daten an die gemeinsame Gutachtenstelle kann nicht nach § 21 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) erfolgen, weil die Erhebung dieser Daten nicht für diese Zwecke erfolgt ist, § 21 Abs. 1 Nr. 2 in Verbindung mit § 20 Abs. 1 ThürDSG. Die Übermittlung bedarf vielmehr einer separaten Rechtsgrundlage, § 20 Abs. 2 Nr. 1 ThürDSG. Die Voraussetzungen für § 20 Abs. 2 Thür DSG liegen nicht vor. Fraglich erschien die Rechtsgrundlage für die Übermittlung der Antragstellerdaten an das Register auch zu dem Zweck, sie für Anfragen anderer Länder weiter zu speichern.
In diesem Zusammenhang wandte sich der TLfDI an das Thüringer Ministerium für Arbeit, Soziales, Gesundheit, Frauen und Familie

(TMASGFF). Er bat um Mitteilung, welche Rechtsauffassung das Ministerium zur Zulässigkeit eines Abgleichs bei Mehrfachanträgen und zur Frage des Vorhalts der Daten beim Register für Abfragen anderer Landesbehörden bei dem vorgesehenen Register vertritt. Das TMASGFF ist der Rechtsauffassung des TLfDI, dass in den Ländern wortgleiche Rechtsgrundlagen in Bezug auf die Verarbeitung und Nutzung der personenbezogenen Daten durch öffentliche Stellen bei dem zu errichtenden Zentralregister geschaffen werden sollten, um Rechtssicherheit zu erhalten und künftige Interpretationsdifferenzen auszuschließen. Das zuständige Ressort bat gleichzeitig um Beratung und Unterstützung durch den TLfDI zur datenschutzrechtlichen Zulässigkeit im Zusammenhang mit der Errichtung des o. g. Zentralregisters. Der TLfDI wird das Verfahren weiter begleiten.

Nach den Erfahrungen der für die Approbation/Berufsanerkennung zuständigen Behörden kommt es vermehrt vor, dass ausländische Antragsteller einen Antrag auf Anerkennung ihres ausländischen Berufsabschlusses gleichzeitig in mehreren Ländern stellen. Um dies zu umgehen, beabsichtigt die Gutachtenstelle für Gesundheitsberufe ein Zentralregister einzuführen. Für die damit verbundene Übermittlung und Verarbeitung personenbezogener Daten muss allerdings noch eine Rechtsgrundlage geschaffen werden.

12.37 Personenbezogene Daten sind beim Versand auch durch Brief- und Postgeheimnis geschützt

Ein Patient richtete sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), weil er auf seine Anfrage keine Antwort von der Landesärztekammer Thüringen erhalten hatte. Der Anfrage lag folgender Sachverhalt zugrunde:
Anfang des Jahres 2016 wurde er an eine radiologische Praxis für eine MRT-Diagnose überwiesen. Die Diagnose des Radiologen erreichte den behandelnden Arzt jedoch erst sieben Wochen später, nachdem die Originale des Gutachtens mehrmals in der Post verloren gegangen zu sein schienen. Der Betroffene wollte wissen, ob entsprechende Vorschriften zur Datensicherung beim Versand von medizinischen Daten bestehen, da medizinische Daten besonders schützenswert sind.
Der TLfDI teilte dem Beschwerdeführer mit, dass aus datenschutzrechtlicher Sicht keine Bedenken gegen das Versenden von medizi-

nischen Daten per Post vorliegen. Aufgrund der zu treffenden technischen und organisatorischen Maßnahmen ist sicherzustellen, dass je nach Art der zu schützenden Daten gewährleistet ist, dass nur Befugte personenbezogene Daten zur Kenntnis nehmen können, § 9 Thüringer Datenschutzgesetz bzw. § 9 Bundesdatenschutzgesetz. Dank des bestehenden Postgeheimnisses ist davon auszugehen, dass unbefugte Dritte auf die Diagnose keinen unberechtigten Zugriff erhalten, wenn diese per Post versandt wird. Nach § 5 des Postgesetzes bedarf der Erlaubnis, wer Briefsendungen gewerbsmäßig für andere befördert. Eine solche Erlaubnis wird nur auf schriftlichen Antrag von der Regulierungsbehörde erteilt, wenn der Postdienstleister die erforderliche Fachkunde besitzt, leistungsfähig und zuverlässig ist. Gemäß Art. 10 Grundgesetz (GG) sind das Brief- sowie das Postgeheimnis unverletzlich. Die Unverletzlichkeit des Briefgeheimnisses bedeutet, dass jede schriftliche Mitteilung, welche an einen individuellen Empfänger gerichtet ist, ausschließlich von diesem selbst zu öffnen ist. Das Briefgeheimnis umfasst jedes Schriftstück, das verschlossen bzw. durch ein verschlossenes Behältnis gegen Kenntnisnahme gesondert gesichert ist. Außerdem ist die Verletzung des Briefgeheimnisses nach § 202 Strafgesetzbuch (StGB) eine Straftat.
Datenschutzrechtlich ist es wesentlich bedenklicher, wenn Diagnosen per Fax oder gar per einfacher E-Mail versandt werden. Bei einem Fax steht zu befürchten, dass möglicherweise unberechtigte Dritte Zugang zu dem Faxgerät haben und die Diagnose lesen könnten. Hier muss beim Empfänger eine entsprechende Vorkehrung getroffen werden. Bei einer unverschlüsselten E-Mail ist ein Zugriff unberechtigter Personen in noch stärkerem Maße zu befürchten.
Der Patient wurde von dem TLfDI darüber informiert, dass der Radiologe mit der Versendung der Diagnose per Post die datenschutzrechtlich sicherste Variante gewählt hat. Die Verspätung konnte allenfalls dem beauftragten Postdienstleister zur Last gelegt werden.

Aus datenschutzrechtlicher Sicht wird das Versenden medizinischer Daten per Post empfohlen. Das Brief- und Postgeheimnis ist nach Art. 10 GG unverletzlich und nach § 202 StGB macht sich strafbar, wer es verletzt. Datenschutzrechtlich ist es wesentlich bedenklicher, wenn Diagnosen per Fax oder gar per einfacher E-Mail versandt werden.

12.38 Gemeinsam für den Datenschutz: Workshops mit der Landeskrankenhausgesellschaft Thüringen

Im Rahmen seiner Arbeit führte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) gemeinsam mit der Landeskrankenhausgesellschaft Thüringen (LKHG) regelmäßige Workshops für die Datenschutzbeauftragten der Krankenhäuser in Thüringen durch.
Im Rahmen der Workshops haben sich im Berichtszeitraum folgende „Hauptprobleme“ herauskristallisiert: Sperr- und Löschkonzepte von Patientendaten, Umgang mit besonders schützenswerten Personendaten (VIP-Problematik), Heranziehung von Vorbehandlungsdaten im Falle von Widersprüchen, Detailprobleme der Rollen- und Berechtigungskonzepte für den Datenzugriff, Protokollierung von lesenden und schreibenden Zugriffen auf die Patientendaten.
Ein Widerspruch des Patienten gegen den Zugriff auf Vorbehandlungsdaten erweist sich inhaltlich als sehr problematisch. Insbesondere besteht das Problem, dass eine wirksame ärztliche Aufklärung über die Risiken des Widerspruchs gegen Einsicht der Vorbehandlungsdaten nur dann erfolgen kann, wenn der/die Arzt/Ärztin die Vorbehandlungsdaten kennt und somit die konkreten Risiken tatsächlich benennen kann. Insofern erscheint den Krankenhäusern die Forderung des Widerspruchsrechtes aus Haftungsgesichtspunkten riskant. Eine pauschale Aufklärung ist aus Haftungsgründen unzulässig. Grundsätzlich muss der Patient bei einer Bewegung im Haus immer neu aufgeklärt werden, da möglicherweise neue Visiten im Rahmen der Behandlung entstehen können. Daher müssen hierzu konkrete rechtliche Regelungen getroffen werden.
Zugriffe des Krankenhauspersonals auf die erforderlichen pflegerischen und medizinischen Daten sind auf die zuständigen Mitarbeiter zu begrenzen und genau in einer Dienstvereinbarung festzulegen; unberechtigte Zugriffe sind mit arbeitsrechtlichen Konsequenzen zu belegen. Das Pflegepersonal muss entsprechende Schulungen erhalten. Jeder Versuch, auf Patientendaten zuzugreifen, muss protokolliert werden. In einem Thüringer Klinikum befasst sich eine Arbeitsgruppe speziell mit dieser Problematik. Hier werden seit Anfang 2017 mithilfe eines speziellen Formblatts stichprobenartige Prüfungen durchgeführt. Hierbei haben sich insbesondere die Pflege-Gruppen-Logins als problematisch erwiesen. Der TLfDI wies darauf hin, dass die Ausgestaltung der Zugriffsrechte noch nicht in allen

Thüringer Krankenhäusern optimal ist, das Rollen- und Berechtigungskonzept wird teilweise noch überarbeitet.
Für den Umgang mit besonders schützenswerten Personendaten existieren fünf verschiedene Systeme in Thüringen. Ein Thüringer Klinikum hat Hinweise und eine Einwilligungserklärung zur Pseudonymisierung von Mitarbeiterdaten erarbeitet und eine Stelle benannt, an die sich Mitarbeiter wenden können, um ein Pseudonym zu erhalten, wenn sie selbst Patienten des Krankenhauses sind. Dennoch müssen Aufklärungsbögen mit Unterschrift und Einwilligungen, Arztbriefe sowie Rezepte mit Klarnamen erstellt werden, da sie sonst nicht rechtsverbindlich sind. Unter Umständen sind die Klarnamen auch in klinischen Subsystemen (Radiologie) notwendig. Die Pseudonymisierung wird von den Mitarbeitern bislang jedoch nicht in Anspruch genommen.
Die Zugriffe der Administratoren werden protokolliert und von einer Innenrevision geprüft. Der TLfDI wies darauf hin, dass eine aussagefähige und revisionsfeste Protokollierung gefordert und Einsichtsrechte festgelegt werden müssen. Für die Löschung von Patientendaten gibt es bisher kein System, das alle Daten löschen kann. Die maximale Verjährungsfrist nach dem Bürgerlichen Gesetzbuch (BGB) beträgt 30 Jahre.
Ab dem 25. Mai 2018 gilt die Datenschutz-Grundverordnung (DS-GVO) unmittelbar auch für die Thüringer Krankenhäuser. Im Hinblick auf die Umsetzung der Datenschutz-Grundverordnung räumte der TLfDI der Landeskrankenhausgesellschaft Thüringern die Möglichkeit ein, ihm datenschutzrechtliche Änderungswünsche zum Thüringer Krankenhausgesetz (ThürKHG) zu melden, da ggf. eine Aufnahme in ein Änderungsgesetz möglich wäre.

Gesundheits- und Patientendaten sind gemäß Art. 9 Abs. 1 DS-GVO i. V. m. Art. 4 Nr. 15 DS-GVO besonders sensible bzw. sensitive personenbezogene Daten. Gemäß Art 4 Nr. 15 DS-GVO sind „Gesundheitsdaten personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen …“. Naturgemäß werden diese Daten von ärztlichem und medizinischem Personal, insbesondere in Krankenhäusern, in großem Umfang erhoben, verarbeitet und übermittelt. Somit besteht hier ein entsprechend großer Informations- und Schulungsbedarf zum Datenschutz.

12.39 Datenschutz wirkt über den Tod hinaus

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) hatte in seinem letzten Tätigkeitsbericht (11. TB, Punkt 11.54) über die Durchführung eines sogenannten Mortalitäts-Follow-Up durch das Robert-Koch-Institut berichtet. Es handelt sich hierbei um eine bundesweite Langzeitstudie zur Gesundheit Erwachsener in Deutschland. Unter anderem werden die Todesursachen von bereits verstorbenen Studienteilnehmerinnen und -teilnehmern festgestellt. Der Zugriff durch das Forschungsinstitut erfolgt auf einen Datenpool, der aus den Jahren 2008 bis 2011 stammt. Der TLfDI hatte die Frage zu klären, ob das Institut aus den bei den unteren Gesundheitsbehörden geführten Toten- und Sektionsscheinen Auskünfte über die darin festgehaltenen Todesursachen erhält.

Der TLfDI teilte dem Institut mit, dass nach § 15 Abs. 4 Nr. 4 Thüringer Bestattungsgesetz (ThürBestG) die für den Wohnort des Verstorbenen zuständige untere Gesundheitsbehörde auf Antrag dem Institut Auskünfte aus den Toten- und Sektionsscheinen erteilen darf, wenn dieses die Angaben für ein wissenschaftliches Forschungsvorhaben benötigt und das für das Gesundheitswesen zuständige Ministerium festgestellt hat, dass das öffentliche Interesse an dem Forschungsvorhaben das Geheimhaltungsinteresse des Verstorbenen und seiner Angehörigen erheblich überwiegt und der Zweck der Forschung nicht auf andere Weise oder mit unverhältnismäßigem Aufwand erreicht werden kann.

Der TLfDI wurde nachrichtlich vom Thüringer Landesverwaltungsamt unterrichtet, dass man dort nach Prüfung des beschriebenen Sachverhalts ein erhebliches öffentliches Interesse an der wissenschaftlichen Folgestudie des Robert-Koch-Instituts sieht und daher die Genehmigung des Antrags auf Einsichtnahme in die Totenbescheinigungen nach § 15 Abs. 4 Nr. 2b ThürBestG befürwortet. Im Ergebnis hatte das Thüringer Ministerium für Arbeit, Soziales, Gesundheit, Frauen und Familie (TMASGFF) dem TLfDI einen Abdruck des Schreibens an das Robert-Koch-Institut übersandt, in dem das Ministerium feststellt, dass unter Berücksichtigung der Stellungnahme des TLfDI aus fachlicher Sicht ein erhebliches öffentliches Forschungsinteresse an der vorgesehenen Erhebung der Todesursachen besteht, der Forschungszweck das Geheimhaltungsinteresse der

Verstorbenen und deren Angehörigen erheblich überwiegt und der Zweck der Langzeitstudie nicht auf andere Weise oder nur mit unverhältnismäßigem Aufwand erreicht werden kann. Das TMASGFF hatte somit keine Bedenken gegen das Forschungsvorhaben. Aus Sicht des TLfDI konnte der Vorgang damit abgeschlossen werden.

Forschungsinstitute dürfen dann Auskünfte aus Toten- und Sektionsscheinen erhalten, wenn diese darlegen, dass sie die Angaben zur Durchführung eines wissenschaftlichen Forschungsvorhabens benötigen und das zuständige Ministerium ein öffentliches Interesse an diesem Forschungsvorhaben feststellt, welches das Geheimhaltungsinteresse des Verstorbenen und seiner Angehörigen erheblich überwiegt und der Zweck der Forschung nicht auf andere Weise oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

12.40 Wissenschaftliche Forschung und Sozialdaten

Das Thüringer Ministerium für Arbeit, Soziales, Gesundheit, Frauen und Familie (TMASGFF) wandte sich hilfesuchend an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Es teilte mit, dass das Bundesministerium für Arbeit und Soziales (BMAS) mit Beginn des Jahres 2011 ein Bund-Länder-Programm „Initiative Inklusion“ ins Leben gerufen habe, welches teilweise auch durch den Freistaat Thüringen mitfinanziert werde. Das Programm sei mit Ende des Jahres 2015 ausgelaufen. Nunmehr möchte das BMAS die Wirksamkeit und Nachhaltigkeit der Förderung in den Handlungsfeldern „Ausbildung“ und „Beschäftigung“ durch ein externes Institut untersuchen lassen. Im Handlungsfeld Ausbildung wurde der Einstieg schwerbehinderter junger Menschen in eine betriebliche Berufsausbildung durch die Schaffung neuer Ausbildungsplätze unterstützt. Demgegenüber standen in dem Handlungsfeld Beschäftigung schwerbehinderte Menschen, die das fünfzigste Lebensjahr vollendet hatten, im Blickpunkt. Sie sollten vermehrt in den allgemeinen Arbeitsmarkt integriert werden. Das mit der Evaluierung zu beauftragende Institut habe einen Antrag auf Übermittlung von Sozialdaten für ein Forschungsvorhaben nach § 75 Sozialgesetzbuch (SGB) Zehntes (X) Buch beim TMASGFF gestellt. Das TMASGFF beabsichtigte, dem Antrag stattzugeben, da nach seiner Auffassung ein hohes Forschungsinteresse an den Daten besteht, und bat den TLfDI um Beratung. Eine Anonymisierung der

Angaben zu den geförderten Personen sei nicht möglich, weil für die Bewertung der Wirksamkeit der Förderung und ihrer Nachhaltigkeit die Daten personenbezogen ausgewertet werden müssen.
Wenn ein privates Institut mit der Auswertung von Sozialdaten beauftragt wird, handelt es sich um einen Dritten. Eine Auftragsdatenverarbeitung war hier nicht vorgesehen, weil das Institut die Daten selbstständig auswerten sollte. Für derartige Vorhaben gibt es eine gesetzliche Ermächtigungsgrundlage:
Nach § 75 SGB X können Sozialdaten an Dritte übermittelt werden, soweit dies erforderlich ist für ein bestimmtes Vorhaben der wissenschaftlichen Forschung im Sozialbereich und schutzwürdige Interessen des Betroffenen nicht beeinträchtigt werden oder das öffentliche Interesse an der Forschung oder Planung das Geheimhaltungsinteresse der Betroffenen erheblich überwiegt. Die Übermittlung bedarf nach § 75 Abs. 2 Satz 1 SGB X der vorherigen Genehmigung durch die Landesbehörde, die für den Bereich, aus dem die Daten herrühren, zuständig ist. Die Genehmigung kann nur erteilt werden, wenn die gesetzlichen Voraussetzungen vorliegen. Wie hoch das Forschungsinteresse im Einzelfall zu bewerten ist, muss durch das TMASGFF fachlich beurteilt werden. Das Verfahren war nach den Angaben des TMASGFF so ausgestaltet, dass zunächst die Identifikationsdaten der Betroffenen an eine dritte Stelle fließen, dort werden die Daten pseudonymisiert, um dann an das Auswertungsinstitut weitergeleitet zu werden. Mit der Pseudonymisierungsstelle ist ein Auftragsdatenverarbeitungsvertrag nach § 70 Abs. 2 SGB X zu schließen. Für alle Daten wurde angegeben, dass diese zu einem bestimmten Stichtag gelöscht werden.
Nach § 75 Abs. 3 SGB X muss die genehmigende Stelle, da Daten an nicht-öffentliche Stellen geschickt werden sollen, durch Auflagen sicherstellen, dass die der Genehmigung durch die gesetzliche Regelung gesetzten Grenzen beachtet und die Daten nur für den Übermittlungszweck gespeichert, verändert oder genutzt werden. Der TLfDI regte an, dass die Daten, die pseudonymisiert worden sind, bei der Pseudonymisierungsstelle früher gelöscht werden. Ansonsten bestanden gegen das Verfahren, das öffentliches Interesse an der Forschung vorausgesetzt, keine Bedenken.

Sozialdaten dürfen pseudonymisiert zu Forschungszwecken übermittelt werden, wenn schutzwürdige Interessen der Betroffenen nicht beeinträchtigt werden oder das öffentliche Interesse an der For-

schung das Geheimhaltungsinteresse des Betroffenen erheblich überwiegt. In jedem Fall muss die Übermittlung genehmigt werden und die genehmigende Stelle muss durch Auflagen sicherstellen, dass schutzwürdige Interessen der Betroffenen gewahrt werden.

12.41 ESF-Programm „JUGEND STÄRKEN im Quartier“

Gegen Ende des Jahres 2015 wurde der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) von der Stadtverwaltung Erfurt gebeten, zu einer beabsichtigten Auftragsdatenverarbeitung im Rahmen der Wahrnehmung eines Programms des Europäischen Sozialfonds (ESF) zu beraten. Das ESF-Programm JUGEND STÄRKEN im Quartier soll junge Menschen im Alter von 12 bis 26 Jahren beim Übergang von der Schule in den Beruf unterstützen mit dem Ziel, auf dem Weg in Richtung Ausbildung und Arbeit individuelle Hürden zu überwinden und eine schulische, berufliche und soziale Integration zu ermöglichen. Das Jugendamt ist dabei für die Koordinierung der einzelnen Projektbausteine verantwortlich. Projektbeginn war am 1. Januar 2015, in Erfurt wurde am 1. April begonnen. Projektende wird am 31. Dezember 2018 sein.
Jeder junge Mensch, der in das Projekt aufgenommen wird, unterschreibt eine Einwilligungserklärung, mit der er sich damit einverstanden erklärt, dass bestimmte Daten über ihn erhoben und ggf. an das Bundesamt für Familie und zivilgesellschaftliche Aufgaben (BAFzA), verschiedene Bundesministerien und mit der Evaluation bzw. Bewertung beauftragte Institute weitergeleitet werden. Der Träger des Projekts legt dann eine elektronische Fallakte an. Dies erfolgt im Wege der Auftragsdatenverarbeitung zwischen der Kommune und dem BAFzA. Das BAFzA stellt als programmumsetzende Stelle des ESF-Modellprogramms den teilnehmenden Kommunen verschiedene EDV-Verfahren einschließlich technischer Infrastruktur zur Verfügung, mit deren Hilfe elektronische Fallakten geführt werden können.
Aus der dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) übermittelten Vereinbarung zur Auftragsdatenverarbeitung ergaben sich keine grundsätzlichen datenschutzrechtlichen Probleme. Die Vereinbarung sieht eine Unterwerfung unter die Kontrolle der zuständigen Aufsichtsstelle für den Datenschutz für die Auftragnehmer vor. Dabei wird darauf hinge-

wiesen, dass für den Auftraggeber hier das Landesrecht anzuwenden ist.
Allerdings stellte sich die Frage, weshalb und auf welcher Rechtsgrundlage die Übermittlung der Daten der elektronischen Fallakten für „JUGEND STÄRKEN im Quartier“ an das Bundesamt für Familie und zivilgesellschaftliche Aufgaben, das Auftragnehmer ist, drei Bundesministerien, das Bundesinstitut für Bau, Stadt und Raumforschung sowie an ein weiteres Institut, das mit der Evaluierung des Programms des Bundes beauftragt wird, vorgesehen ist. Es sollte in der Einwilligung differenziert werden, auf welcher Rechtsgrundlage die Weiterleitung der Daten stattfindet. Diese Angabe einer entsprechenden Rechtsgrundlage fehlte in der Einwilligungserklärung für die Jugendlichen. Deren Information scheint aus Sicht des TLfDI besonders wichtig, damit sie für die Entscheidung über die Abgabe der Einwilligung ausreichend informiert sind, um deren Tragweite erfassen zu können (informierte Einwilligung).
Weiterhin ist noch zu klären, ob und ggf. welche Daten zur Evaluierung und zum Nachweis der Verwendung der Förderprogramme an EU-Institutionen zu erheben sind. Lediglich aus den Angaben zu Speicherfristen ist zu entnehmen, dass Daten, die an die Europäische Kommission geliefert werden, mehrere Jahre im elektronischen Datenerfassungssystem gespeichert werden. Aus der Einwilligungserklärung der Jugendlichen ist dies wiederum nicht zu entnehmen. Insoweit bedarf es eines Merkblattes für die Betroffenen, das weiteren Aufschluss gibt.
Nachdem die Stadt die geforderten Änderungen vorgenommen hatte, konnte der Fall abgeschlossen werden.

Auch bei der Umsetzung von durch den Europäischen Sozialfonds geförderten Programmen müssen ergänzende rechtliche Prüfungen vorgenommen werden. Sollen Einwilligungserklärungen von Betroffenen für die Erhebung, Verarbeitung, Übermittlung und Nutzung eingeholt werden, müssen die Betroffenen ausreichend über die Gründe und den Zweck sowie nicht zuletzt über die Speicherdauer informiert sein.

12.42 Wann kommen und gehen die Mitarbeiter? – Doppelte Buchführung in der Stadtverwaltung

Ein Mitarbeiter einer Stadt in Thüringen wandte sich anonym mit folgenden Anliegen an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI): In der Stadtverwaltung seien mehrere Mitarbeiter im Außendienst tätig. Ein Arbeitskollege von ihnen mache Arbeitsaufzeichnungen über deren Tätigkeit, um sie zu überwachen. Dabei werde aufgeschrieben, wann den Mitarbeitern mobile Datenerfassungsgeräte (MDA-Geräte) ausgehändigt werden und wann diese zurückgegeben werden. Mit diesen Geräten werden Verwarnungen bei Verstößen im ruhenden Verkehr ausgestellt. Nachdem die Mitarbeiter den Amtsleiter kontaktiert hätten, teilte dieser mit, er wisse von der Überwachung, sie werde im Auftrag des Personalamts durchgeführt.
Der TLfDI schrieb die Stadtverwaltung an und teilte mit, dass nach seinem Kenntnisstand neben der automatisierten Zeiterfassung in bestimmten Bereichen Personen beauftragt seien, das Kommen und Gehen anderer Beschäftigter manuell festzuhalten und bat um entsprechende Stellungnahme. Die Stadtverwaltung übersandte die derzeit gültige Dienstvereinbarung zur gleitenden Arbeitszeit und legte dar, dass gesonderte Festlegungen zu weiteren manuellen oder auch anonymisierten Zeiterfassungen durch die Stadtverwaltung nicht getroffen worden seien. Insoweit sei davon auszugehen, dass allein das der Dienstvereinbarung zur gleitenden Arbeitszeit zugrundeliegende automatisierte Arbeitszeiterfassungssystem genutzt werde.
Dem hielt der TLfDI entgegen, dass ihm Ablichtungen eines Dienstkalenders zur Kenntnis gegeben worden seien, in dem das Kommen und Gehen bestimmter Personen notiert worden sei. Aus den Eintragungen im Dienstkalender sei ersichtlich, dass einzelne Mitarbeiter im Außendienst von einer besonderen Überwachung der Arbeitszeit betroffen sind. Unter Hinweis auf § 38 Thüringer Datenschutzgesetz (ThürDSG), nach dem der Landesbeauftragte für den Datenschutz und seine Beauftragten zu unterstützten sind und ihm im Rahmen der Kontrollbefugnis nach § 37 ThürDSG insbesondere Auskunft zu seinen Fragen sowie die Einsicht in alle Unterlagen und Akten, insbesondere in die gespeicherten Daten und die Datenverarbeitungsprogramme zu gewähren ist, wurde die Stadtverwaltung gebeten, ihre Stellungnahme nochmals zu überprüfen.

Der Inhalt des Schreibens des TLfDI habe, so die Stadtverwaltung in ihrer Antwort, verwundert. Man habe Kontakt zum Personalrat aufgenommen, um die Angelegenheit zu klären. Folgendes sei festgestellt worden: In der Stadtverwaltung sei eine Organisationskontrolle zu Controllingzwecken durchgeführt worden. In einer Dienstberatung seien alle beteiligten Akteure über das Verfahren informiert worden. Zweck der Maßnahme war in erster Linie die Optimierung der Einteilung der Vollzugsdienstkräfte in die entsprechenden Kontrollgebiete. Im Rahmen dieser Organisationskontrolle seien anhand der von bestimmten Mitarbeitern im Außendienst bei der Überprüfung des ruhenden Verkehrs ausgestellten Verwarnungen deren Arbeitszeiten überprüft worden. Diese Daten werden zum Nachweis der ausgestellten Verwarnungen verarbeitet und stellen Protokolldaten dar. Sie bieten natürlich andererseits auch die Möglichkeit einer konkreten Leistungs- und Verhaltenskontrolle eines bestimmten Mitarbeiters. Dies ist nach § 33 Abs. 4 ThürDSG unzulässig.
Die Nutzung dieser Protokolldaten für eine Leistungs- und Verhaltenskontrolle stellt eine unzulässige Zweckänderung dar. Nach § 20 Abs. 3 Thüringer Datenschutzgesetz ist eine Verarbeitung oder Nutzung von Daten für andere Zwecke nicht gegeben, wenn sie u. a. der Durchführung von Organisationsuntersuchungen sowie der Prüfung und Wartung von automatisierten Verfahren der Datenverarbeitung oder zur Erstellung von Geschäftsstatistiken für die Daten verarbeitende Stelle dient. Bei der Durchführung einer Organisationskontrolle ist jedoch mit Blick auf § 33 Abs. 4 ThürDSG vorab zu prüfen, welche konkreten personenbezogenen Daten hierzu unabdingbar benötigt werden und ob entgegenstehende Interessen des Betroffenen zu berücksichtigen sind. Bei der Durchführung einer Controllingmaßnahme sind grundsätzlich keine personenbezogenen Daten (hier die Namen der Bediensteten) erforderlich. Nach dem geschilderten Zweck – insbesondere der Optimierung der Einteilung der Vollzugsdienstkräfte in die entsprechenden Kontrollgebiete – kommt es grundsätzlich nicht darauf an, welcher Bedienstete die entsprechende Verwarnung ausgestellt hat. Der TLfDI bat daher, die Vorgehensweise nochmal dahingehend zu überprüfen, ob für die Organisationskontrolle Ausdrucke ohne den konkreten Namensbezug ausreichen. Darüber hinaus seien in einem solchen Fall schriftliche Festlegungen zur Vorgehensweise erforderlich.
Da sich die Stadtverwaltung innerhalb der gesetzten Frist nicht rührte, wurde sie unter Hinweis auf die Unterstützungspflicht nach § 38

Abs. 1 ThürDSG nachdrücklich um Stellungnahme gebeten. In der gesetzten Frist ging keine Stellungnahme ein, weswegen der TLfDI eine Beanstandung androhte. Die Stadtverwaltung teilte daraufhin mit, man habe nunmehr eine interne Überprüfung zur Auswertung der Protokolldaten der Erfassungsgeräte der Dienstkräfte durchgeführt. Im Ergebnis sei festzustellen, dass für das verwaltungsinterne Controlling nicht zwingend den Namen des jeweiligen Erfassers benötige. Daher habe man technisch beim Ausdruck der Daten den Personenbezug ausgeschlossen. Darüber hinaus wurden die Belehrung der Mitarbeiter und die Anweisung zur Einhaltung der datenschutzrechtlichen Vorschriften entsprechend geändert. Damit hielt es der TLfDI für ausgeschlossen, dass eine weitergehende Erfassung der An- und Abwesenheitszeiten erfolgt, als in der Arbeitszeitregelung vorgesehen und festgelegt. Das Verfahren konnte damit abgeschlossen werden.

Im Datenschutzrecht gilt der Grundsatz der Zweckbindung, § 20 Abs. 1 ThürDSG, nach dem Daten grundsätzlich nur für den Zweck genutzt werden dürfen, für den sie erhoben wurden. Keinesfalls dürfen bestimmte Daten, die in einem anderen Zusammenhang erhoben wurden, dafür genutzt werden, eine Verhaltens- und Leistungskontrolle der Mitarbeiter durchzuführen, § 33 Abs. 4 ThürDSG. Eine Verarbeitung von Daten für andere Zwecke liegt nicht vor, wenn sie zur Durchführung von Organisationsuntersuchungen erforderlich ist, § 20 Abs. 3 ThürDSG. Allerdings ist in diesem Fall in aller Regel die Nutzung von personenbezogenen Mitarbeiterdaten nicht notwendig.

12.43 Kindergeld – was muss die Familienkasse wissen?

Auch wenn die Kinder flügge werden, haben die Eltern über das 18. Lebensjahr ihrer Kinder hinaus ihren Anspruch auf Zahlung von Kindergeld, wenn die Kinder sich in einer Ausbildung befinden. Dies allerdings nur, wenn gegenüber der zuständigen Familienkasse nachgewiesen wird, dass das Kind eine Ausbildung absolviert. Ein Familienvater wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und beschwerte sich darüber, dass nicht nur das Abschlusszeugnis seines volljährigen Kindes von der Kindergeldstelle gefordert worden sei, sondern auch das Abschlusszeugnis seines zweiten Kindes, das erst 17 Jahre alt war. Diese Bitte konnte er nicht nachvollziehen. Nach-

dem der Beschwerdeführer zugestimmt hatte, dass gegenüber der Familienkasse sein Name genannt wurde, da ansonsten seine Beschwerde nicht bearbeitet werden konnte, wurde diese um Stellungnahme gebeten. Dabei wurde darauf hingewiesen, dass das Abschlusszeugnis neben dem Namen und dem Geburtsdatum des Kindes sowie dem Schuljahr auch die Leistungsbenotungen in einer Vielzahl von Fächern sowie unter Umständen auch Bemerkungen zu persönlichen Entwicklungen enthält. Die Prüfung dieser Daten des jüngeren Kindes erschien dem TLfDI für die Aufgabenerfüllung der Kindergeldkasse, nämlich der Prüfung, ob die Voraussetzungen für die weitere Zahlung von Kindergeld vorliegen, nicht erforderlich.
Die Thüringer Landesfinanzdirektion als zuständige Familienkasse teilte darauf mit, dass nicht die Vorlage des Zeugnisses des minderjährigen Kindes gefordert worden sei, sondern die Vorlage des Abschlusszeugnisses zur Berufsausbildung des älteren Sohnes. Dabei sei in der Aufforderung „Bitte senden Sie eine Kopie des Abschlusszeugnisses bis zum … an die Landesfamilienkasse“ nicht eindeutig formuliert worden, da die Festsetzung von Kindergeld sowohl das minderjährige als auch das volljährige Kind betraf. Der Kindergeldberechtigte habe daraufhin das Abschlusszeugnis des minderjährigen Kindes vorgelegt. Die Landesfamilienkasse habe ihn bereits über das Missverständnis aufgeklärt und das Abschlusszeugnis des minderjährigen Kindes umgehend zurückgesandt. Die Familienkasse legte die rechtlichen Grundlagen dafür dar, dass Zeugnisse von volljährigen Kindern angefordert werden können. Bei ihnen ist jeweils der Zeitraum seit der vorangegangenen letzten Festsetzung zu prüfen, da gemäß § 32 Abs. 4 Satz 1 Nr. 2 des Einkommensteuergesetzes besondere Anspruchsvoraussetzungen gelten. Diese sind bei Beginn und Ende der Ausbildung zu prüfen. Der Beschwerdeführer sollte daher eine Erklärung zu den Verhältnissen seines volljährigen Kindes abgeben, um die Anspruchsvoraussetzungen in Bezug auf dieses Kind nachzuweisen. Erforderlich war hier der Nachweis über den Zeitpunkt der Beendigung der Berufsausbildung bzw. den Zeitpunkt der Bekanntgabe des Prüfungsergebnisses. Die Landesfinanzdirektion wies dabei den Beschwerdeführer darauf hin, dass in dem Zeugnis bestimmte Angaben geschwärzt werden können, da für die Prüfung lediglich der Beweis notwendig ist, dass die Berufsausbildung durch die bestandene Prüfung absolviert und abgeschlossen wurde sowie der Zeitpunkt der Bekanntgabe des Prüfungsergebnisses.

Die Thüringer Landesfinanzdirektion wurde darauf hingewiesen, dass öffentliche Stellen nach den allgemeinen Vorschriften nur die Daten erheben dürfen, die für die Aufgabenerfüllung erforderlich sind, § 19 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG). Die erhobenen Daten dürfen nach § 20 Abs. 1 ThürDSG nur gespeichert werden, wenn dies zur Erfüllung der in der Zuständigkeit der Daten verarbeitenden Stelle liegenden Aufgaben erforderlich ist. Bei der Anforderung von Zeugniskopien werden durch die Landesfinanzdirektion Daten erhoben, die für die Erfüllung ihrer Aufgaben nicht erforderlich sind. Nachgewiesen werden müssen nur der Zeitpunkt und die Tatsache, dass eine Berufsausbildung abgeschlossen worden ist. Grundsätzlich kann bei der Einreichung von ungeschwärzten Zeugnissen nicht ohne Weiteres davon ausgegangen werden, dass die Betroffenen, also die Kindergeldberechtigten und die „Kinder“ konkludent in die weitere Verarbeitung der nicht erforderlichen Angaben einwilligen. Um den Aufwand für die Mitarbeiter der Landesfamilienkasse gering zu halten, sollte daher bei der Anforderung der Unterlagen konkret darauf hingewiesen werden, welche Angaben erforderlich sind. Die Betroffenen sollten auf die Möglichkeit der Schwärzung oder anderweitige Unkenntlichmachung der nicht erforderlichen Angaben in jedem Fall hingewiesen werden. Sollten ungeschwärzte Kopien bzw. Kopien mit nicht erforderlichen Angaben eingereicht werden, müssen diese von der Landesfamilienkasse unkenntlich gemacht werden. Die Landesfinanzdirektion wurde gebeten, dies künftig zu berücksichtigen. Hierüber wurde der Beschwerdeführer informiert.

Öffentliche Stellen dürfen nach den allgemeinen Vorschriften nur die Daten erheben, die für die Aufgabenerfüllung erforderlich sind, § 19 Abs. 1 ThürDSG. Die erhobenen Daten dürfen nach § 20 Abs. 1 ThürDSG nur gespeichert werden, wenn dies zur Erfüllung der in der Zuständigkeit der Daten verarbeitenden Stelle liegenden Aufgaben erforderlich ist. Danach dürfen beim Nachweis gegenüber der Kindergeldstelle in Zeugnissen enthaltene Angaben, die über den Zeitpunkt des zu bestätigenden Abschlusses hinausgehen, nicht verarbeitet werden. Diese Daten sind zu löschen bzw. zu schwärzen.

12.44 Feuchte Akten brennen schlecht

Wenn nicht einige Jugendliche in ein Gebäude der Stadt Gera eingebrochen wären und nicht versucht hätten, die dort gelagerten Akten in Brand zu setzen, so hätte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit
(TLfDI) vielleicht nie davon erfahren, dass dort seit vielen Jahren geschätzt mindestens 150.000 Patientenakten aufbewahrt werden. Der TLfDI hatte sich unmittelbar nach Kenntnisnahme des Vorfalls bei der Oberbürgermeisterin mit einer Vor-Ort-Besichtigung des Gebäudes angekündigt. Wie der TLfDI feststellte, nutzt das Gesundheitsamt der Stadt mehrere Räume eines ehemaligen Internatsgebäudes zur Zwischenarchivierung von Akten. Die jugendlichen Einbrecher hatten sich nach bisheriger Erkenntnis durch das Einschlagen eines Fensters zunächst Zutritt ins Gebäude verschafft und bei der „Gebäudebesichtigung“ eine weitere Glastür eingeschlagen, mit der der Lagerraum der Akten gesichert war. Im weiteren Verlauf sollen die Täter in einem Raum einige Aktenstapel angezündet haben, die aber möglicherweise aufgrund der Papierfeuchte nur geschwelt, aber nicht richtig gebrannt haben. Die Aktenbündel sind nach menschlichem Ermessen zwar nicht mehr nutzbar, vereinzelt sind aber noch darin enthaltene Dokumente lesbar.
Der TLfDI musste feststellen, dass diese Tür am Tag der Vor-Ort-Besichtigung noch immer offenstand. Die Eingangstüren der Zimmer standen ebenfalls offen. In jedem der 12 Zimmer werden Patientenunterlagen teils in Umzugskartons, in verschnürten Aktenbündeln oder in Karteikästen verschiedenster Ausführungen aus den Bereichen ehemaliger Polikliniken, Betriebsambulatorien, „Arbeitsmedizin“, örtliches Gesundheitsamt sowie niedergelassener Ärzte, die ihre Praxis aufgegeben hatten, gelagert. In Teilbereichen der Zimmer, etwa in ehemaligen Nasszellen, sind Röntgenunterlagen aufgeschichtet. Verschiedene Stichproben von Akten zeigten, dass die Unterlagen zu Zeiten der ehemaligen DDR entstanden sind, in einigen Fällen aber Unterlagen bis zum Jahre 1997 enthalten sind. Nach Angaben der Stadt wurden alle hier gelagerten Unterlagen in Form von Mikrofiches erfasst. Eine Möglichkeit festzustellen, ob die gelagerten Unterlagen vollständig sind, besteht nicht. Aus datenschutzrechtlicher Sicht war festzustellen, dass die Unterlagen bei deren Übernahme in das Archiv nicht daraufhin geprüft wurden, ob diese bereits gelöscht werden konnten. Man hatte deshalb eine einheitliche

Aufbewahrungsfrist von 30 Jahren festgesetzt, die im Jahr 2021 endet. Dieses Verfahren sei der Tatsache geschuldet, dass man seitens der Stadt nicht imstande gewesen sei, für übernommene Unterlagen eine Differenzierung der Aufbewahrungsfristen vorzunehmen. Die Frage des TLfDI, wieso die schriftlichen Unterlagen überhaupt noch nach der Mikroverfilmung aufbewahrt werden, begründete die Stadt mit der Forderung der Gerichte, die danach bis vor 5 Jahren nur die Originalunterlagen, nicht aber Mikrofiche in Verfahren als Beweiswert akzeptiert haben sollen. In diesen Fällen seien die Originalunterlagen aus dem Archiv entnommen worden.
Zum Zeitpunkt der Vor-Ort-Besichtigung gab es nach Einschätzung des TLfDI an und in dem Gebäude mehrere Schwachstellen, die die Vertraulichkeit und Integrität der darin gelagerten Gesundheitsakten nicht ausreichend sicherstellen konnten. Die ohne großen Aufwand erreichbaren Fenster waren weder vergittert noch sonst besonders gesichert. Ein unbefugtes Eindringen war letztendlich durch die vorhandenen Sicherheitsmaßnahmen nicht zu verhindern. Auch die o. g. Glaseingangstür zum eigentlichen Archivbereich bot keinen ausreichenden Schutz gegen einen Einbruchsversuch. Nach Angaben der Ansprechpartner der Stadt sei zu berücksichtigen, dass das Ende der festgesetzten Aufbewahrungszeit im Jahre 2021 nicht allzu fern sei und eine Nachnutzung des Gebäudes derzeit nicht im Raum stehe. Insoweit habe man bauliche Veränderungen als unverhältnismäßig angesehen.
In einem Schreiben an die Stadt hat der TLfDI die unverzügliche Sicherung der Räume gefordert, in denen die Patientenakten gelagert sind. Hierzu wurde dringend empfohlen, eine Vergitterung der Fensterfront zu prüfen, in der ein Fenster eingeschlagen wurde. Ebenfalls wurde die Stadt aufgefordert, den unmittelbaren Zugangsbereich zu dem Archiv mit einer ausreichend sicheren Eingangstür zu sichern. Weiterhin informierte der TLfDI über die bestehenden gesetzlichen Speicherfristen. Hierzu gehört, dass ärztliche Patientendokumentationen gemäß § 10 (Muster-)Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte oder nach § 630f Bürgerliches Gesetzbuch im Allgemeinen 10 Jahre nach Ende des Behandlungsvorgangs aufzubewahren sind, es sei denn, es besteht nach den gesetzlichen Vorschriften eine längere Aufbewahrungspflicht. Solche längeren Aufbewahrungsfristen ergeben sich z. B. aus der Röntgenverordnung, dem Transfusionsgesetz oder auch aus Gerichtsverfahren, bei denen Schadensersatzansprüche geltend gemacht werden.

Die Stadt muss zunächst die eingelagerten Unterlagen darauf durchsehen, wann diese tatsächlich abgeschlossen wurden. Der TLfDI hat die Stadt aufgefordert, ihn rechtzeitig über den Zeitpunkt der Vernichtung und die beauftragte Firma zu informieren. In einer ersten Reaktion der Stadtverwaltung hat diese erklärt, Maßnahmen zur Sicherung des Gebäudes zu veranlassen, wobei eine Notsicherung der Eingangstür zum Aktenlager bereits erfolgt sei. Außerdem könne nach derzeitigem Kenntnisstand der komplette Aktenbestand der Vernichtung zugeführt werden, da die bis 1991 übernommenen Akten als Mikrofiche vorliegen. Bei den Unterlagen jüngeren Datums handle es sich um Reihenuntersuchungen des Kinder- und Notärztlichen Dienstes, die ebenfalls vernichtet werden können. Es werde eine Ausschreibung vorbereitet, um eine zertifizierte Firma mit der datenschutzgerechten Vernichtung der Akten zu beauftragen. Der TLfDI hat die Stadtverwaltung ergänzend aufgefordert, ihm mitzuteilen, auf welcher Rechtsgrundlage die Entscheidung über die Vernichtung der Akten getroffen wurde und welche Akten weiterhin aufzubewahren sind. Da es sich um als sensibel einzustufende Patientendaten handelt, wurde die Stadtverwaltung auch aufgefordert, dafür Sorge zu tragen, dass die Akten unter Anwendung der adäquaten Vernichtungsstufe geschreddert werden. Der TLfDI wird den Fortgang der Sache selbstverständlich im Auge behalten.

Bei der Einlagerung von Patientenakten hat die verantwortliche Stelle ebenso wie bei der laufenden Datenverarbeitung die erforderlichen technischen und organisatorischen Maßnahmen gemäß § 9 Thüringer Datenschutzgesetz zu treffen, die erforderlich sind, um die Ausführung der Bestimmungen dieses Gesetzes zu gewährleisten. Hierzu gehört im vorliegenden Fall die Gewährleistung eines angemessenen Einbruchschutzes, die Lagerung unter angemessenen klimatischen Bedingungen und die zeitgerechte Verfügbarkeit von personenbezogenen Daten. Unter Berücksichtigung einer Anbietung an das zuständige Archiv sind personenbezogene Daten zu löschen, wenn durch Gesetz oder Vertrag bestimmte Speicherfristen abgelaufen sind.



Landstraße, Windkraft, Umwelt © mahey / Fotolia.com

13. Infrastruktur und Landwirtschaft

13.1 Anfrage zur Bestellung von mehreren Personen für die Stelle eines Datenschutzbeauftragten

Ein Kommunaler Zweckverband bat den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) um Auskunft, ob es möglich sei, „… zwei Datenschutzbeauftragte nebeneinander mit unterschiedlicher Gewichtung (40% / 60%) zu berufen und wenn ja, ob es hierfür bereits eine Verankerung im Gesetz oder der Rechtsprechung/Urteil?“ geben würde.
Hierauf teile der TLfDI Folgendes mit:
Nach dem Wortlaut des § 10a Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) sind Daten verarbeitende Stellen verpflichtet, einen ihrer Beschäftigten zum Beauftragten für den Datenschutz schriftlich zu bestellen. Daraus ergibt sich, dass die Bestellung von mehreren Personen einen Verstoß gegen datenschutzrechtliche Vorschriften darstellen würde. Der Vorteil der gesetzlichen Regelung besteht u. a. darin, dass ein eindeutiger Ansprechpartner in Sachen Datenschutz vor Ort vorhanden ist.

Weiterhin wies der TLfDI auf die Möglichkeit hin, für mehrere Daten verarbeitende Stellen einen gemeinsamen Datenschutzbeauftragten gemäß § 10a Abs. 6 ThürDSG zu bestellen.

Da die gesetzliche Regelung zum (internen) Datenschutzbeauftragten im ThürDSG klar und verständlich formuliert ist, zeigt die Anfrage, wieviel Informationsbedarf in Sachen Datenschutz noch immer besteht.

13.2 Einsatz funkbasierter „intelligenter“ Wasserzähler

Auch vor der Wasserversorgung macht die Digitalisierung keinen Halt. Elektronische Wasserzähler mit Funkmodul ermöglichen den Wasserversorgern im Vergleich zum Ablesen herkömmlicher Zähler vor Ort Kosten einzusparen und die Administration zu vereinfachen. Auf dem Markt sind verschiedene Modelle dieser „intelligenten“ Wasserzähler. Sie speichern zumindest den Wasserdurchfluss und -verbrauch mehrfach pro Minute, alle 24 Stunden den Zählerstand für mehrere Hundert Tage im „Tagesregister“ und einmal monatlich zu einem Stichtag den Monatsverbrauch für mehrere Jahre in einem „Monatsregister“, aber auch Informationen zum Höchst- und Mindestdurchfluss, sodass bei atypischen Abweichungen des Wasserdurchflusses eine Fehlermeldung (z. B. „Verdacht auf Rohrbruch“) generiert wird. Die o. g. Daten sind vor Ort am Wasserzähler über ein Lesegerät auslesbar. Zudem werden innerhalb eines festgelegten Zeitraums (z. B. mehrfach pro Minute) Signale zum aktuellen Zählerstand, dem Monatszählerstand und mögliche Fehlermeldungen gesendet, die der Wasserversorger zum Zwecke der Jahresabrechnung oder bei Verdachtsfällen zur Lokalisierung von Wasserlecks aus der Ferne ausliest. Dies geschieht regelmäßig ohne Mitwirkung und Kenntnis der Verbraucher.

Eine Umwelt- und Verbraucherorganisation bat den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) im Dezember 2016 um eine Beurteilung der datenschutzrechtlichen Zulässigkeit von funkbasierten Wasserzählern. Der TLfDI setzte die Verbraucherschützer darüber in Kenntnis, dass er in Übereinstimmung mit dem Bayerischen Landesbeauftragten für den Datenschutz die Auffassung vertritt, dass der Betrieb von funkbasierten Wasserzählern, die eine unzulässige Erhebung und Verarbeitung personenbezogener Daten ermöglichen, einen Verstoß gegen daten-

schutzrechtliche Vorschriften darstellt. Daher seien solche Wasserzähler stillzulegen bzw. abzubauen (vgl. Gliederungspunkt 6.3 des 27. Tätigkeitsberichts des Bayerischen Landesbeauftragten für den Datenschutz). Weiter teilte der TLfDI mit, dass ihm bislang keine Bestrebungen zur Schaffung einer formell-gesetzlichen Rechtsgrundlage für den Einsatz von „intelligenten“ Wasserzählern bekannt geworden sei.

Der Einsatz „intelligenter“ Wasserzähler greift in das informationelle Selbstbestimmungsrecht (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 Grundgesetz) ein, da die im Wasserzähler gespeicherten und von dort gesendeten Verbrauchsdaten einen Personenbezug aufweisen und die Bildung eines Verbrauchsprofils ermöglichen. Für die Beurteilung der Zulässigkeit des Einsatzes von „intelligenten“ Wasserzählern stellt sich zunächst die Frage, ob es hierfür eines Gesetzes bedarf oder ob Satzungsregelungen genügen.

Die ständige Rechtsprechung des Bundesverfassungsgerichts verpflichtet den Gesetzgeber, die für Grundrechtseingriffe wesentlichen Regelungen durch Gesetz zu treffen, wobei das entsprechende Gesetz die wichtigsten inhaltlichen Aspekte regeln muss. Im Falle von „intelligenten“ Wasserzählern ist zu klären, wie intensiv der mit dem Einsatz der „intelligenten“ Wasserzähler verbundene Eingriff in das Grundrecht auf informationelle Selbstbestimmung ausfällt. Die Intensität des Eingriffs hängt insbesondere von der konkreten Funktionalität des jeweiligen Zählers ab.

Im Zuge weiterer Recherchen stellte der TLfDI fest, dass sich der Bayerische Landesbeauftragte für den Datenschutz, die zuständigen Bayerischen Staatsministerien und der Bayerische Gemeindetag zu dieser Thematik auf gemeinsame Eckpunkte verständigt haben, die den Gemeinden durch ein Rundschreiben des Bayerischen Innenministeriums vom 29. März 2017 bekannt gegeben wurden. Zweck dieses Rundschreibens war es, die bestehenden Unsicherheiten zum Einsatz und Betrieb von „intelligenten“ Wasserzählern zu beseitigen. Um den Einbau und Betrieb von elektronischen Wasserzählern zu ermöglichen, hat das Bayerische Innenministerium in Abstimmung mit dem Bayerischen Landesbeauftragten für den Datenschutz eine Neufassung der dortigen Wasserabgabensatzung mit datenschutzkonformen Regelung für „intelligente“ Wasserzähler vorgeschlagen.

Es ist die Aufgabe des Gesetzgebers zu entscheiden, ob eine Rechtsgrundlage für einen verpflichtenden Einbau und Betrieb von „intelli-

genten“ Wasserzählern geschaffen werden soll. Solange ein solches Gesetz noch nicht vorliegt, wird der TLfDI darauf hinwirken, dass keine Wasserzähler eingebaut werden, für die eine formell-gesetzliche Rechtsgrundlage erforderlich ist. Ebenso sind gesetzeswidrige Wasserzähler zu deaktivieren bzw. abzubauen.

13.3 Verkehrsbeobachtung: immer diese Radfahrer – und ihre Daten

Im April 2016 wandte sich eine Studentin der Fachhochschule (FH) Erfurt an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und informierte über eine in Erfurt und Weimar geplante Verkehrsbeobachtung mittels Videotechnik. Die Beobachtung sollte im Rahmen des Projektes „Mit dem Rad zum Einkauf in die Innenstadt – Konflikte und Potenziale bei der Öffnung von Fußgängerzonen für den Radverkehr“ erfolgen. Das Projekt wurde vom Bundesministerium für Verkehr und Infrastruktur gefördert und von der FH Erfurt bearbeitet.
Die Beobachtung sollte in den innerstädtischen Fußgängerzonen an zwei Tagen und an jeweils drei verschiedenen Standorten durchgeführt werden, in erster Linie zur Konfliktbeobachtung und -analyse zwischen Radfahrern und Fußgängern. Weiterhin sollten auch Geschwindigkeiten über die Videobeobachtung erfasst werden. Die Kameras sollten in ca. 5 Meter Höhe installiert und auf die größtmögliche Unschärfe eingestellt werden, um eine Personenidentifikation auszuschließen. Die Daten sollten nicht personenbezogen ausgewertet und das Videomaterial nicht veröffentlicht werden. Stattfinden sollte die Videobeobachtung in Erfurt am 6. und 7. Mai 2016, in Weimar am 3. und 4. Juni 2016 jeweils zwischen ca. 8:00 Uhr und 20:00 Uhr.
Für das Vorhaben bat die FH Erfurt den TLfDI um datenschutzrechtliche Hinweise und Einwände sowie um Information, ob das Vorhaben nach § 25a Thüringer Datenschutzgesetz (ThürDSG) oder § 6b Bundesdatenschutzgesetz (BDSG) zu behandeln sei.
Der TLfDI teilte der FH Erfurt mit, dass die Fachhochschule als staatliche Einrichtung des Freistaats Thüringen gemäß § 3 Abs. 5 Thüringer Datenschutzgesetz (ThürDSG) eine Daten verarbeitende Stelle ist und das Vorhaben somit grundsätzlich nach dem ThürDSG beurteilt werden muss.

Die Verarbeitung und Nutzung personenbezogener Daten ist nach § 4 Abs. 1 ThürDSG nur zulässig, wenn dieses Gesetz oder eine andere Rechtsvorschrift dies erlauben, anordnen oder wenn der Betroffene selbst eingewilligt hat. Der dargelegte Forschungszweck und die tatsächliche Ausgestaltung des Projekts schließen das Einholen einer Einwilligung der Betroffenen von vornherein aus. Gemäß § 25a ThürDSG ist eine Videoüberwachung (Videobeobachtung oder -aufzeichnung) mithilfe optisch-elektronischer Einrichtungen nur zulässig, wenn sie zur Wahrung des Hausrechts der verantwortlichen öffentlichen Stelle erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Diese Norm greift im vorliegenden Fall also nicht.
Gemäß § 25 Abs. 1 ThürDSG dürfen jedoch für Zwecke der wissenschaftlichen Forschung erhobene oder gespeicherte Daten nur für Zwecke der wissenschaftlichen Forschung verarbeitet oder genutzt werden. Gleichwohl ist hierdurch eine Erhebung und Speicherung personenbezogener Daten im Wege einer Videoüberwachung aber nicht geregelt. Die Videoüberwachung ist ein intensiver Eingriff in das Persönlichkeitsrecht von Betroffenen und bedarf nach § 4 Abs. 1 ThürDSG einer speziellen Erlaubnisvorschrift oder der Einwilligung der Betroffenen. Da eine vorherige Einwilligung aus tatsächlichen Gründen nicht möglich ist und eine gesetzliche Erhebungsgrundlage fehlt, war die Videoüberwachung in der geplanten Form unzulässig.
Aus datenschutzrechtlicher Sicht ist die Durchführung der dargelegten Beobachtung nur dann zulässig, wenn die Auflösung der eingesetzten Videokameras keinen Personenbezug im Sinne von § 3 Abs. 1 ThürDSG zulässt, d. h. keine Personen bestimmbar sind. Weiterhin ist zu beachten, dass betroffene Passanten die Videokameras erkennen und hierdurch ggf. verunsichert werden, da sie nicht wissen, in welcher Auflösungsqualität die Kameras Bilder erfassen und aufzeichnen. Bei einem fehlenden Personenbezug fallen die Videokameras zwar nicht unter die Regelungen des ThürDSG, trotzdem kann auch das Anbringen dieser Kameras mit geringer Auflösung als unzulässiger Eingriff in das Persönlichkeitsrecht der Betroffenen angesehen werden. Die Betroffenen dürfen nicht darüber im Unklaren gelassen werden, „wer was wann und bei welcher Gelegenheit über sie weiß“ (BVerGE 65, 1 (42), [„Volkszählungsurteil“]). Daher muss in den Videobereichen auf den Zweck der Kameras aufmerksam gemacht und die verantwortliche Stelle angegeben werden.

Um zu entscheiden, ob ein Personenbezug bei der Beobachtung und der Auswertung der Videoaufzeichnung weitgehend ausgeschlossen werden kann, bat der TLfDI die FH darum, die erforderliche Bildauflösung der Kameras als Ausdruck vorzulegen. Weiterhin wurde die FH gebeten, mitzuteilen, wie die Betroffenen auf die Videobeobachtung aufmerksam gemacht werden. Darüber hinaus sollte die Verfahrensdurchführung schriftlich festgelegt und dem TLfDI mitgeteilt werden (Zweck der Maßnahme, welche Kameratypen, Auflösung, Standorte, Dauer der Maßnahme, Beteiligung des behördlichen Datenschutzbeauftragten der Fachhochschule Erfurt, Gestaltung der Hinweise an die Betroffenen usw.).
Nach datenschutzrechtlicher Prüfung der Unterlagen wies der TLfDI darauf hin, dass die „Information der Bevölkerung“ in lesbarer Größe nahe der Videoüberwachung anzubringen ist und empfahl, bei den Videokameras eine noch geringere Bildauflösung einzustellen. Hierdurch wäre der Forschungszweck nicht gefährdet, Radfahrer und Fußgänger wären dennoch zu unterscheiden und auch die Bewegungen wären gut sichtbar.
Die FH setzte die Hinweise des TLfDI um, sodass bei der Bildauflösung keine Personenidentifikation möglich war und die Konturen unscharf waren. Daher informierte der TLfDI die FH im Mai 2016 darüber, dass gegen die Durchführung des wissenschaftlichen Forschungsprojekts keine Bedenken bestehen.

Im Rahmen einer Verkehrsbeobachtung ist eine Videoüberwachung zu nachgewiesenen Forschungszwecken zulässig, wenn

1) ein Hinweisschild zur Information der Bevölkerung in lesbarer Größe in der Nähe der Überwachungskamera angebracht ist und
2) die Bildauflösung der Kamera gering eingestellt ist, sodass keine Personenidentifikation möglich ist.

13.4 Bericht aus dem Arbeitskreis Verkehr: Anwohnerparken nach § 45 Abs. 1b Nr. 2a StVO

Im Rahmen des Arbeitskreises Verkehr der Datenschutzbeauftragten der Länder erfragte der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (HmbBfDI) im Januar 2017 bei seinen Länderkollegen, welche Regelungen im Bereich des Anwohnerparkens nach § 45 Abs. 1b Nr. 2a Straßenverkehrsordnung in den jewei-

ligen Bundesländern bestehen, wie diese praktisch umgesetzt werden und ob in diesem Zusammenhang auch sogenannte Besucherausweise ausgestellt werden. Sofern dies der Fall sei, wollte der HmBfDI außerdem wissen, unter welchen Voraussetzungen die Ausweise ausgestellt werden.
Nach Information des HmbBfDI war das Parken für Anwohner und Besucher in der Hansestadt bis 1991 folgendermaßen geregelt: Vom zuständigen Polizeirevier wurden auf Antrag Besucherparkscheine ausgegeben, auf denen das Kennzeichen des besuchenden Kfz zusammen mit dem Besuchstag und einer laufenden Nummer vermerkt war und die sichtbar hinter der Windschutzscheibe hinterlegt werden mussten. Anschließend erhielten die Antragsteller einige Blanko-Besucherscheine mit unterschiedlicher laufender Nummer übersandt und konnten diese bei Bedarf mit den ergänzenden Angaben ihren Gästen überlassen. Durch eine Änderung der Zuständigkeiten entstand jedoch der Verdacht auf missbräuchliche Nutzung dieser Regelung. Daher wurde wieder eine Beantragung vor Ort eingeführt unter Angabe des Besucherkennzeichens und des Besuchstages. Das Besucherkennzeichen wird direkt in die Ausweise eingetragen, aber von der ausstellenden Dienststelle nicht gespeichert.
Der HmbBfDI hegte Bedenken hinsichtlich der Eingriffstiefe und der Erhebung der maßgeblichen Daten über Dritte statt bei den Betroffenen. Die vollziehenden Behörden teilten diese Bedenken jedoch nicht, sondern erwogen eher, grundsätzlich keine Besucherausweise mehr ausstellen zu lassen da dies anderenorts oftmals auch nicht gängige Praxis sei.
Nach Auskunft des Bayerischen Landesbeauftragten für den Datenschutz (BayLDA) bestehen in Bayern in vielen Kommunen sogenannte Parkraumbewirtschaftungsmaßnahmen, die die Einrichtung von Zonen für Bewohnerparken betreffen. Jedoch gibt es aufgrund technisch-organisatorischer Schwierigkeiten keine Regelungen zur Ausstellung von Besucherparkausweisen, d. h., für Bewohner ohne Haupt- und/oder Nebenwohnsitz und Besucher in der jeweiligen Anwohnerparkzone wird aktuell keine Parklizenz ausgestellt. Jedoch können juristische Personen eine Ausnahmegenehmigung beantragen. Der gewerbliche Parkausweis ist nicht kennzeichenbezogen. Auch im gewerblichen Bereich gilt: Für Besucher, Kunden oder Mitarbeiter können keine Ausnahmegenehmigungen beantragt werden.

Daher sehen die Bayerischen Regelungen grundsätzlich vor, dass bei der Einrichtung von parklizenzpflichtigen Zonen abgestufte Parknutzungsregelungen (Besucherparken, Misch-/Bewohnerparken, Kurzzeit-/Mischparken, Mischparken mit Parkscheibe, Halte- und Parkverbot) innerhalb eines Lizenzgebietes vorzusehen sind. Nach Möglichkeit sind ausreichend Flächen für Besucherfahrzeuge (Mischparken, mit Parkscheibe für maximal vier Stunden, mit Lizenz frei, ab 18 Uhr bis 8 Uhr freies Parken) vorzuhalten. Insoweit erübrige sich die gesonderte Erteilung von Parkausweisen für Besucher.
Nach Auskunft der Bremer Landesbeauftragten für Datenschutz und Informationsfreiheit (LfDI Bremen) besteht auch in Bremen die Möglichkeit, dass Besucher Parkausweise erhalten. Diese kann man sowohl online als auch persönlich beim Amt für Straßenbau und Verkehr beantragen. Es gibt Wochen- und Tageskarten. Monatlich dürfen höchstens vier Wochenkarten oder 20 Tageskarten pro Anwohner erworben werden. Hierfür ist eine Gebühr zu entrichten; Personalausweis und Meldebescheinigung müssen vorgelegt werden. Eine Eintragung der Namen der Besucher, der Besuchszeiten oder ihrer Kfz-Kennzeichen erfolgt allerdings nicht.

In den Bundesländern bestehen unterschiedliche Regelungen zur Ausstellung von Besucherparkausweisen in Parkzonen für Anwohner; in einigen Ländern werden entsprechende Ausweise auf Antrag ausgestellt, in anderen nicht.

13.5 Elektronisches Wohngeldverfahren – Verbundverfahren oder nicht?

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) wurde vom Thüringer Ministerium für Infrastruktur und Landwirtschaft (TMIL) über die Einführung eines Wohngeldfachverfahrens informiert und um eine datenschutzrechtliche Bewertung des Verfahrens gebeten. In diesem Zusammenhang ist darauf hinzuweisen, dass Wohngeldangelegenheiten von den Landkreisen und kreisfreien Städten im übertragenen Wirkungskreis wahrgenommen werden. Somit nutzen diese Stellen alle das vom TMIL vorgegebene Wohngeldfachverfahren. Daher lag es auf der Hand zu prüfen, ob es sich hierbei um ein Verbundverfahren gemäß § 7a Thüringer Datenschutzgesetz handelt. Nach Prüfung des TLfDI stellte sich aber heraus, dass dies nicht der Fall ist, da zwar das glei-

che automatisierte Verfahren in den Wohngeldstellen genutzt wird, eine gemeinsame Verarbeitung personenbezogener Daten aber nicht möglich ist. Die Wohngeldstellen können nur jeweils auf die Daten im eigenen Aufgabenkreis zugreifen. Wie sich weiter zeigte, werden die Daten nicht durch die Wohngeldstellen selbst, sondern mittels Auftragsdatenverarbeitung durch das Thüringer Landesrechenzentrum (TLRZ) verarbeitet. Der TLfDI hat dem TMIL mitgeteilt, dass zweckmäßigerweise ein Musterformblatt für das Verfahrensverzeichnis gemäß § 10 ThürDSG sowie eine Mustervereinbarung zur Vereinbarung über die Auftragsdatenverarbeitung nach § 8 ThürDSG mit dem TLRZ zentral erstellt werden und diese dann von den zuständigen Wohngeldstellen als Daten verarbeitende Stellen jeweils angepasst und unterschrieben in das eigene Verfahrensverzeichnis bzw. zu den Akten genommen werden muss. Der TLfDI hatte sich die Musterunterlagen zur datenschutzrechtlichen Prüfung vorlegen lassen und gegen deren Verwendung in den Wohngeldstellen keine Bedenken erhoben. Im Zusammenhang mit der Einführung dieses Verfahrens fragte ein Landkreis an, ob die Formblätter zur Eintragung in das Verfahrensverzeichnis vom behördlichen Datenschutzbeauftragten (bDSB) des Landkreises unterschrieben werden können. Wie dies vom TLRZ bereits gegenüber der Arbeitsgemeinschaft der kommunalen Spitzenverbände, Gemeinde- und Städtebund Thüringen e. V. vertreten wurde, bestätigte der TLfDI dem Landkreis, dass die Formblätter zum Verfahrensverzeichnis keinesfalls vom bDSB unterschrieben werden dürfen. Dies muss im Regelfall durch den für die Verarbeitung der Wohngelddaten verantwortlichen Leiter erfolgen. Aufgabe des bDSB ist nach § 10a Abs. 2 Nr. 2 ThürDSG lediglich, das Verfahrensverzeichnis zu führen und die verantwortliche Stelle über die datenschutzrechtlichen Vorschriften sowie über die sich hieraus ergebenden Erfordernisse zu informieren.

Verfahren, die von einem Ministerium zur Nutzung zentral den hierfür verantwortlichen Stellen vorgegeben werden, sind nicht notwendigerweise Verbundverfahren gemäß § 7a ThürDSG. Wenn keine gemeinsame Verarbeitung der personenbezogenen Daten erfolgt, so bleibt jede Daten verarbeitende Stelle für die Verarbeitung der Daten selbst verantwortlich. Sie muss die Formblätter über das automatisierte Verfahren in das bei ihr geführte Verfahrensverzeichnis aufnehmen. Dies gilt gleichfalls für eine vorgegebene Verarbeitung als

Auftragsdatenverarbeitung. Auch hier muss jede Daten verarbeitende Stelle einen eigenen Vertrag mit dem Auftragnehmer abschließen.

13.6 Wer darf was sehen? – Die Last mit dem Baulastenverzeichnis

Ein Bürger bat den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) im Berichtszeitraum um seine rechtliche Einschätzung, von wem unter welchen Bedingungen eine Einsicht in das Baulastenverzeichnis erfolgen kann. Der Bürger trug vor, dass das für ihn zuständige Landratsamt von Kaufinteressenten für die Gewährung der Einsichtnahme in das besagte Baulastenverzeichnis die Vorlage eines Kaufvertragsentwurfs verlange.
Der TLfDI hielt diese Praxis des Landratsamtes aus folgenden Gründen für zu restriktiv:
§ 82 Abs. 5 Thüringer Bauordnung (ThürBO) regelt, dass derjenige Einsicht in das Baulastenverzeichnis nehmen darf, der ein **berechtigtes Interesse** darlegt. In der Gesetzesbegründung zu § 82 Abs. 5 ThürBO (siehe dazu die Drucksache 5/5768, Seiten 155 bis 156) wird ausgeführt, dass ein berechtigtes Interesse regelmäßig bei denjenigen gegeben ist, die Rechte am Grundstück haben oder erwerben wollen. Aufgrund dieser Formulierung reicht nach Auffassung des TLfDI ein Interesse am Kauf eines Grundstücks aus. Die Vorlage eines Kaufvertrages wird indes nicht gefordert.
Zu dem parallel verwendeten Begriff „berechtigtes Interesse“ in § 12 Grundbuchordnung wird in der einschlägigen Literatur (z. B. Demharter, Kommentar zur Grundbuchordnung, 29. Auflage, § 12, Rd. 7) ausgeführt, es genüge, dass der Antragsteller ein verständiges, durch die Sachlage gerechtfertigtes Interesse verfolge; ausreichend sei, dass sachliche Gründe vorgetragen werden, welche die Verfolgung unbefugter Zwecke oder bloßer Neugier ausgeschlossen erscheinen lassen.
Der beabsichtigte Grundstückskauf stellt nach Auffassung des TLfDI ein durch die Sachlage gerechtfertigtes Interesse an der Einsicht in das Baulastenverzeichnis dar. Die dortigen Eintragungen können Einfluss auf die Höhe des Kaufpreises oder auch darauf haben, ob das Grundstück überhaupt der Interessenlage des möglichen Käufers genügt, und ob so überhaupt ein Kaufvertrag geschlossen werden soll. Gerade in Bezug auf die letzte Alternative macht es daher keinen Sinn, den Entwurf eines Kaufvertrages zu verlangen, der in aller

Regel mit Kosten verbunden sein dürfte. Der Einblick in das Baulastenverzeichnis soll gerade erst der Feststellung dienen, ob es Sinn macht, weiter in Grundstückskaufverhandlungen einzutreten. Die Forderung nach einer Vorlage eines Kaufvertragsentwurfes steht dazu im Widerspruch.
Daher sah der TLfDI im Ergebnis die Forderung des Landratsamtes, für die Gewährung der Einsichtnahme in das Baulastenverzeichnis einen Kaufvertragsentwurf vorzulegen als unverhältnismäßig an.
Ferner wies der TLfDI auf Folgendes hin: Eine praktische Lösung des Problems könnte für den Fall, dass tatsächlich personenbezogene Daten im Baulastenverzeichnis enthalten sind, darin bestehen, dass der Grundstückseigentümer dem Kaufinteressenten eine Einwilligung zur Einsichtnahme ins Baulastenverzeichnis erteilt.

Die Einsichtnahme in das Baulastenverzeichnis setzt gem. § 82 Abs. 5 ThürBO ein berechtigtes Interesse voraus. Dies ist bereits dann gegeben, wenn sachliche Gründe vorgetragen werden, die die Verfolgung unbefugter Zwecke ausgeschlossen erscheinen lassen. Regelmäßig die Vorlage eines Kaufvertragsentwurfes für die Gewährung der Einsichtnahme zu verlangen, ist hingegen unverhältnismäßig.

13.7 Verwendung von Vordrucken im Wohngeldbereich

Im Arbeitskreis Gesundheit und Soziales der Konferenz der unabhängigen Datenschutzbeauftragten des Bundes und der Länder (DSK) wurden Informationen über die in den Ländern verwendeten Formulare zur Beantragung von Wohngeld ausgetauscht. Auf Bundesebene gibt es hierfür keine einheitlichen Formulare, d. h. die Wohngeldbehörden der Bundesländer haben jeweils eigene Formulare. Im Hinblick auf die entsprechenden Thüringer Formulare wandte sich der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) mit datenschutzrechtlichen Bedenken an das für Wohngeld zuständige Thüringer Ministerium für Infrastruktur und Landwirtschaft (TMIL).
Der TLfDI bat das TMIL um Auskunft darüber, warum in dem entsprechenden Thüringer Formular zur Beantragung von Wohngeld besondere Angaben des Antragstellers durch die Leitung des Wohnheims, in dem der Antragsteller untergebracht ist bzw. untergebracht werden soll, bestätigt werden müssen. Die zu bestätigenden Angaben

ergeben sich bereits aus den vom Antragsteller vorzulegenden Dokumenten. Der TLfDI wies das TMIL darauf hin, dass erforderliche Daten gemäß § 19 Abs. 2 Satz 1 Thüringer Datenschutzgesetz (ThürDSG) beim Betroffenen erhoben werden müssen (Grundsatz der Datenerhebung beim Betroffenen). Daher sollten die dem TMIL nachgeordneten Bereiche darüber informiert werden, dass Formulare, die eine Bestätigung durch die Heimleitung vorsehen, nicht mehr genutzt werden dürfen.
Das TMIL legte gegenüber dem TLfDI dar, dass die Thüringer Wohngeldbehörden Antragsformulare für Heimbewohner verwenden, die inhaltlich dem vom TMIL als zuständigem Ministerium vorgegebenen Formular entsprechen. Angaben zum Heim selbst und zum genutzten Wohnraum müssen nach Aussage des TMIL gemäß Wohngeldgesetz zur Prüfung der Wohngeldberechtigung und für statistische Zwecke grundsätzlich erhoben werden. Wie der TLfDI, so hielt es auch das TMIL für datenschutzrechtlich bedenklich, Angaben über den Antragsteller im gleichen Formular zu erheben wie Angaben über die Heimleitung. Daher regte der behördliche Datenschutzbeauftragte (bDSB) des TMIL an, das Thüringer Formular zum Wohngeldantrag für Heimbewohner diesbezüglich abzuändern. Im neuen Formular sollen zukünftig alle Angaben entfallen, die durch die Heimleitung bzw. deren Vertretung auszufüllen sind. Nach Darlegung des bDSB soll die Heimleitung diese Angaben in einer separaten Anlage zum Wohngeldantrag selbst an die Behörde übermitteln. Dies schließt auch bestätigende Angaben der Heimleitung über den/die wohngeldbeantragende/n Heimbewohner/in ein.
Nach Information des TMIL soll die datenschutzrechtliche Anpassung des Wohngeldformulars im Rahmen der nächsten Überarbeitung am Jahresende 2017 erfolgen. Im Hinblick darauf bat der TLfDI das TMIL, ihm ein Exemplar des künftigen neuen Formulars zu übersenden, sobald dieses vorliegt. Vorab geht der TLfDI jedoch davon aus, dass mit dem neuen Formular die datenschutzrechtlichen Anforderungen ab 1. Januar 2018 erfüllt werden und dankte dem TMIL für die in dieser Hinsicht getroffenen Maßnahmen.

Gemäß § 19 Abs. 2 Satz 1 Thüringer Datenschutzgesetz (ThürDSG) müssen personenbezogene Daten beim Betroffenen erhoben werden. Dies gilt auch für amtliche Formulare zur Beantragung von Wohngeld. Entsprechende Formulare, die eine Bestätigung von personenbezogenen Daten des Antragstellers/der Antragstellerin durch die

Heimleitung vorsehen, dürfen aus datenschutzrechtlichen Gründen nicht genutzt werden.



Brigth lightbulbs and connections… - © sdecoret

14. Umwelt, Energie und Naturschutz

14.1 Wildwuchs: Wildkameras

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) erhielt die Anfrage eines Bürgers zum Einsatz von Wildkameras im Stadtwald von Jena. Hintergrund hierfür war eine entsprechende Stadtratsanfrage, deren Beantwortung den Bürger aber wohl nicht zufrieden stellte. Wie aus dem Stadtratsprotokoll zu entnehmen war, ist der Stadt Jena nicht bekannt, ob und falls ja, wie viele Wildkameras im Jenaer Stadtwald zum Einsatz kommen. Dieses sei weder beantragt worden, noch habe es bislang eine Erfordernis gegeben, zu prüfen, ob die Stadt Jena das Aufstellen von Kameras genehmigen kann oder nicht. Es wurde weiterhin darauf verwiesen, dass fast der gesamte Stadtwald unter Naturschutz stehe und es daher Waldbesuchern ohnehin nur erlaubt sei, auf den hierfür vorgesehenen Wegen zu bleiben. Es sei untersagt, auf den öffentlich begehbaren Flächen Wildkameras einzusetzen. In allen anderen Bereichen gehe man davon aus, dass unter bestimmten Umständen das Installieren von Wildkameras zulässig sein könne. Die Stadt Jena sei der Auffassung, dass die bestehenden datenschutzrechtlichen Bestimmungen nicht ausreichen und der Gesetzgeber gefragt sei, für diesen Bereich klare Regelungen zu schaffen.
Der TLfDI wies in seiner Stellungnahme gegenüber dem Bürger darauf hin, dass beim Betrieb einer Wildkamera zu unterscheiden ist, ob diese von einer öffentlichen Stelle, zum Beispiel einem Forstamt, oder von einer nicht-öffentlichen Stelle, hier überwiegend der privaten Jägerschaft, eingesetzt wird. Während die Zulässigkeit des Ein-

satzes von Wildkameras durch die private Jägerschaft in öffentlich zugänglichen Räumen sich nach § 6b Bundesdatenschutzgesetz (BDSG) bestimmt, sind die Zulässigkeitsvoraussetzungen für Videoüberwachung, etwa durch Forstämter, worunter auch Wildkameras fallen, in § 25a Thüringer Datenschutzgesetz (ThürDSG) geregelt. Der TLfDI hält den Einsatz von Wildkameras in öffentlich zugänglichen Gebieten regelmäßig für unzulässig. Wenn solche Kameras in ausdrücklich vom Betreten durch die Öffentlichkeit ausgeschlossenen forstbetrieblichen und jagdlichen Einrichtungen betrieben werden, ist hingegen nicht von einem überwiegenden schutzwürdigen Interesse der Betroffenen, z. B. Spaziergänger, auszugehen. Bei einer Interessenabwägung überwiegt hier das Interesse der verantwortlichen Stelle an der Videoüberwachung. Im Einzelfall sind auch zahlreiche Graubereiche zu bewerten. Gibt es in grundsätzlich öffentlich zugänglichen Bereichen ein Interesse an einer Beobachtung mit der Wildkamera und ist hierbei eine Beobachtung von Personen äußerst unwahrscheinlich oder lässt die Anbringungshöhe oder die Auflösung der Bilder keinen Personenbezug zu, so kann dies eventuell ebenfalls aus datenschutzrechtlicher Sicht unproblematisch sein. Nach § 6b Abs. 2 BDSG muss der Umstand der Beobachtung und die verantwortliche Stelle durch geeignete Maßnahmen erkennbar gemacht werden. Weiterhin müssen nicht-öffentliche Stellen, wie etwa private Jäger, die eine Wildkamera einsetzen wollen, dies zuvor dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) als zuständige Aufsichtsbehörde melden. Der Inhalt der erforderlichen Meldepflicht auch für Private (Nichtjäger) ergibt sich aus § 4e BDSG. (siehe hierzu auch die Pressemitteilung des TLfDI vom 19. Mai 2016 Anlage 27 und unter https://www.tlfdi.de/mam/tlfdi/presse/pm19052016.pdf). Ein unzulässiger Einsatz von Wildkameras kann vom TLfDI als Ordnungswidrigkeit mit einer Geldbuße geahndet werden. In der Tat besteht aber für den Bereich der öffentlichen Stellen bei Einsatz von Wildkameras eine Regelungslücke. Da der bereits genannte § 25a ThürDSG lediglich den Einsatz von Videoüberwachung zur Wahrnehmung des Hausrechts der verantwortlichen öffentlichen Stelle regelt, ein solches Hausrecht der öffentlichen Stelle am Staats- und

Körperschaftswald aber grundsätzlich nicht zukommt, hätte dies zur Folge, dass z. B. die Landesforstanstalten auf jegliche Wildkameras verzichten müssten. Um diesen vom Gesetzgeber nicht gewollten Zustand zu verhindern, ist der TLfDI hier nach Prüfung zum Ergebnis gekommen, dass öffentliche Stellen in den von ihnen verwalteten Wäldern zumindest an jagdlichen Einrichtungen, deren Betreten dem einfachen Waldbesucher aufgrund von Bußgeldvorschriften untersagt ist, ein Hausrecht innehaben können. Auch hier verlangt § 25a Abs. 2 ThürDSG eine Kenntlichmachung der Videoüberwachung. Darf der Jenaer Stadtwald also aus Naturschutzgründen von der Öffentlichkeit nur auf den hierzu vorgesehenen Wegen betreten werden, so kann ein Betrieb von Wildkameras jenseits der Wege zumindest aus datenschutzrechtlicher Sicht erlaubt sein.

In öffentlich zugänglichen Räumen bestimmt sich die Zulässigkeit des Einsatzes von Wildkameras für private Stellen nach den Regelungen des § 6b BDSG. Im Regelfall überwiegt hierbei das schutzwürdige Interesse des Betroffenen. Bei öffentlichen Stellen gibt es im ThürDSG keine speziellen Vorschriften, die diesen Sachverhalt regeln. Auch hier überwiegt regelmäßig das schutzwürdige Interesse des Betroffenen. In nicht-öffentlich zugänglichen Waldgebieten wird der Einsatz von Wildkameras weder vom BDSG noch vom ThürDSG geregelt. Schutzwürdige Interessen des Betroffenen bestehen hier überwiegend nicht.

14.2 Immissionsschutzbehörde versus Schornsteinfegerinnung: entrußter Datenschutz

Wie im 11. Tätigkeitsbericht unter 13.6 berichtet, hatte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) der unteren Immissionsschutzbehörde mitgeteilt, dass es aus datenschutzrechtlicher Sicht unzulässig ist, bei den Bezirksschornsteinfegern ohne gesetzliche Grundlage personenbezogene Daten von Eigentümern, die Feuerungsanlagen betreiben, zu erheben. Erst nachdem der TLfDI die untere Immissionsschutzbehörde unter Hinweis auf eine mögliche Beanstandung mehrfach auf ihre Unterstützungspflicht hingewiesen hatte, nahm die Behörde zum Sachverhalt Stellung. Danach werden seit Jahren die Grenzwerte von Luftschadstoffen überschritten, unter anderem auch im Zuständigkeitsbereich der unteren Immissionsschutzbehörde. Aufgrund eines von der EU in

diesem Zusammenhang eingeleiteten Vertragsverletzungsverfahrens bestehe dringender Handlungsbedarf festzustellen, wer welchen Hausbrand mit Brennstoffen erzeugt, die einen hohen Emissionsanteil enthalten. Die Betreiber bzw. Besitzer von Hausbrandanlagen sollen angeschrieben und auf bestehende Fördermöglichkeiten bei einer Nachrüstung ihrer Anlagen hingewiesen werden. Die Behörde hatte angekündigt, zwar auf die Erhebung der von den Bezirksschornsteinfegern festgestellten Messwerte der Feuerungsanlagen zu verzichten, jedoch weiterhin bei der Schornsteinfegerinnung die Adressen der Betreiber bzw. Besitzer von Hausbrandanlagen in dem betroffenen Gebiet zu erheben. Der TLfDI schlug der Behörde vor, zur gezielten Ansprache des betroffenen Personenkreises ein sogenanntes Adressmittlungsverfahren einzusetzen. Bei diesem Verfahren kann die untere Immissionsschutzbehörde die zu versendenden Anschreiben der Schornsteinfegerinnung übergeben, die diese dann an die Zielpersonen versenden können, ohne dass der Behörde die konkreten Adressen zur Verfügung gestellt werden müssen.
Erst nach mehreren Nachfragen und Erinnerungsschreiben teilte die untere Immissionsschutzbehörde mit, dass sie die Auffassung des TLfDI akzeptiere und auf die generelle Datenerhebung zu Betreibern und Besitzern von Feuerungsanlagen sowohl bei den Bezirksschornsteinfegern als auch bei der Schornsteinfegerinnung verzichte.

Ohne begründete Anhaltspunkte darf die untere Immissionsschutzbehörde den Bezirksschornsteinfeger nicht auffordern, ihr personenbezogen wahllos alle Eigentümerdaten einer Feuerungsanlage einschließlich der technischen Daten der Anlage sowie der dort gemessenen Werte vorzulegen. Dies stellt zum einen alle Feuerstättenbetreiber unter einen gewissen Generalverdacht und zum anderen ist gegebenenfalls hier auch ein Misstrauen gegenüber den Bezirksschornsteinfegern dahingehend abzuleiten, ob diese ihrer Anzeigepflicht nachkommen.

14.3 Erstellung eines Solarkatasters – datenschutzrechtlich sonnenklar

Eine Agentur wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und bat um eine Grundsatzberatung, was für die Erstellung eines Solarkatasters für den gesamten Freistaat zu beachten sei.

Das Ziel besteht darin, flächendeckend für den gesamten Freistaat eine Solarpotenzialanalyse zu erstellen. Damit sollen einerseits Analysen auf regionaler Ebene ermöglicht und damit eine Grundlage für Maßnahmenpläne im Rahmen von Energie- und Klimaschutzkonzepten geliefert werden, andererseits soll es den privaten und den öffentlichen Eigentümern von Immobilen oder Freiflächen belastbare Informationen über die zu erwartenden energetischen und finanziellen Erträge einer möglichen Solaranlage liefern und damit zu entsprechenden Investitionen anregen.
Um individuelle Nutzerabfragen zu ermöglichen, wird eine interaktive Web-Anwendung unter Zugrundelegung von Satelliten- und Luftbildern entwickelt und zur Verfügung gestellt (Anwendung wird beim Anbieter betrieben).
Das Solarkataster ist in folgende Bestandteile untergliedert:

1. Datenbank mit den landesweit berechneten Solarpotenzialdaten,
2. Bereitstellung der Inhalte für die Web-GIS-Anwendung und Bereitstellung der Solarpotenzialdaten als WMS- und WFS-Dienst,
3. Einrichtung und Betrieb der Web-GIS-Anwendung einschl. notwendiger Datenhaltung auf der IT-Infrastruktur des Auftragnehmers (Software-As-A-Service) und
4. Bereitstellung eines webbasierten Wirtschaftlichkeitsrechners für PV und Solarthermie unter Berücksichtigung bestimmter Parameter (z. B. Stromspeicher für den Eigenverbrauch) und Kopplung mit der Web-GIS-Anwendung.

Der TLfDI wies darauf hin, dass durch die Erkennbarkeit der Lage der Grundstücke ein Bezug zum Eigentümer hergestellt wird. Daher geht der TLfDI davon aus, dass es sich um personenbezogene Daten handelt.
Die von der Agentur geplante Datenerhebung unter Zugrundelegung von Satelliten- und Luftbildern kann nach § 19 Abs. 2 Nr. 3 Thüringer Datenschutzgesetz (ThürDSG) erfolgen, da die Datenerhebung beim Betroffenem einen unverhältnismäßigen Aufwand erfordern würde und keine Anhaltspunkte dafür vorliegen, dass überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt sind.
Die Datenspeicherung und Nutzung kann nach § 20 Abs. 2 Nr. 3 ThürDSG erfolgen, da offensichtlich ist, dass es im Interesse des Betroffenen liegt und kein Grund zu der Annahme besteht, dass er

seine Einwilligung verweigern würde in Verbindung mit § 5 Thüringer Geodatengesetz.
Als praktischer Hinweis wurde auf §§ 9 und 10 Thüringer Datenschutzgesetz, das Sicherheitskonzept und das Verfahrensverzeichnis aufmerksam gemacht.
Vermutlich wird die Umsetzung des Vorhabens so erfolgen, dass eine Auftragsdatenverarbeitung nach § 8 ThürDSG erfolgen wird. Die Voraussetzungen der Vorschrift wurden erläutert.
Im Ergebnis könnte eine „Widerspruchslösung“ entstehen, wie sie auch in Hessen praktiziert wird und die der TLfDI auch für das Solarkataster einer Kommune bereits empfohlen hat.
Unter Widerspruchslösung ist zu verstehen, dass zunächst eine Veröffentlichung erfolgt, der Betroffene jedoch eine Löschung jederzeit beantragen kann, und er auf diese Möglichkeit bei der Veröffentlichung auch entsprechend hingewiesen wird.

Der TLfDI hat auch eine Beratungsfunktion, die kostenlos wahrgenommen werden kann. Die Erstellung eines Solarkatasters ist grundsätzlich datenschutzrechtlich möglich.

14.4 Webcam: Kraniche versus Segler

Ein Segler, der regelmäßig mit seinem Boot den Stausee Kelbra befährt, wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und beschwerte sich über eine am sogenannten Vogelbeobachtungsturm installierte Kamera, die auf die Wasserfläche des Stausees gerichtet sei. Die Naturparkverwaltung Kyffhäuser bestätigte auf Anfrage des TLfDI die Inbetriebnahme einer solchen Kamera für die Monate Oktober bis Dezember. Ziel der Kamera sei es, den abendlichen Einflug tausender Kraniche auf den in dieser Zeit abgelassenen Stausee, sodass Wassersportaktivitäten nicht möglich sind, auf die Internetseite des Naturparks Kyffhäuser zu übertragen. Der TLfDI stellte bei der Bewertung des Sachverhalts zunächst fest, dass die Naturparkverwaltung Kyffhäuserkreis eine Einrichtung im Geschäftsbereich des Thüringer Ministeriums für Umwelt, Energie und Naturschutz ist und somit als öffentliche Stelle im Sinne von § 2 Thüringer Datenschutzgesetz (ThürDSG) gilt. § 25 ThürDSG regelt aber lediglich den Einsatz von Videoüberwachung im Zusammenhang mit der Wahrnehmung des Hausrechts der verantwortlichen öffentlichen Stelle. Die-

ser geregelte Sachverhalt war im beschriebenen Fall nicht betroffen, sodass sich hieraus keine Rechtsgrundlage über die Zulässigkeit des Betriebs der Videoüberwachung ergab. Spezielle Rechtsvorschriften, die den Kamerabetrieb erlauben, konnten ebenso wenig herangezogenen werden, wie die vorherige Einholung einer Einwilligung bei den Betroffenen. Ein zulässiges Betreiben der Videoüberwachung konnte sich deshalb nur dann ergeben, wenn entweder die Verarbeitung personenbezogener Daten grundsätzlich ausgeschlossen ist oder wenn das beobachtete Gebiet von hierzu nicht autorisierten Personen ausdrücklich nicht betreten werden darf. Wie sich aus einer Nachfrage bei der Naturparkverwaltung Kyffhäuser ergab, wird auf der Grundlage des Bundesnaturschutzgesetzes in den letzten Jahren ein Betretungsverbot zum Schutz des Kranichs vom Landkreis Nordhausen erlassen. Dieses Betretungsverbot gilt jeweils vom 1. Oktober bis 15. Dezember eines Jahres. Hierauf wird mit öffentlichen Bekanntmachungen sowie mit Schildern vor Ort hingewiesen. Ergänzend argumentierte die Naturparkverwaltung, dass das Naturschauspiel Kranichzug jährlich tausende Naturinteressierte anziehe und es ohne eine gezielte Besucherlenkung zu massiven Beunruhigungen der Tiere komme. Mit der Übertragung des Kranichzugs per Webcam sei es den zahlreichen Interessierten möglich, die Versammlung der Kraniche auf dem abgelassenen Stausee per Internet zu verfolgen, ohne persönlich vor Ort anwesend zu sein. Da viele Segler der Naturschutzbehörde gegenüber zum Ausdruck brachten, deren Angaben über die Betriebszeiten der Kamera nicht zu trauen, hat die Naturschutzparkverwaltung die Kamera vorläufig deinstalliert. Sie soll aber zu den angegebenen Zeiten wieder zum Einsatz gebracht werden. Der TLfDI hat gegen den Einsatz der Webcam in der geschilderten Form aufgrund des Betretungsverbots keine Bedenken geltend gemacht und dies dem Beschwerdeführer auch so mitgeteilt. Wenn der Zutritt von bestimmten Bereichen ausdrücklich untersagt ist, so handelt es sich um nicht-öffentliche Räume. Das sich aus dem Bundesnaturschutzgesetz ableitbare Betretungsverbot überwiegt hier die schutzwürdigen Interessen von Betroffenen, die sich unzulässiger Weise in diesem Bereich aufhalten und möglicherweise in den Beobachtungsbereich der Kamera gelangen.

Der Einsatz einer Webcam in einem aufgrund von naturschutzrechtlichen Vorschriften zum Schutz von Tieren durch Verbotsschilder ausdrücklich als nicht-öffentlich zugänglich gekennzeichneten Be-

reich ist zulässig. Die verantwortliche Stelle muss hier nicht mit einem schutzwürdigen Interesse von Betroffenen rechnen.



©determined-city on the construction helmet – fotolia.com

15. Wirtschaft, Wissenschaft und digitale Gesellschaft

15.1 Thüringer Zentrum für Existenzgründungen und Unternehmertum (ThEx)

Das neu gegründete Thüringer Zentrum für Existenzgründungen und Unternehmertum (ThEx) wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und bat diesen um eine umfassende datenschutzrechtliche Beratung des Projekts. Die finanzielle Förderung der ThEx und der darin tätigen 18 Projektpartner erfolgt durch das Thüringer Ministerium für Wirtschaft, Wissenschaft und Digitale Gesellschaft aus Mitteln des Europäischen Sozialfonds (ESF). Aufgabe des ThEx ist es, Gründungsinteressierten und Unternehmern bei Schritten in die Selbsts-

ändigkeit, bei der Suche nach Unternehmensnachfolgern, bei der Unternehmensförderung etc. Unterstützung zu leisten. Der Servicegedanke des ThEx ist es, diese Interessenten über nur einen Ansprechpartner direkt an die für ihn passenden Projektpartner zu vermitteln („One face to the customer“ oder „One-stop-office“). Hierfür steht den Gründungsinteressierten in der ThEx als erster Kontakt ein sogenannter Lotse zur Verfügung, der den Beratungsbedarf ermittelt und die passenden Projektpartner bestimmt. Ergibt sich aus dem so15.1 vermittelten Kontakt eine weitere Betreuung durch den Projektpartner, so erstellt die ThEx auf einer gemeinsamen webbasierten Arbeitsplattform „Kundenbeziehungsmanagementsystem“ einen Stammdatensatz über den jetzt als Teilnehmer bezeichneten Gründungsinteressierten. Dieser Stammdatensatz wird dann durch weitere Daten, z. B. Termin- und Projektdaten, die mit der individuellen Förderung des Teilnehmers entstehen, ergänzt. Zugriff auf diese Daten haben dann neben der ThEx selbst auch je nach Fallkonstellation die Projektpartner.

Der TLfDI bewertete die beschriebene Datenverarbeitung als automatisiertes Verbundverfahren nach § 7a Thüringer Datenschutzgesetz (ThürDSG) und wies die ThEx auf die sich hieraus ergebende Verpflichtung hin, die in § 7a Abs. 2 ThürDSG aufgeführten schriftlichen Festlegungen zu treffen. Das ThEx legte dem TLfDI diese Festlegungen sowie die Eintragung zum Verfahrensverzeichnis nach § 10 ThürDSG, die Einwilligungstexte für die Existenzgründer, die Netzwerkstruktur, das Sicherheitskonzept nach § 9 Abs. 2 ThürDSG, ein Rollen- und Berechtigungskonzept sowie zusätzlich, da das automatisierte Verfahren in Auftragsdatenverarbeitung durch eine private Stelle erfolgt, die vertragliche Vereinbarung über diese Auftragsdatenverarbeitung nach § 8 ThürDSG zur datenschutzrechtlichen Prüfung vor. Da die Unterlagen einige Fehler und Unklarheiten enthielten, bat der TLfDI die ThEx um eine entsprechende Überarbeitung der Papiere, was inzwischen auch erfolgt ist.

Im Zusammenhang mit der beschriebenen Datenverarbeitung wurde der TLfDI darauf aufmerksam, dass alle potenziellen Gründer einen speziellen Förderantrag ausfüllen müssen, der an die Gesellschaft für Arbeits- und Wirtschaftsförderung des Freistaats Thüringen mbH (GFAW) übermittelt wird. Mit diesem Fragebogen werden teilweise sensible Daten über die Teilnehmer der Fördermaßnahme erhoben. Nach einer intensiven Korrespondenz mit der GFAW konnte geklärt werden, dass gemäß der Verordnung (EU) Nr. 1304/2013 DES EU-

ROPÄISCHEN PARLAMENTS UND DES RATES vom 17. Dezember 2013 über den Europäischen Sozialfonds und zur Aufhebung der Verordnung (EG) Nr. 1081/2006 des Rates im Anhang 1 die Verpflichtung besteht, über Teilnehmer, die von einer ESF-Intervention profitieren, gemeinsame Outputindikatoren zu erheben. Hierzu zählen Fragen etwa nach dem erreichten Schul- und Berufsabschluss, Erwerbsstatus, Arbeitslosigkeit, Nichterwerbstätigkeit, Schulbildung, der Anzahl der im Haushalt lebenden unterhaltsberechtigten Kinder usw. Fragen nach der Angehörigkeit zu einer Minderheit oder nach einer Behinderung sind im Fragebogen als freiwillig gekennzeichnet. Auch dies sieht die oben genannte EU-Verordnung so vor. Vor diesem Hintergrund hat der TLfDI gegen den Fragebogen keine Bedenken mehr geltend gemacht.

Das ThEx verarbeitet im Zusammenhang mit der Förderung von Existenzgründern zahlreiche personenbezogene Daten. Der TLfDI konnte erreichen, dass die formalen Voraussetzungen zur Verarbeitung dieser Daten im Verbundverfahren inzwischen gegeben sind.

15.2 GFAW will Daten der Verbraucherzentrale

Den Bundesländern werden in der Förderperiode 2014 bis 2020 aus dem Europäischen Sozialfonds (ESF) Fördergelder für unterschiedliche Zwecke zur Verfügung gestellt, z. B. zur Förderung nachhaltiger und hochwertiger Beschäftigung. Im Regelfall stellen die sogenannten Projektträger einen ESF-Antrag für eine Zuwendung. Werden die Prüfkriterien vom Projektträger erfüllt, so werden die Fördermittel bewilligt.
In diesem Zusammenhang beschwerte sich eine Verbraucherzentrale beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) über den Umgang der Gesellschaft für Arbeits- und Wirtschaftsförderung des Freistaats Thüringen mbH (GFAW) mit den Personalakten der Mitarbeiter der Verbraucherzentrale. Die GFAW wollte zur Prüfung der förderfähigen Bestandteile der Personalkosten die Eingruppierungen der Mitarbeiter der Verbraucherzentrale prüfen, indem sie Einsicht in die Personalakten der Mitarbeiter nehmen wollte und die Herausgabe von Kopien verschiedener Teile der Personalakten, wie Arbeitsverträge, Qualifikationsnachweise, Stellenbeschreibungen usw. verlangte. Die Unterlagen sollten bei der GFAW für mindestens zehn Jahre aufbewahrt

werden. Da die Verbraucherzentrale es abgelehnt hatte, diese Kopien der GFAW zu übermitteln, wurde ihr nahe gelegt, dass ohne die Übermittlung der vollständigen, nicht pseudonymisierten Personalunterlagen eine Streichung der ESF-Projektfördermittel in Betracht gezogen werden müsse.
Der TLfDI wandte sich zur Klärung des Sachverhalts an die GFAW und bat um Mitteilung, aus welchen Rechtsgrundlagen sich die Zulässigkeit ergibt, umfassende Personalunterlagenkopien derjenigen Mitarbeiter der Verbraucherzentrale, die aus den an die Verbraucherzentrale ausgereichten Fördergeldern bezahlt werden, bei der GFAW für zehn Jahre zu speichern. In ihrer Antwort verwies die GFAW darauf, dass diese mit der Wahrnehmung hoheitlicher Aufgaben auf dem Gebiet von Zuwendungen beliehen sei, daher in diesem Bereich die Funktion einer Behörde ausführe und an die Einhaltung der geltenden Rechtsvorschriften gebunden sei. Das Zuwendungsverfahren sei im Wesentlichen in den Verwaltungsvorschriften zu den §§ 23 und 44 Thüringer Landeshaushaltsordnung sowie den hierzu erlassenen Allgemeinen Nebenbestimmungen geregelt. Hierzu gehört auch die Prüfung, ob der Zuwendungsempfänger nicht gegen das Besserstellungsverbot verstößt, das die geförderte Person hinsichtlich der Gehaltshöhe und der regelmäßigen Arbeitszeit nicht besser stellt als vergleichbare Bedienstete im Landesdienst.
Nach Prüfung der von der GFAW angegebenen Rechtsvorschriften kam der TLfDI zum Ergebnis, dass hierin nicht ausdrücklich geregelt ist, welche Personalunterlagen in welcher Form geprüft werden müssen. Darüber hinaus wird eine stichpunktartige Prüfung der Unterlagen für ausreichend angesehen. Eine Erforderlichkeit für eine vollständige Übersendung dieser Unterlagen von allen betroffenen Mitarbeitern der Verbraucherzentrale hatte sich aus der Vorschrift jedenfalls nicht ergeben. Da die GFAW sich dieser datenschutzrechtlichen Bewertung des Sachverhalts keinesfalls anschließen konnte, führte der TLfDI mit der GFAW ein Gespräch, an dem auch das Thüringer Ministerium für Arbeit, Soziales, Gesundheit, Frauen und Familie als Prüfbehörde und der Thüringer Rechnungshof teilnahmen. Die Gesprächspartner verwiesen neben ihren eigenen Prüfkompetenzen auf eine weitere mögliche Prüfung der Personalunterlagen auf der Ebene der EU-Kommission. Die GFAW sei verpflichtet, die Rechtmäßigkeit der ausgezahlten Förderbedarfe der Höhe und Dauer nach gegenüber den genannten Institutionen nachzuweisen. Dabei sei nicht bekannt, wann die EU-Kommission die Prüfungen innerhalb der

Förderperiode für abgeschlossen erklärt, sodass man keine konkrete Aufbewahrungsfrist für die kopierten Unterlagen festlegen könne. Der TLfDI blieb nach nochmaliger Prüfung aller angegebenen Rechtsgrundlagen und Verfahrensbeschreibungen bei seiner Rechtsauffassung, wonach auch aus den entsprechenden EU-Verordnungen (Art. 122 ff., insbesondere Art. 127 Abs. 1 Verordnung (EU) Nr. 1303/2013 und Art. 27 ff. der delegierten Verordnung (EU) 480/2014) lediglich die Anwendung von Stichprobenverfahren für Prüfungen der Prüfbehörden vorgeschrieben ist. Einig war sich der TLfDI mit den Gesprächspartnern darüber, dass die Zuwendungsempfänger verpflichtet sind, die bei ihm aus EU-Fördergeldern finanzierten Mitarbeiter über das Prüfverfahren vor Abschluss eines Arbeitsvertrags zu unterrichten. Die Bewilligungsbehörde ist berechtigt, Geschäftsunterlagen sowie die zur Aufgabenerfüllung erforderlichen Personalaktenteile der aus den Zuwendungen entlohnten Beschäftigten durch örtliche Erhebungen zu prüfen oder auch für Prüfungen anzufordern. Der TLfDI hat auch zugestimmt, dass bei Personalakten, aus denen sich eine Differenz zwischen der Vergütung und z. B. der Qualifikation des Beschäftigten, der zu erfüllenden Aufgabe, des zeitlichen Einsatzes usw. ergibt, entsprechende Kopien für einen Kürzungsbescheid erstellt und zu den Akten der GFAW genommen werden dürfen.

Allerding ist gemäß § 4 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) die Verarbeitung und Nutzung personenbezogener Daten nur zulässig, wenn dieses Gesetz oder eine andere Rechtsvorschrift sie erlaubt oder anordnet oder soweit der Betroffene eingewilligt hat. In § 20 Abs. 1 Satz 1 ThürDSG ist näher bestimmt, dass das Speichern, Verändern oder Nutzen personenbezogener Daten zulässig ist, wenn es zur Erfüllung der in der Zuständigkeit der Daten verarbeitenden Stelle liegenden Aufgabe erforderlich ist und es für Zwecke erfolgt, für die die Daten erhoben worden sind. Eine solche Erlaubnisnorm zur umfassenden Datenspeicherung kann der TLfDI aber, wie oben dargelegt, weder den geprüften EU-Verordnungen noch der Thüringer Landeshaushaltsordnung entnehmen. Auch die Gesprächspartner der GFAW, des Thüringer Ministeriums für Arbeit, Soziales, Gesundheit, Frauen und Familie sowie des Thüringer Rechnungshofs konnten auf keine spezielle Rechtsgrundlage verweisen, die das bislang praktizierte Verfahren konkret regelt. Zum anderen ist auch dem ThürDSG keine Rechtsvorschrift zu entnehmen, die das Erheben dieser Daten erlaubt. Gemäß § 20 Abs. 1 ThürDSG

muss das Speichern zur Erfüllung der Aufgabe der verarbeitenden Stelle erforderlich sein. Der Begriff der Erforderlichkeit ist vor dem Hintergrund des Gebotes der Datenvermeidung und Datensparsamkeit auszulegen. Das Bundesverfassungsgericht (BVerfG) hat in seinem sogenannten Volkszählungsurteil (BVerfGE 65, 1/46) festgestellt, dass das Sammeln auf Vorrat zu unbestimmten oder noch nicht bestimmten Zwecken mit dem Gebot der notwendigen gesetzlichen Festlegung des Verwendungszweckes nicht vereinbar ist. Diese Wertung trifft auch die ab 25. Mai 2018 wirksam werdende Verordnung (EU) 2016/679 des Europäischen Parlaments und des vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung – DS-GVO) in Artikel 5 Buchstabe d). Danach müssen personenbezogene Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein (Grundsatz der Datenminimierung). Aus datenschutzrechtlicher Sicht ist keine Erforderlichkeit festzustellen, alle prüfungsrelevanten Personalaktenteile des beim Zuwendungsempfänger beschäftigten Personals grundsätzlich mit der Begründung, die umfassende Prüfaufgabe könne von der GFAW nicht in absehbarer Zeit bewältigt werden, zu kopieren und dort quasi eine Teilakte der Personalakte auf unbestimmte Zeit aufzubewahren. Ebenso wenig kann die Aufbewahrung der Kopien mit einer möglichen Prüfung durch weitere Prüfstellen gerechtfertigt werden. „Es genügt nicht, dass die Daten zur Aufgabenerfüllung geeignet und zweckmäßig sind.“ Eine Erforderlichkeit ist erst dann gegeben, wenn die Stelle „im jeweiligen konkreten Einzelfall ihre Aufgabe nicht, nicht vollständig oder nicht in rechtmäßiger Weise erfüllen kann und außerdem erst aktuell dann und nur in dem Umfang, wie es die Aufgabenerfüllung gerade in Bezug auf die betroffene Person erfordert“ (Sokol/Scholz in: Simitis, BDSG, § 13 Rdnr. 26). Es muss auch berücksichtigt werden, dass die Originalunterlagen beim Zuwendungsempfänger geführt werden und für eventuelle Prüfungen den Prüfstellen zur Verfügung stehen. Bereits aus diesem Grund sieht der TLfDI keine Erforderlichkeit, alle genannten Unterlagen bei der Prüfbehörde in Kopie aufzubewahren. Die Verbraucherzentrale wurde über das Ergebnis des TLfDI unterrichtet.

In einem weiteren Gespräch zwischen dem TLfDI und der GFAW hat diese die Verfahrensweise der nunmehr stichprobenartigen Prü-

fung der Verwendungsnachweise dargelegt. Die Grundlage ist hierbei immer das jeweils geförderte Projekt. Alle Projekte, die im Zusammenhang mit der Finanzierung von Mitarbeitern stehen, werden danach stichprobenartig untersucht, indem aus dem Pool der von der Förderung betroffenen Mitarbeiter im Hinblick auf diese Stichproben von der GFAW Unterlagen angefordert werden. Bei der Anforderung stellt die GFAW noch genauer dar, welche Informationen konkret benötigt werden und macht deutlich, dass alle anderen, nicht zur Prüfung erforderlichen Informationen vom Zuwendungsempfänger geschwärzt werden können. Der TLfDI hält die nunmehr vorgeschlagene Verfahrensweise der Zuwendungsprüfung aus datenschutzrechtlicher Sicht für akzeptabel.

Bei der Inanspruchnahme von Fördergeldern aus dem ESF ist der Zuwendungsempfänger gegenüber den hierzu bestimmten Prüfungsstellen verpflichtet, den Nachweis über die korrekte Verwendung dieser Fördermittel zu führen. Bei der Fördermittelprüfung dürfen z. B. Vor-Ort-Prüfungen erfolgen, bei denen auch in alle relevanten Originalbelege Einsicht genommen werden darf und in Fällen von festgestellten Unregelmäßigkeiten dürfen auch Kopien hiervon erstellt werden. Eine anlasslose und flächendeckende Erstellung von Kopien aller Verwendungsnachweise und deren Speicherung bei der Prüfstelle ist aber aus datenschutzrechtlicher Sicht nicht zulässig.

15.3 Untersagung der Berufsausübung per E-Mail?

Im Rahmen der Zusammenarbeit mit Gremien hat der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) an den Sitzungen der Arbeitsgruppe „Rechtssetzung“ unter Vorsitz des Thüringer Ministeriums für Wirtschaft, Wissenschaft und digitale Gesellschaft teilgenommen und die Beratungen zum Thüringer Gesetz zur Verbesserung der Feststellung und Anerkennung im Ausland erworbener Berufsqualifikationen – Thüringer Anerkennungsgesetz – datenschutzrechtlich begleitet.
Das zum 1. Mai 2014 in Kraft getretene Thüringer Anerkennungsgesetz schafft für landesrechtlich reglementierte Berufe einen Anspruch auf Feststellung der Gleichwertigkeit von im Ausland erworbener Qualifikationen. In Bezug auf die Richtlinie 2013/55/EU des Europäischen Parlaments und des Rates vom 20. November 2013 zur Änderung der Richtlinie 2005/36/EG (Berufsanerkennungsrichtlinie)

und der Verordnung (EU) Nr. 1024/2012 (IMI-Verordnung) wurde die Änderung des Thüringer Berufsqualifikationsfeststellungsgesetzes als vorteilhaft gegenüber der Änderung in den Fachgesetzen angesehen. Entsprechend der Vorgaben der EU musste dies bis spätestens 18. Januar 2016 erfolgen.
Den Beratungen lag der Musterentwurf für ein Anerkennungsgesetz durch die Länder zugrunde, das in einer Unterarbeitsgruppe zur Koordinierung der zuständigen Ressorts der Länder erarbeitet wurde. Es regelt das Verfahren für die Feststellung der Gleichwertigkeit im Ausland erworbener Ausbildungsnachweise unter Berücksichtigung sonstiger nachgewiesener Berufsqualifikationen und inländischer Ausbildungsnachweise für Berufe, die durch Rechtsvorschriften der Länder oder des Bundes geregelt sind. Hierfür müssen die Antragsteller neben den Nachweisen der Berufsqualifikation auch einen Identitätsnachweis vorlegen. Dabei können die Unterlagen, die in einem Mitgliedsstaat der Europäischen Union oder einem weiteren Vertragsstaat des Abkommens über den europäischen Wirtschaftsraum ausgestellt oder anerkannt wurden, auch elektronisch übermittelt werden. Hierzu ist das Binnenmarktinformationssystem (IMI) zu nutzen.
Zentrale datenschutzrechtliche Relevanz kam dem nach der Berufsanerkennungsrichtlinie vorgesehenen „Vorwarnmechanismus“ zu. Danach sind nämlich von der im Lande zuständigen Stelle die anderen zuständigen Stellen der Mitgliedsstaaten zu informieren, wenn einem Berufsangehörigen durch gerichtliche Entscheidung oder durch Verwaltungsakt die Ausübung seines Berufes ganz oder teilweise – auch vorübergehend – untersagt worden ist oder ihm Beschränkungen auferlegt wurden. Auch hierzu ist das IMI zu nutzen.
Die Vorschrift soll einen Schutz dagegen sicherstellen, dass eine Person, die in einem Mitgliedsstaat ein Berufsverbot hat, einfach ihre Qualifikation in einem anderen Mitgliedssaat anerkennen lässt und dort dann unbehelligt den ihr verbotenen Beruf ausübt. Hierzu waren weitere Festlegungen erforderlich, welche Stelle diese Aufgabe wahrnehmen sollte. Besondere Schwierigkeiten bereitete dabei der Zeitfaktor, denn es mussten kurze Fristen eingehalten werden. Dabei oblag die Entscheidung, ob eine Vorwarnung eingegeben wird, immer der Berufsverbot aussprechenden Stelle, deren „Weg“ in das IMI auch datenschutzgerecht gestaltet werden musste. Bei der Übersendung und Weiterleitung der Anträge an die zuständigen Stellen und für die Eingabe der Vorwarnung per E-Mail war daher besonde-

res Augenmerk auf die Vertraulichkeit und Integrität bei der Übertragung zu legen.
Daher hat der TLfDI eine verschlüsselte Übertragung als erforderliche technische Maßnahme nach § 9 Thüringer Datenschutzgesetz (ThürDSG) vorausgesetzt. Die verschlüssele Übertragung wurde in der Verordnung indes nicht festgeschrieben. Der TLfDI wies darauf hin, dass er ggf. in einer datenschutzrechtlichen Prüfung die verschlüsselte Datenübermittlung als erforderliche Maßnahme nach § 9 ThürDSG zur Gewährleistung des Datenschutzes ansieht.

Werden personenbezogene Daten per E-Mail weitergeleitet, sind die erforderlichen technischen und organisatorischen Maßnahmen nach § 9 ThürDSG zu treffen. Dies umfasst auch eine Verschlüsselung der Daten.

15.4 Schutz vor Spielsucht – Einführung einer Sperrdatei für Spielhallen datenschutzrechtlich unbedenklich?

Anfang 2016 wandte sich das (TMWWDG) an den Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Es war geplant, das Thüringer Spielhallengesetz zu ändern. Es sollte ein zentrales Sperrsystem unter Nutzung des hessischen Systems eingeführt werden. Der TLfDI wurde um Prüfung gebeten, ob grundsätzliche datenschutzrechtliche Bedenken bestehen würden.
Hessen hat auf der Grundlage des 1. Glücksspieländerungsstaatsvertrags für den Bereich der Sportwetten, Spielcasinos und Lotto ein bundesweites zentrales Sperrsystem entwickelt und ist hier auch zentraler Dienstleister. Auf der technischen Basis dieses Systems wurde auch ein landeseigenes zentrales Sperrsystem für Spielhallen entwickelt. Die notwendigen rechtlichen Grundlagen wurden in § 11 Spielhallengesetz Hessen (SpielhG He) festgelegt. Dieser hat folgenden Wortlaut:

„§ 11 SpielhG* [-Hessen] – *Sperrsystem

(1) [1]Mit der Sperrdatei werden die für eine Sperrung erforderlichen Daten verarbeitet und genutzt. [2]Es dürfen folgende Daten gespeichert werden:

Familiennamen, Vornamen, Geburtsnamen, Aliasnamen, verwendete Falschnamen, Geburtsdatum, Geburtsort, Anschrift, Lichtbilder, Grund der Sperre, Dauer der Sperre und meldende Spielhalle.

[3]Daneben dürfen die Dokumente, die zur Sperrung geführt haben, gespeichert werden.
(2) [1]Die gespeicherten Daten sind im erforderlichen Umfang an die Spielhallen zu übermitteln, die die Spielverbote zu überwachen haben. [2]Die Datenübermittlung kann auch durch automatisierte Abrufverfahren erfolgen.
(3) Datenübermittlungen an öffentliche Stellen, insbesondere an Strafverfolgungsbehörden und Gerichte, sind im Rahmen bestehender gesetzlicher Verwendungsregeln zulässig.
(4) Erteilte Auskünfte und Zugriffe im elektronischen System sind zu protokollieren.
(5) Die Daten sind sechs Jahre nach Ablauf der Sperre zu löschen.
(6) Soweit in diesem Gesetz nichts anderes bestimmt ist, sind die jeweiligen Vorschriften für den Schutz personenbezogener Daten anzuwenden, auch wenn die Daten nicht in Dateien verarbeitet oder genutzt werden.
(7) [1]Die für den Betrieb des Sperrsystems zuständige Behörde wird durch die für das Glücksspielwesen zuständige Ministerin oder den hierfür zuständigen Minister im Einvernehmen mit der Ministerin oder dem Minister der Finanzen durch Rechtsverordnung bestimmt. [2]Der zuständigen Behörde kann in der Rechtsverordnung gestattet werden, dritte Personen mit dem Betrieb des Sperrsystems zu beauftragen. [3]In der Rechtsverordnung können Einzelheiten zur Einrichtung und Ausgestaltung des Sperrsystems getroffen werden."

Von Seiten des TMWWDG war beabsichtigt, die Regelung des § 11 SpielhG He in das Thüringer Spielhallengesetz zu übernehmen und mit dem hessischen Innenministerium eine Verwaltungsvereinbarung zur Nutzung der zentralen Sperrdatei des Landes Hessen zu treffen. Zuständige Stelle sollte das Thüringer Landesverwaltungsamt als obere Gewerbebehörde werden.
Der TLfDI teilte als Ergebnis seiner Prüfung mit, dass keine grundsätzlichen Bedenken gegen diese Vorgehensweise bestünden. Als entscheidend sah der TLfDI jedoch die konkrete Umsetzung des Sperrsystems im Thüringer Spielhallengesetz an. Hierzu gab der TLfDI folgende Hinweise:
Die Daten verarbeitende und somit verantwortliche Stelle sollte bestimmt werden. Dies betrifft z. B. die Phase des Erhebens und Speicherns von Daten der zu sperrenden Person in Form der Fremd-

oder Eigensperre. Hier liegt möglicherweise die datenschutzrechtliche Verantwortung beim jeweiligen Spielhallenerlaubnisinhaber.
Für die Führung der Sperrdatei insgesamt, etwa hinsichtlich der erforderlichen Protokollierungen von Abrufen aus der Sperrdatei, das Einrichten von Zugriffsberechtigungen und das Ergreifen der weiteren erforderlichen technischen und organisatorischen Maßnahmen, wäre dann das Thüringer Landesverwaltungsamt als zuständige Stelle verantwortlich.
Hinsichtlich der Übermittlung von in der Sperrdatei gespeicherten Daten sollte nach Auffassung des TLfDI gesetzlich genau bestimmt werden, welche Daten im Einzelnen an die Spielhallen übermittelt werden dürfen. Dies muss bei der Einrichtung eines automatisierten Abrufverfahrens ohnehin vorab festgelegt werden.
Die Einführung der Sperrdatei ist vom TMWWDG noch nicht umgesetzt worden. Es soll demnächst eine Änderung des Glücksspielstaatsvertrages erfolgen, in die die Änderung eingearbeitet wird.

Die Einführung einer Sperrdatei zum Schutz vor Spielsucht im Anschluss an das hessische Sperrdateisystem ist grundsätzlich datenschutzrechtlich zulässig. Die verarbeitende und somit verantwortliche Stelle sollte jedoch konkret bestimmt werden. Für die Führung der Sperrdatei wäre das Thüringer Landesverwaltungsamt als zuständige Stelle verantwortlich. Die zu übermittelnden Daten sind genau zu bestimmen. Personalausweiskopien dürfen nicht zu den Akten genommen werden.



© Fotolia.com – Lehrerin und Grundschüler vor einer Wandtafel

16. Bildung, Jugend und Sport

16.1 Schule online – die Zweite

Bereits in seinem 11. Tätigkeitsbericht für den öffentlichen Bereich wies der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) unter den Nummern 14.2 und 14.33 darauf hin, dass unter seinem Vorsitz an einer Orientierungshilfe für den Einsatz von Online-Lernplattformen an Schulen gearbeitet wird. Damit wollen die Datenschutzbeauftragten der Länder auf die Entwicklung reagieren, dass immer mehr Bildungsinstitutionen auf internetgestützte Vermittlung von Wissen und den elektronischen Kontakt zwischen Lehrern und Schülern setzen.
Aus datenschutzrechtlicher Sicht werden mit dem Verfahren viele personenbezogene Schüler- und Lehrerdaten in aller Regel internetbasiert verarbeitet. Aus diesem Grund soll die Orientierungshilfe als Hilfestellung für die Schulverwaltung und für die Schulen dienen, welche datenschutzrechtlichen Mindestkriterien einzuhalten sind.



Die endgültige Fassung der Orientierungshilfe ist unter https://www.tlfdi.de/mam/tlfdi/gesetze/orientierungshilfen/oh-lernplattformen.pdf auf der Homepage des TLfDI veröffentlicht. Allerdings macht das Wirksamwerden der Europäischen Datenschutz-Grundverordnung (DS-GVO) eine Überarbeitung der Orientierungshilfe erforderlich. Es muss für die Schulen dargelegt werden, welche neuen Anforderungen die Datenschutz-Grundverordnung an die Datenverarbeitung in einer Online-Lernplattform stellt. Dies gestaltet sich deswegen nicht ganz einfach, weil zwar die Datenschutz-Grundverordnung prinzipiell für alle öffentlichen Stellen verbindlich gilt, sie jedoch insbesondere für den öffentlichen Bereich Öffnungsklauseln enthält. Deswegen kommt es auch darauf an, ob und gegebenenfalls welche Regelungen die Länder im Hinblick auf das Datenschutzrecht der Schulen in den Landesschulgesetzen treffen. Zum Abschluss des Berichtszeitraums war die Überarbeitung noch nicht abgeschlossen, da die Entwicklung in den Ländern noch abgewartet werden soll.

Mit dem Wirksamwerden der Datenschutz-Grundverordnung am 25. Mai 2018 stehen alle rechtlichen Regelungen und auch Handreichungen zum Datenschutz, wie beispielsweise Orientierungshilfen, auf dem Prüfstand. Da die DS-GVO für den öffentlichen Bereich Öffnungsklauseln enthält, spielt auch eine Rolle, ob und in welcher Weise der jeweils zuständige Gesetzgeber von ihnen Gebrauch macht.

16.2 KITA-Eintritt: unklare Rechtslage zu Impfschutz-Daten

Durch Anfragen von Kindertagesstätten an das Thüringer Ministerium für Bildung, Jugend und Sport (TMBJS) wurde der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) auf das datenschutzrechtliche Problem des § 34 Abs. 10a Infektionsschutzgesetz (IfSG) aufmerksam gemacht und um Unterstützung gebeten. Diese Regelung wendet sich direkt an die Träger von Kindertageseinrichtungen.

Nach § 34 Abs. 10a des Infektionsschutzgesetzes (IfSG) sind die Personensorgeberechtigten, d. h. in der Regel die Eltern eines Kindes, verpflichtet, bei der Erstaufnahme in eine Kindertageseinrichtung einen Nachweis über eine erfolgte ärztliche Beratung zum Impfschutz des Kindes vorzulegen. Wenn dieser Nachweis nicht erbracht wird, kann das Gesundheitsamt die Eltern zu einer Beratung laden. Somit setzt diese Vorschrift voraus, dass das Gesundheitsamt über eine ladefähige Adresse der Sorgeberechtigten verfügt. Diese Adresse kann nur von den Sorgeberechtigten selbst – was regelmäßig nicht der Fall sein wird, wenn diese offensichtlich keinen Nachweis beibringen wollen – oder durch die Kindertageseinrichtung mitgeteilt werden. Dabei bleibt jedoch die Frage offen, auf welchem Wege das Gesundheitsamt die Adressdaten der Eltern erfahren darf, die keinen Nachweis über eine erfolgte Impfberatung in der Kindertagesstätte vorgelegt haben.

Die Regelung des § 34 Abs. 10a IfSG enthält nach Auffassung des TLfDI keine Ermächtigungsgrundlage zu einer Verarbeitung oder Nutzung personenbezogener Daten, d. h., aus der Regelung ergibt sich keine Zulässigkeit zur Übermittlung von Namen und Adressen der Sorgeberechtigten durch die Kindertagesstätte an das Gesundheitsamt. Dennoch ist in der Bußgeldvorschrift gemäß § 73 Nr. 17a IfSG ausgeführt, dass ein nicht oder nicht rechtzeitig erbrachter Nachweis eine Ordnungswidrigkeit darstellt, die mit einer Geldbuße bis zu zweitausendfünfhundert Euro geahndet werden kann. Somit ist die Vorschrift des § 34 Abs. 10a IfSG nicht eindeutig hinsichtlich ihrer Wirkung und der Verfahrensdurchführung. Ebenso ist nicht klar dargelegt, wieso dem Gesundheitsamt ein Ermessen hinsichtlich der Ladung zu einer Beratung eingeräumt wird („… *kann* das Gesundheitsamt die Personensorgeberechtigten zu einer Beratung einladen“). Hierdurch liefe die o. g. Bußgeldvorschrift ins Leere.

Der Bundesgesetzgeber sieht dies alles aber offensichtlich anders und schreibt in der Gesetzesbegründung zur Einfügung des § 34 Abs. 10a IfSG, Bundestagsdrucksache 18/5261, S. 64, letzter Satz: „Die Kindertageseinrichtung darf dazu das Gesundheitsamt entsprechend informieren.“ Diese Aussage ist erklärungsbedürftig, denn gemäß Art. 6 Abs. 3 der Thüringer Verfassung sind Eingriffe in das Recht auf informationelle Selbstbestimmung nur durch oder auf der Grundlage eindeutiger rechtlicher Regelungen zulässig. Aus diesen Regelungen muss sich ergeben, welche personenbezogenen Daten für welchen Zweck verarbeitet oder genutzt werden. Nach Ansicht

des TLfDI stellt die Regelung des § 34 Abs. 10a IfSG keine Rechtsgrundlage für die Übermittlung der Adressen von betroffenen Sorgeberechtigten durch die Kindertagesstätten an die Gesundheitsämter dar, da diese Rechtsnorm nur den Nachweis über die ärztliche Beratung fordert und das Gesundheitsamt ermächtigt, die Eltern zu einer Beratung einzuladen. Eine Ermächtigung, die Daten der Sorgeberechtigten an das Gesundheitsamt zu übermitteln, ist aus § 34 Abs. 10a IfSG nicht herzuleiten.

Zur Klärung dieses Sachverhalts bat der TLfDI die Bundesbeauftragte für Datenschutz und Informationsfreiheit (BfDI) um eine entsprechende Auskunft und um Mitteilung, ob aus Sicht der BfDI eine Übermittlung der Adressdaten auf der Grundlage der genannten Regelung zulässig ist. Die BfDI bat ihrerseits die Datenschutzbeauftragten der Länder um eine Stellungnahme, ob sie eine Ermächtigungsgrundlage für die Datenübermittlung von Kindertagesstätten an die Gesundheitsämter sehen.

Die Auswertung der Rückmeldungen ergab höchst unterschiedliche Rechtsauffassungen. Allerdings bestand Übereinstimmung darin, dass sich aus der Regelung des § 34 Abs. 10a IfSG keine ausdrückliche Befugnis zur Übermittlung der Daten entnehmen lässt. Der gesetzliche Auftrag ergebe sich nicht aus der Regelung im Abs. 10a selbst, sondern direkt aus § 34 Abs. 10 IfSG. Danach sollen die Gesundheitsämter gemeinsam mit den Gemeinschaftseinrichtungen über den ausreichenden Impfschutz aufklären. Eine Stellungnahme bezog sich ausdrücklich auf die Zulässigkeit von Übermittlungen nach § 64 Abs. 1 SGB VIII, wenn diese dem Kindeswohl dienen. In einem Bundesland wurde diese unklare Rechtslage im Rahmen des entsprechenden Landesgesetzes über Kindertagesstätten geklärt. In diesem Gesetz ist ausdrücklich festgelegt, dass bei der ärztlichen Untersuchung der Impfstatus des Kindes zu erfassen ist und die Eltern entsprechend beraten werden müssen. Schlussendlich ist aus den Stellungnahmen ersichtlich, dass die Landesdatenschutzbeauftragten eine gesetzliche Klarstellung zwingend für geboten halten. Die BfDI wurde deshalb gebeten, gegenüber dem Bundesministerium für Gesundheit darauf hinzuwirken, eine entsprechende Übermittlungsbefugnis im Gesetz normenklar zu verankern. Unabhängig davon wird sich der TLfDI dafür einsetzen, dieses Thema im Arbeitskreis Gesundheit und Soziales der Datenschutzkonferenz zu diskutieren, um hier eine Klärung herbeizuführen.

Der Gesetzgeber hat in der letzten Änderung des IfSG 2017 in § 34 Abs. 10a IfSG die Kindertageseinrichtungen ausdrücklich ermächtigt, den Gesundheitsämtern personenbezogene Daten der Sorgeberechtigten zu übermitteln. Damit gibt es nunmehr eine gesetzliche Übermittlungsbefugnis.

Nach § 34 Abs. 10a Infektionsschutzgesetz (IfSG) sind die Sorgeberechtigten eines Kindes verpflichtet, bei der Erstaufnahme in eine Kindertageseinrichtung die erfolgte ärztliche Beratung zum Impfschutz des Kindes vorzulegen bzw. den Impfschutz des Kindes nachzuweisen. Fehlt dieser Nachweis, kann das Gesundheitsamt die Eltern zu einer Beratung laden. Nach der Änderung des IfSG 2017 stellt die Übermittlung der personenbezogenen Daten der Eltern an das Gesundheitsamt keinen Verstoß gegen datenschutzrechtliche Bestimmungen dar.

16.3 Fotos von KITA-Kindern: brisant!

Im September 2016 wandte sich eine Familie an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und beschwerte sich über die Kindertagesstätte (KITA), die ihr Sohn besuchte. Die Familie legte dar, dass die Erzieher Fotos und Videos der Kinder auf privaten Mobiltelefonen aufnehmen und über soziale Netzwerke, insbesondere WhatsApp, an andere Eltern verschicken würden. Die Familie war damit nicht einverstanden und hatte dementsprechend die Einverständniserklärung der KITA für Foto- und Videoaufnahmen der Kinder nicht unterzeichnet. Dennoch seien Bilder ihres Sohnes weiterhin über die sozialen Netzwerke verbreitet worden. Die Gemeinde, würde nichts dagegen unternehmen, so die Familie, die den TLfDI darum bat, den Sachverhalt datenschutzrechtlich zu prüfen.
Der TLfDI bat zunächst den Träger der KITA, die Verwaltungsgemeinschaft (VG) „Haselgrund“, um eine Stellungnahme zum vorgetragenen Sachverhalt. Die VG trug vor, dass die Kinder während der Betreuungszeiten bei bestimmten Anlässen (Geburtstage, Ausflüge, verschiedene Lernsituationen usw.) durch das Erziehungspersonal fotografiert würden. Geschätzt treffe dies für jedes Kind etwa einmal pro Monat zu. Den Eltern wurde hierfür bei der Aufnahme ihres Kinds in die Einrichtung eine Medienerlaubnis zur Unterzeichnung vorgelegt. Die Erlaubnis beinhaltete die Erstellung von Bildmaterial

zum Gebrauch in der Einrichtung und zur Dokumentation für die Eltern. Die Verbreitung der Fotos über soziale Netzwerke war hingegen von der Erlaubnis nicht erfasst, auch nicht innerhalb einer geschlossenen Gruppe. Nach Angaben der Mitarbeiterinnen der KITA würde die Nichterteilung der Einwilligung jedoch berücksichtigt und die betreffenden Kinder würden bei der Erstellung von Fotos ausgenommen.
Allerdings hatte die VG zwischenzeitlich festgestellt, dass die Aufnahmen nicht nur mit der dienstlichen Digitalkamera, sondern auch mit privaten Mobiltelefonen erstellt wurden. Die Mitarbeiterinnen hätten jedoch versichert, keine Bilder in Facebook oder anderen sozialen Netzwerken einzustellen, mit Ausnahme einer geschlossenen Gruppe im Messenger WhatsApp. Diese Gruppe bestand aus der Erzieherin und den Eltern der jeweiligen Kindergartengruppe. Hier wurden Bilder der Gruppe geteilt, allerdings sei dabei die nicht erteilte Medienerlaubnis der Eltern berücksichtigt worden. Es habe eine „Einwilligungserklärung zur Bildungs- und Entwicklungsdokumentation“, nach der die Erziehungsberechtigten einwilligen können, dass „Fotos/Videoaufnahmen in WhatsApp bzw. in der WhatsApp-Gruppe der KITA-Gruppe veröffentlicht werden, gegeben sowie eine handschriftlich erstellte Liste, die während der Elternabende den Eltern vorgelegt worden sein soll. Diese Liste war als „Einverständniserklärung“ ausgewiesen für Bilder in drei KITA-WhatsApp-Gruppen. Die Liste enthielt die Namen der Erziehungsberechtigten, ja/nein (Zustimmungserklärung), Datum und Unterschrift.
Die VG hatte nach eigenen Angaben erst durch das Schreiben des TLfDI Kenntnis von der praktizierten Nutzung des WhatsApp-Messengers erhalten und daraufhin sofort eine Dienstanweisung in Kraft gesetzt, die die Nutzung privater Kommunikationsmittel und sozialer Netzwerke sowie das Erstellen und Teilen von Bildmaterial in diesen sozialen Netzwerken während der Dienstzeit für das Personal der KITA untersagt. Nach Aussage der VG hatte die KITA-Leitung bereits in Dienstberatungen der Einrichtung darauf hingewiesen, die datenschutzrechtlichen Vorschriften einzuhalten. Daher habe die VG die entsprechenden Pflichtverletzungen disziplinarrechtlich geahndet.
Aufgrund der Darlegungen der VG und der bereits ergriffenen organisatorischen wie dienstrechtlichen Maßnahmen sah der TLfDI von einer Beanstandung der Verstöße ab. Zudem hatte die VG zugesichert, dass die WhatsApp-Gruppen für das Teilen von Bildern der

Kinder und auch der Erwachsenen in der KITA nicht mehr verwendet werden.
Weiterhin teilte der TLfDI der die Beschwerde führenden Familie mit, dass das KITA-Personal nicht flächendeckend verhindern kann, dass Eltern auf dem Gelände der KITA „privat“ Aufnahmen von anderen Kindern erstellen. Hierzu verwies der TLfDI auf einen Beschluss des Landgerichts Frankfurt vom 28. Mai 2015 – 2-3 O 452/14. Danach stellt die bloße Mitgliedschaft einer Person in einer WhatsApp-Gruppe keine schlüssige Einwilligung in die Verbreitung heimlich von ihr erstellter Aufnahmen innerhalb dieser Gruppe dar.
Der TLfDI teilte der Familie, der KITA-Leitung und dem KITA-Träger mit, dass er den Vorgang wieder aufgreift, wenn gegen das zugesicherte datenschutzkonforme Handeln beim Anfertigen von Bildaufnahmen erneut verstoßen wird. Zusätzlich wies der TLfDI den Träger im Hinblick auf die „Einwilligungserklärung“ darauf hin, dass die dienstliche Nutzung von WhatsApp für den Austausch von personenbezogenen Daten grundsätzlich datenschutzrechtlichen Bedenken begegnet.

Fotoaufnahmen von Kindern durch das Personal der KITA mit Einwilligung der Erziehungsberechtigten zur Bildungs- und Entwicklungsdokumentation, sind datenschutzrechtlich zulässig. Kinder, bei denen die Erziehungsberechtigten nicht in das Erstellen von Fotos eingewilligt haben, dürfen jedoch nicht fotografiert werden. Wenn Eltern außerhalb der Verantwortlichkeit der KITA bzw. ohne deren Wissen Aufnahmen anderer Kinder erstellen und in einem Messenger-Dienst teilen, so fällt dies in die Verantwortung der einzelnen Eltern.

16.4 Einsatz von Office 365 an Schulen?

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) wurde ebenso wie auch andere Landesdatenschutzbeauftragte mit Fragen von Schulleitern und Lehrern konfrontiert, ob der schulische Einsatz von Microsoft Office 365 datenschutzrechtlich zulässig ist. Bei dem Produkt handelt es sich um eine Sammlung von Diensten, die z. B. ein Textverarbeitungsprogramm, ein Termin- und E-Mail-Verwaltungsprogramm, ein Präsentationsprogramm usw. sowie als zentrales Angebot eine Webanwendung

„SharePoint“ enthält. Mit dieser Anwendung kann eine gemeinsame virtuelle Plattform mit anderen Nutzern erstellt werden, in der Nachrichten, Kommentare, Texte, Bilder, Videos usw. ausgetauscht und Projekte verwaltet oder Zeitpläne bearbeitet werden. Das Verfahren bietet sich deshalb für die Gestaltung einer zeit- und ortsunabhängigen Online-Lernplattform für einen ergänzenden Schulunterricht an. Die Fairma Microsoft stellt seit mehreren Jahren Schülern und Lehrkräften dieses Online-Verfahren kostenlos zur Verfügung. Voraussetzung hierfür ist, dass der Nutzer sich bei Microsoft unter Nennung seiner Schule registrieren muss. Verständlicherweise entsteht bei den Schulen der Wunsch, dieses Programm für die eigene Schularbeit zu verwenden.

Aus datenschutzrechtlicher Sicht werden mit der Einrichtung sowie bei der Nutzung dieses Produkts personenbezogene Schüler- und Lehrerdaten verarbeitet. Setzt eine Schule Microsoft Office 365 als Lernmittel ein, so ist die Schule als Daten verarbeitende Stelle gemäß § 8 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) für die Einhaltung der Bestimmungen des ThürDSG und anderer Vorschriften über den Datenschutz verantwortlich. Grundsätzlich darf Microsoft als Auftragnehmer die Daten nur im Rahmen der Weisungen der Schule verarbeiten oder nutzen. Da die Schule nur die Möglichkeit hat, dass angebotene Verfahren anzunehmen oder abzulehnen und im weiteren Verlauf keinen Einfluss auf die Datenverarbeitungsprozesse von Microsoft hat, muss das Verfahren der Datenverarbeitung und Nutzung transparent gemacht werden.

Die Datenschützer haben in der Vergangenheit problematisiert, dass Microsoft ein US-amerikanisches Unternehmen ist und deshalb nicht ausgeschlossen werden kann, dass aufgrund des USA PATRIOT Acts US-Sicherheitsbehörden auf Server von US-Unternehmen zugreifen dürfen und auch ausländische Töchter verpflichtet sind, solche Zugriffe auf ihre Server zuzulassen. Microsoft hat zur Vermeidung dieser Problematik eine „deutsche Cloud“ eingerichtet. Den Datenschutzbeauftragten wurde mitgeteilt, dass die personenbezogenen Daten ausschließlich in einem deutschen Rechenzentrum einer deutschen Firma verarbeitet werden, wobei die Firma als Dienstleister und Datentreuhänder tätig wird. Um die Aussagen von Microsoft als auch weitere Aspekte des Office 365-Verfahrens näher zu prüfen, haben die Landesdatenschutzbeauftragten einen Fragenkatalog erarbeitet, der Microsoft mit der Bitte um Beantwortung übergeben wurde. Darüber hinaus führte der TLfDI in seinen Diensträumen eine

Sondersitzung im Rahmen des Unterarbeitskreises Datenschutz und Schule gemeinsam mit Microsoft zum Thema Office 365 durch. Im Zuge der Diskussion kristallisierte sich heraus, dass eine zentrale Koordination der datenschutzrechtlichen Beurteilung sich als hilfreich erweist. Der TLfDI hat hier die Federführung für die Verhandlungen mit Microsoft übernommen, die sich konstruktiv gestalten, aber noch andauern. Daher ist es dem TLfDI nicht möglich, die Anfragen von Schulen und Lehrkräften zum Einsatz von Microsoft Office 365 abschließend zu beantworten.

Schulen dürfen nur Webanwendungen zu Unterrichtszwecken einsetzen, wenn dies aus datenschutzrechtlicher Sicht zulässig ist. Im Regelfall liegt eine Verarbeitung oder Nutzung personenbezogener Daten im Auftrag vor, bei der die Schule nach § 8 Abs. 1 ThürDSG als Auftraggeber für die Einhaltung der datenschutzrechtlichen Bestimmungen verantwortlich bleibt. Die Schule muss sich davon überzeugen, dass der Anbieter von Webanwendungen die erforderlichen technischen und organisatorischen Maßnahmen gemäß § 9 ThürDSG getroffen hat.

16.5 Cloud-Lösung für Schulen – TLfDI mitten drin

Es gibt sie schon, auch an einigen Thüringer Schulen: onlinebasierte Lernplattformen, in denen Schüler und Lehrer außerhalb der Schule miteinander arbeiten. Statt zwischen vier Klassenzimmerwänden wird in virtuellen Räumen gelernt. Lehrer stellen Aufgaben und geeignete Materialien im Netz bereit, Schüler greifen daheim oder sonst irgendwo mit ihrem Laptop darauf zu, laden ihre Arbeitsergebnisse hoch, andere Schüler arbeiten daran weiter, stellen Rückfragen, Lehrer kommentieren und bewerten Schülerleistungen, setzen Termine. Natürlich wird der reale Klassenraum deshalb nicht zugeschlossen. Lernplattformen bilden aber eine sinnvolle Ergänzung für zeitversetztes Lernen in individuellem Tempo. Leider gibt es in Thüringen noch keine landesweit einheitliche Lösung, wie z. B. in Bremen oder Nordrhein-Westfalen. So basteln Schulen notgedrungen an ihren eigenen Lösungen oder sind auf Angebote zukunftsorientierter Schulträger angewiesen, wie z. B. in Jena.
Dass aus solchen Schulclouds keine Arbeitsergebnisse und andere personenbezogenen Informationen auf Abwege in die Untiefen des Internets geraten dürfen, ist im Interesse aller Beteiligten. Datensi-

cherheit und Datenschutz sind also auch hier Gebot der Stunde und damit im Fokus des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Der TLfDI steht im Kontakt zu verschiedenen Akteuren auf diesem Gebiet. So stellte ein Thüringer Institut dem TLfDI die Grundzüge eines zukünftigen „Bildungsservers+“ vor. Mithilfe des Instituts entstanden Kontakte zum „Bündnis für Bildung“ (BfB), dessen Mitglieder aus der IT-Wirtschaft und dem Verlagswesen nach Wegen suchen, digitale Bildungsmaterialien in Schulclouds anzubieten. Gerade hier wird es notwendig sein, genau zu prüfen, ob Schüler- und Elterndaten bis zum Anbieter fließen dürfen, um gezielte Werbeansprachen und Verkaufsvorgänge mit einzelne Personen zu ermöglichen oder ob hier ein daten- und schulrechtliches Veto eingelegt werden muss. In konzeptionellen Gesprächen mit dem BfB berät der TLfDI als Vorsitzender des bundesweiten Arbeitskreises „Datenschutz und Bildung“ die Datenschutzbeauftragten des Bundes und der Länder. Schließlich steht der TLfDI auch mit einem weiteren Institut in Verbindung, um sich über den Entwicklungsstand des Schulcloud-Projektes dieses Institutes zu informieren, das sich als bundesweite Lösung für alle Schulen empfiehlt. Bei allen Gesprächen in dieser Sache machte der TLfDI immer deutlich, dass es zwingend geboten ist, Datenschutz durchgängig als systemimmanente Komponente mitzubedenken und technisch „datendicht“ zu implementieren. Ein System, das bei einer entsprechenden Prüfung durch den TLfDI datenschutzrechtliche Lecks offenbaren würde, wäre in Thüringer Schulen nicht einsetzbar.

Onlinebasierte Lernsysteme, sogenannte Schulclouds, werden mehr und mehr zum schulischen Arbeits- und Kommunikationsmittel auch an Thüringer Schulen. Der TLfDI beobachtet die bundesweite Entwicklung in diesem Bereich und appelliert an die Entwickler, Datenschutzfragen von Anfang an mit zu bedenken. Aktuell steht der TLfDI als Vorsitzender des Arbeitskreises Datenschutz und Bildung in dieser Sache mit verschiedenen nationalen und globalen Playern in Kontakt und kommentiert deren Cloud-Projekte datenschutzrechtlich.

16.6 Evaluation Kurs Medienkunde

Die Eltern von Fünft- bis Zehntklässlern wissen es: Den Rahmen für die Medienbildung ihrer Kinder in der Schule soll der Kurs Medienkunde bilden. Das ist Praxis in Thüringen seit 2001, zunächst für die Klassenstufen 5 bis 7, später inhaltlich aktualisiert und erweitert bis Klassenstufe 10. Thüringen war damals Vorbild deutschlandweit. Andere Bundesländer zogen nach. „Kurs“ bedeutet hier, dass alle Unterrichtsfächer ihren Beitrag zur Medienbildung der Schülerinnen und Schüler leisten sollen. Dieser integrative Ansatz geht von den inhaltlichen Bezugspunkten zur Medienwelt aus, die das jeweilige Unterrichtsfach in sich trägt. Das ist plausibel und gut, erfordert aber eine solide schulinterne Abstimmung und Kontrolle, damit das, was am Ende des Schuljahres im Medienpass des Schülers verbrieft ist, nicht nur auf dem Papier steht. Logisch, dass damit jede Lehrerin und jeder Lehrer medienpädagogisch auf der Höhe der Zeit sein müsste und Verantwortung nicht abschieben kann.
Gut aus Sicht des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) ist auch, dass der verbindliche Kursplan einen Lernbereich vorsieht, der sich mit Recht und Datensicherheit inkl. Datenschutzaspekten beschäftigt. Letzteres gewinnt ja im Big-Data-Zeitalter massiv an Bedeutung – ein Grund mehr für den TLfDI, sich immer wieder kräftig in Medienbildungsfragen einzumischen.
Wie die Umsetzung dieses Kurses an den Thüringer Schulen gelingt, wird seit Frühjahr 2017 auf Veranlassung des Bildungsministeriums evaluiert. Vorausgegangen waren deutliche Impulse des TLfDI, u. a. im Rahmen einer Beratung der interministeriellen Arbeitsgruppe „Stärkung der Medienkompetenz in Thüringen“ im Jahr 2015. Nach seiner Kenntnis aus Gesprächen mit Schülern, Lehrern und Schulleitungen klappt die bisherige Kursumsetzung nicht in allen Schulen. Bei solch einem wichtigen Schlüsselthema wie der Medienkompetenz dürfen Papierform und schulische Realität nicht derart voneinander abweichen.
Die Fakultät für Wirtschaftswissenschaften und Medien der Technischen Universität (TU) Ilmenau ist federführend bei der gegenwärtigen Evaluation des Medienkunde-Kurses. Der TLfDI war von Anfang an als Unterstützer gefragt: Im Januar 2017 begann die Zusammenarbeit mit einem Gespräch über das Evaluationsdesign. Im März bat die TU Ilmenau den TLfDI um Auffassungen zu einem Frageka-

talog an Lehrerinnen und Lehrer. Hierzu hat der TLfDI ausführlich Stellung genommen. Seiner Anregung folgend, wurde ein Fragebogen entwickelt, mit dem die spezielle Sicht der Schulleitungen auf den Kurs Medienkunde erfasst werden soll. Die Befragung von Lehrern und Schulleitungen fand im Frühsommer 2017 onlinegestützt statt. Unter anderem wird auch erfragt, wie die Lehrkräfte zu einem eigenen Unterrichtsfach zur Medienbildung in Ergänzung des fächerintegrativen Kurskonzeptes stehen.

Der Kurs Medienkunde an Thüringer Schulen steht nach Impulsen des TLfDI auf dem Prüfstand. Die Technische Universität Ilmenau evaluiert und wird dabei vom TLfDI aktiv unterstützt. Der TLfDI nahm zu den Inhalten der enthaltenen Lehrerbefragung ausführlich Stellung. Auf seine Anregung hin wurde die Sichtweise von Schulleitungen zur Kursumsetzung an der jeweiligen Schule gesondert erfasst.

16.7 WhatsApp in der Jugendsozialarbeit und Schule?

Ja, es ist so: Nicht allen Kindern und Jugendlichen in unserem Land geht es wirklich gut. Gewalt, Kinderarmut, Alkohol und andere Drogen, Misserfolg in der Schule, Mobbing und häufig das Gefühl, schon in jungen Jahren auf dem Abstellgleis zu sein, prägen ihren Alltag. Solche Probleme zu erkennen und frühzeitig zu mindern ist selbstverständliche Aufgabe unserer humanistischen Gesellschaft. Wenn Eltern überfordert sind, greifen Jugend- und Sozialbehörden ein. Freie Träger der Kinder- und Jugendhilfe und viele engagierte Ehrenamtliche unterstützen. Sie leisten Basisarbeit, sprechen mit den Betroffenen, ggf. den Eltern. Sie suchen gemeinsam mit Jugend- und Sozialämtern nach Hilfsangeboten und sind so selbst schon eins. Klar, dass erstmal Kontakt zwischen Sozialarbeitern, Streetworkern und den Betroffenen hergestellt und möglichst stabil aufrechterhalten werden muss. Das direkte Gespräch ist und bleibt dabei die erste Wahl. Aber reicht das in einer digital geprägten Lebenswelt, die längst bei den Kindern und Jugendlichen voll angekommen ist? Ein Handy ist in der Hand von 98 Prozent der 12- bis 19-Jährigen und die Kommunikation per Chat steht an erster Stelle, wie wir aus der JIM-Studie von 2016 wissen. Chat womit? – Keine Frage, wenn WhatsApp von mehr als 90 Prozent der Jugendlichen genutzt wird. Keine Frage auch, dass sich Sozialarbeit darauf einstellen muss.

Alles wäre kein Problem, wenn das Jugend- bzw. das Sozialamt bei der Nutzung von WhatsApp Herr der Daten bliebe. Davon ist aber nicht auszugehen. Bei blickdichter Software und blickdichten Servern in Übersee kann man trotz Inhaltsverschlüsselung kein Vertrauen aufbauen. Helfer und die Träger kennen die datenschutzrechtlichen Argumente gegen die WhatsApp-Nutzung, auch die Tatsache, dass WhatsApp selbst in seinen Nutzungsbestimmungen eine nichtprivate Nutzung seiner Dienste ausschließt. Aber wie ist der gordische Knoten zwischen Lebensrealität der Zielgruppe und rechtssicherem Handeln der professionellen Helfer zu lösen?
Mit genau dieser Frage wandte sich eine Kinderschutzorganisation an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). WhatsApp ja oder nein? Was geht, was geht nicht? – Sofortlösungen für das Problem, das gleichermaßen für die Kommunikation an unseren Schulen zwischen Lehrern, Schülern, Eltern zutreffen dürfte, kann auch der TLfDI nicht liefern. Grundsätzlich bleibt der begründete Standpunkt des TLfDI, dass WhatsApp und andere Kanäle in sozialen Netzwerken für jegliche dienstliche bzw. geschäftliche Kommunikation datenschutzrechtlich ausscheiden. Die für Schulen relevanten Rechtsgrundlagen (vgl. hierzu § 57 Thüringer Schulgesetz, § 136 Thüringer Schulordnung in Verbindung mit § 9 Thüringer Datenschutzgesetz) sprechen hier eine klare Sprache. Im Jugend- und Sozialbereich sind Inhalte und Metadaten von Chats zwischen Helfern und Schutzbedürftigen als Sozialdaten zu betrachten, für deren Übermittlung § 67d des Sozialgesetzbuchs (SGB) Zehntes Buch (X) Anwendung findet. Für den Transfer von Sozialdaten über/zu WhatsApp, der schon dann stattfindet, wenn die Kontakte ausgelesen werden, besteht keine Übermittlungsbefugnis aufgrund einer Rechtsvorschrift. Nach § 78a SGB X haben Stellen, die Sozialdaten erheben, verarbeiten oder nutzen – hier also das Jugend- bzw. Sozialamt und freie Träger der Jugendhilfe – die entsprechenden technischen und organisatorischen Maßnahmen zu treffen, um die Ausführung des Sozialgesetzbuches einschließlich der Wahrung des Sozialgeheimnisses abzusichern. Da die verantwortlichen Stellen aber auf die Datenverarbeitung durch WhatsApp keinen Einfluss haben, sind auch die Voraussetzungen von § 78a SGB X nicht erfüllt.
Es würde in der Sache nicht helfen, wenn der TLfDI die Beschäftigten im Jugendsozialbereich und die Pädagogen an den Thüringer Schulen mit dieser Aussage allein „im Regen stehen“ ließe. Es gilt,

nach einer praxistauglichen Lösung zu suchen, die sowohl die Lebenswirklichkeit der Beteiligten widerspiegelt, als auch dem rechtlich gesicherten Anspruch der Betroffenen auf Schutz ihrer Privatsphäre entspricht. So wurde in seiner Behörde mit einer Vergleichsanalyse zeitgemäßer und praktikabler Messenger-Lösungen begonnen. Neben der funktionellen Tauglichkeit für typische Dienst-Kommunikationsbedürfnisse der genannten Zielgruppen liegt der Schwerpunkt auf ihrer datenschutzrechtlichen Tauglichkeit. Die Analyse war bei Redaktionsschluss noch nicht abgeschlossen. Im nächsten Tätigkeitsbericht wird über die Ergebnisse informiert.

Sowohl Mitarbeiter von Jugend- und Sozialbehörden, Sozialarbeiter, Streetworker als auch Lehrkräfte möchten moderne Kommunikationsmöglichkeiten wie WhatsApp nutzen, um Kontakte mit Kindern und Jugendlichen aufzubauen und zu pflegen. Die datenschutzrechtliche Problematik dabei ist den meisten Beschäftigten bewusst. Eine Kinderschutzorganisation trug das Problem an den TLfDI heran, der daraufhin eine Vergleichsanalyse möglicher Alternativen zu WhatsApp begann, die sowohl praktikabel als auch datenschutzgerecht sind. Die Analyse ist noch nicht abgeschlossen.

16.8 E-Mail-Nutzung zwischen Lehrern und Schülern

Ein Lehrer wandte sich mit Fragen bezüglich elektronischer Kommunikation an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Genauer wollte er wissen, ob das Schreiben von E-Mails zwischen Lehrern und Schülern als Nutzung von sozialen Netzwerken zähle und ob eine Hausaufgabenverteilung sowie der Versand von selbst erstellten Unterrichtsmaterialien per E-Mail an Schüler datenschutzrechtlich bedenklich wäre. Er erklärte zudem, dass in den E-Mails keine personenbezogenen Daten enthalten seien.

Der TLfDI antwortete, dass der E-Mail-Verkehr nicht zu den sozialen Netzwerken zähle, denn soziale Netzwerke sind virtuelle Gemeinschaften, wo man eine eigene Seite erstellen und den Zugriff auf diese beliebig vielen Personen erlauben kann. In sozialen Netzwerken können zwar auch Nachrichten versandt werden, dies wird jedoch vom TLfDI als problematisch angesehen, da die Daten über die Nutzer von den (außereuropäischen) Anbietern verarbeitet werden und die genauen Datenverarbeitungsprozesse nicht transparent

dargelegt werden. Diese Kommunikationsmöglichkeit darf von öffentlichen Stellen, wie einer staatlichen Schule, nicht genutzt werden. Die E-Mail-Nutzung ist davon nicht betroffen.
Aus datenschutzrechtlicher Sicht ist es zulässig, wenn Schulen mit anderen Personen per E-Mail über allgemeine Sachverhalte, wie zum Beispiel Terminabstimmungen, Einladungen zu Schulveranstaltungen usw., die keine personenbezogenen Daten enthalten, kommunizieren. Beim Versand von personenbezogenen Daten mittels einfacher E-Mail ist allerdings die Vertraulichkeit nicht sichergestellt, dafür müsste eine geeignete Verschlüsselungstechnik zur Verfügung stehen. Lässt eine Schule es zu, dass Lehrkräfte zu dienstlichen Zwecken unverschlüsselt personenbezogene Daten per E-Mail versenden, so trägt die Schule als verantwortliche Stelle im Sinne von § 3 Abs. 5 Thüringer Datenschutzgesetz die Verantwortung für die Datenverarbeitung. Das Versenden von Unterrichtsmaterialien und Hausaufgaben ist aus datenschutzrechtlicher Sicht zwar als unproblematisch anzusehen, wenn darin keine personenbezogenen Daten enthalten sind, dennoch ist zu beachten, dass die E-Mail-Adressen der Empfänger zu den genannten Zwecken freiwillig herausgeben wurden und dass für den Zugriff auf die Unterrichtsmaterialien alternative Wege für diejenigen Schüler angeboten werden, die ihre E-Mail-Adresse nicht bekanntgeben wollen oder keine E-Mail-Adresse besitzen.

Die Kommunikation von Lehrern und Schülern mittels E-Mail ist zulässig, wenn in den E-Mails keine personenbezogenen Daten enthalten sind. Weiterhin ist von den Lehrkräften zu beachten, dass eine E-Mail-Adresse nicht eine Voraussetzung für den Erhalt wichtiger Unterrichtsmaterialien sein kann. Es müssen alternative Zugangsmöglichkeiten für Schüler ohne E-Mail-Adresse oder für diejenigen, die ihre E-Mail-Adresse nicht bekanntgeben wollen, zur Verfügung stehen.

16.9 Schule 2.0 – Schuldatenschutzgesetz notwendig

Das Thüringer Ministerium für Bildung, Jugend und Sport (TMBJS) bat den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) um eine datenschutzrechtliche Stellungnahme zum Entwurf einer Verordnung zur Änderung der Thü-

ringer Schulordnung (ThürSchulO), der Thüringer Schulordnung für das berufliche Gymnasium und der Thüringer Kollegordnung.
Der TLfDI prüfte den Entwurf datenschutzrechtlich und teilte dem TMBJS mit, dass die geänderten und ergänzten Vorschriften keine datenschutzrechtliche Relevanz enthalten und somit auch kein entsprechender Änderungs- oder Ergänzungsbedarf besteht.
Der TLfDI wies jedoch darauf hin, dass der Entwurf leider nicht die Gelegenheit ergreift, auf die technische Entwicklung zu reagieren, die in der Verarbeitung von personenbezogenen Schüler-, Eltern- und Lehrerdaten stattgefunden hat. Dies betreffe insbesondere die Regelungen in § 136 Abs. 9 ThürSchulO. Die durch Lehrer verwendeten Datenverarbeitungsgeräte beschränken sich nicht mehr nur auf den klassischen PC. Dieser wird zunehmend von den Lehrkräften durch Tablets und Smartphones ersetzt. Diese Geräte bieten völlig geänderte Gefahrenpotentiale für die Sicherheit der hiermit verarbeiteten Daten. Der Gesetzgeber ist aufgefordert zu entscheiden, ob solche Geräte überhaupt zur automatisierten Verarbeitung personenbezogener Daten herangezogen werden dürfen und, falls dies der Fall ist, welche konkreten Maßnahmen dann von den Nutzern dieser Technik ergriffen werden müssen. In diesem Zusammenhang wies der TLfDI auch auf die Nutzung von Lehrer-Apps anstelle von klassischen Noten- und Kalenderbüchern hin.
Weiterhin empfahl der TLfDI dem Verordnungsgeber zu regeln, mit welchen technischen Geräten die Daten der Schulverwaltung verarbeitet werden dürfen, also z. B. nur mit Datenverarbeitungsgeräten des Schulträgers. Der TLfDI legte dar, dass in der Praxis immer wieder Unsicherheiten bestehen hinsichtlich der vertraglichen Vereinbarungen über eine Auftragsdatenverarbeitung, beispielsweise bei der Wartung des Schulservers, auf dem Schüler-, Eltern- und Lehrerdaten in der Verantwortung der Schule gespeichert sind, durch den Schulträger oder eine private Firma. Deshalb empfahl der TLfDI, festzulegen, wer als Auftraggeber solche Vereinbarungen abschließen darf.
Weiterhin griff der TLfDI die Regelungen zur Führung von Klassen- und Kursbüchern in § 136 Abs. 4 ThürSchulO auf und legte dar, dass bereits in verschiedenen Thüringer Schulen elektronische Klassenbücher geführt werden. Jedoch sind für die Nutzung von digitalen Klassenbüchern eigene Regeln erforderlich. Beispielsweise muss entschieden werden, ob Klassenbücher parallel in Papierform und in digitaler Form geführt werden dürfen. Ebenso müssen für die schuli-

sche Kommunikation zwischen Eltern bzw. Schülern und Lehrern als auch zwischen Lehrkräften untereinander besondere Regelungen getroffen werden. Stichworte hierbei sind E-Mail-Verkehr, Verschlüsselungsverfahren, Messenger-Dienste, soziale Netzwerke usw. Ein weiteres großes Thema ist die Cloud-Nutzung – der Einsatz von Lernsoftware und die Einrichtung von Online-Lernplattformen durch die Schule. Auch dies sollte geregelt werden.
Nach Ansicht des TLfDI ist zu überlegen, ob die Regelungen dieser Sachverhalte vom Umfang her noch in die ThürSchulO integriert werden können oder ob eine eigene Schuldatenschutzverordnung geschaffen werden sollte. Der TLfDI wies darauf hin, dass einige dieser Problemfelder in anderen Bundesländern bereits gesetzlich geregelt sind. Außerdem sollte geprüft werden, inwieweit eine Überarbeitung der ThürSchulO aufgrund der Regelungen der Datenschutz-Grundverordnung (DS-GVO), die am 25. Mai 2018 wirksam wird, notwendig ist. Im Hinblick darauf bat der TLfDI das TMBJS um eine entsprechende Prüfung und um Mitteilung, inwiefern ein entsprechender Regelungsbedarf gesehen wird und ob entsprechende Vorschriften in die ThürSchulO aufgenommen werden. Eine Antwort liegt bislang noch nicht vor.

Die 2017 geänderten und ergänzten Vorschriften der ThürSchulO enthielten keine datenschutzrechtlich relevanten Regelungen. Aufgrund technischer Neu- und Weiterentwicklungen ist es aus Sicht des TLfDI jedoch erforderlich, insbesondere die Regelungen in § 136 Abs. 9 ThürSchulO zur Nutzung von Datenverarbeitungsgeräten zu ändern und zu aktualisieren. Dies gilt auch für § 136 Abs. 4 ThürSchulO, der die Führung von Klassen- und Kursbüchern regelt. Weiterhin hält der TLfDI aus datenschutzrechtlichen Gründen die Aufnahme von genauen Regelungen zur Nutzung der elektronischen Kommunikation für erforderlich. Aufgrund des Umfangs entsprechender Rechtsnormen könnte eine gesonderte Verordnung zum Schuldatenschutz in Betracht gezogen werden.

16.10 Kultusministerkonferenz macht Medienkompetenz verbindlich

Bereits im Jahr 2012 veröffentlichte die Kultusministerkonferenz (KMK) – hierbei handelt es sich um einen freiwilligen Zusammenschluss der für Kultusfragen zuständigen Minister bzw. Senatoren

der Länder – einen Beschluss zur Medienbildung in der Schule. Hierin war u. a. die verbindliche Festschreibung von Medienbildung in Lehrplänen und in der Lehrerausbildung vorgesehen. Doch der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) gewann trotz dieser Absichtserklärung den Eindruck, dass die Vermittlung von Medienkompetenz durch die Schulen in der Praxis auch nach dem Erscheinen des KMK-Beschlusses nicht mit dem erforderlichen Einsatz betrieben wurde. Wie der TLfDI feststellen musste, war eine Evaluation dieses KMK-Beschlusses weder erfolgt noch geplant und die Verbindlichkeit der in dem Papier aufgeführten Forderungen sehr infrage gestellt. Dies erschien dem TLfDI bedenklich, da die Entwicklung der digitalen Welten in rasanter Geschwindigkeit voranschreitet. Die Schere zwischen der Zunahme des digitalen Fortschritts einerseits und der Vermittlung von Medienkompetenz durch die Schule andererseits droht sich weiter zu öffnen. Die Wirtschaft fördert mit riesigen Anstrengungen die digitale Kommunikationstechnologie, die Schulen halten in der Regel mit dieser Entwicklung nicht Schritt. Beispiel hierfür ist die teilweise schlechte informationstechnische Infrastruktur an den Schulen, die nicht ausreichende Anpassung der Lehrerausbildung an die neuen Gegebenheiten oder anstelle einer Förderung der Medienkompetenz das Festhalten an den bisherigen Lehrplänen. Dabei steht aus der Sicht des Datenschutzes an erster Stelle, sich nicht nur technische Fähigkeiten im Umgang mit den neuen Medien anzueignen, sondern insbesondere auch das Durchblicken dieser Verfahren bezüglich der Frage, wie geht das Verfahren mit meinen personenbezogenen Daten um und welche Möglichkeit habe ich, mich hiervor zu schützen.

Der TLfDI wurde in seiner Eigenschaft als Vorsitzender des Arbeitskreises „Datenschutz und Bildung“ sowie des Unterarbeitskreises „Datenschutz und Schule“ zur Sitzung einer Arbeitsgruppe „Rechtliche und funktionale Rahmenbedingungen“ im Kontext der KMK-Strategie „Bildung in der digitalen Welt“ eingeladen. Ziel der Sitzung war es, den Rohentwurf eines neuen Strategie-Papiers der KMK zu erstellen. Der TLfDI wurde um seine Mitarbeit für den Bereich Informationelle Selbstbestimmung und Datenschutz gebeten. Nachdem dieser die entsprechenden Textpassagen des Entwurfs mit Änderungs- und Ergänzungsvorschlägen überarbeitet hatte, wurde das Papier zur weiteren Abstimmung im Umlaufverfahren mit Zustimmung der KMK auch an die anderen Landesdatenschutzbeauftragten weitergereicht. In mehreren Fachgesprächen der KMK, an

denen auch der TLfDI teilnahm, wurde über die erforderlichen Änderungen des Entwurfspapiers diskutiert und der TLfDI erneut um Stellungnahme zu dem geänderten Text gebeten. Auch dieser Text wurde wiederum im Umlaufverfahren von allen beteiligten Landesdatenschutzbeauftragten mit erforderlichen Änderungen und Ergänzungen versehen und der KMK mit der Bitte um Aufnahme in das endgültige Papier zugeleitet. Der TLfDI lud den Vorsitzenden der KMK-Arbeitsgruppe zur Erstellung des neuen KMK-Strategiepapiers „Bildung in der digitalen Welt“ Ende November 2016 in den Arbeitskreis „Datenschutz und Bildung“ ein, um über den erreichten Stand zu berichten. Im Ergebnis hat die Kultusministerkonferenz am 8. Dezember 2016 ihre Strategie „Bildung in der digitalen Welt“ veröffentlicht. (https://www.kmk.org/aktuelles/thema-2016-bildung-in-der-digitalen-welt.html)

Im neuen Strategiepapier haben die für den Kultusbereich zuständigen Minister verbindlich festgelegt, was sich in Sachen Medienbildung an Schulen und Hochschulen ändern muss. Das Ergebnis der Kooperation zwischen der Kultusministerkonferenz und den Datenschützern des Bundes und der Länder kann sich sehen lassen. Dieses Strategiepapier schlägt jenes von 2012 um Längen. Klar wird definiert, was Schülerinnen und Schüler können müssen, um im Digitalzeitalter zu bestehen. Dabei ist auch ein Kompetenzbereich „Schützen und sicher agieren“, der zum sensiblen Umgang mit Risiken für die Privatsphäre befähigen soll. Kompetenz meint: kennen, bewerten und handeln können. Veränderungen in der Schule brauchen veränderte Lehrer. Folgerichtig sind klare und verbindliche Anforderungen an deren Aus- und Fortbildung formuliert. Hochschulen mit Lehramtsstudiengängen haben hier eine Schlüsselposition. Neben eigener Medienkompetenz heißt das für angehende Lehrer auch, digitale Medien im Fachunterricht sinnvoll nutzen und über Medieninhalte mit den Schülern reflektieren zu können. Es geht alle Lehrer an, denn Medienbildung ist und bleibt Sache aller Unterrichtsfächer. Deshalb sollen Bildungs- und Lehrpläne ausnahmslos auf den Prüfstand und jene Lehrer, die bereits in den Schulen unterrichten, durch zeitgemäße Fortbildungsangebote fit gemacht werden. Die KMK-Strategie ist eine Seite, die andere deren Umsetzung. Sie

muss sportlich angegangen werden, denn bereits ab Schuljahr 2018/19 soll es losgehen in den Klassenstufen 1 und 5. Der betreffende Arbeitskreis der Datenschutzbeauftragten unter Vorsitz des TLfDI hat bereits gegenüber dem KMK-Sekretariat seine Unterstützung bei der Implementation erklärt. Das Angebot des TLfDI gilt selbst verständlich auch für Thüringen – eine entsprechende Kooperation mit den Thüringer Ministerien, der Landesmedienanstalt und dem Lehrerfortbildungsinstitut besteht bereits.

Das neue Strategiepapier der KMK „Bildung in der digitalen Welt“ stellt an alle im Kultusbereich agierenden Akteure klare Anforderungen an die Vermittlung von Medienkompetenz durch die Schulen. Der TLfDI wird das für ihn Mögliche tun, um hierbei seine Unterstützung zu leisten. Gleichzeitig wird der TLfDI die künftige Entwicklung an den Schulen genau beobachten, um da, wo es erforderlich ist, die Einhaltung des Fahrplanes zur Vermittlung von Medienkompetenz in den Schulen zu fordern.

16.11 Datenschutz für junge Lehrer!!!

Wie schon an anderer Stelle mehrfach berichtet, widmet der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) Datenschutzaspekten in der Schule besondere Aufmerksamkeit. Hier werden Weichen gestellt für die Sensibilisierung von Kindern und Jugendlichen für ihr (!) Grundrecht auf informationelle Selbstbestimmung und den Erwerb entsprechender Kompetenzen, z. B. zur Wahrnehmung ihrer Rechte bis hin zum Selbstdatenschutz bei der Nutzung moderner Medien. Dass Lehrer, besonders jene, die am Anfang ihrer Berufslaufbahn stehen, eine Schlüsselrolle bei der Vermittlung einnehmen müssen, versteht sich von selbst. Das sah eine erfahrene Lehrerin, die junge Lehrkräfte im Vorbereitungsdienst am Studienseminar für Regelschulen betreut, ebenso. Am Rande der Veranstaltung vom „Runden Tisch Medienkompetenz“ in Nordhausen (s. dazu Betrag 2.2 Runder Tisch Medienkompetenz) griff sie das Gesprächsangebot des TLfDI auf und es wurde eine erste Veranstaltung vereinbart. Dabei sollten zunächst Datenschutzregelungen, die in der Schule selbst zu beachten sind, thematisiert werden. Schließlich wird es nicht gelingen, Schüler von der Bedeutung des Privatsphärenschutzes zu überzeugen, wenn die Lehrkräfte selbst die datenschutzrechtlichen Bestimmungen im Zusammenhang

mit ihrer täglichen Arbeit nicht kennen. Allein deshalb könnte es zu ungewollten Verstößen kommen.
In der Folgezeit wurden Details vereinbart. Im Studienseminar wurden mit den Lehramtsanwärtern typische Problemfälle aus der Praxis zusammengetragen, die in der Veranstaltung diskutiert werden sollten. Praxisnähe steht verständlicherweise hoch im Kurs bei Lehrern. Fragen wie „WhatsApp in der Kommunikation mit Schülern?“ und „Wofür brauche ich eine Einwilligung der Eltern?“ wurden deshalb ebenso auf die Agenda gesetzt wie: „Darf man Kontaktdaten der Eltern sammeln und die Liste an andere Eltern verteilen?“. In der Veranstaltung stellten der TLfDI und zwei Mitarbeiter die Verbindung zwischen Thüringer Schulgesetz, Thüringer Schulordnung, Thüringer Datenschutzgesetz und diesen schulpraktischen Fragen her und ermöglichten es, dass nunmehr die Lehramtsanwärter viele Antworten selbst geben konnten. In der Diskussion wurde deutlich, dass Recht und tägliche Schulpraxis nicht immer zusammengehen. Wissen, was „Recht“ ist, tut not. Zwei Veranstaltungsstunden sind wenig. Zudem wurden nur Lehramtsanwärter für Regelschulen, nicht aber für die anderen Schularten, erreicht. Das Angebot des TLfDI, diese Veranstaltung als Auftakt für Folgeveranstaltungen zu betrachten, fand Zustimmung bei den Lehramtsanwärtern und dem Lehrkörper des Studienseminars. In der Folge wandte sich das Staatliche Studienseminar für das Lehramt an berufsbildenden Schulen unter Bezugnahme auf abrufbare Vortragsangebote des TLfDI an die Behörde und vereinbarte für Oktober 2017 zwei Veranstaltungen zu Datenschutzfragen für die Lehramtsanwärter dieser Schulart. Dieses Engagement des TLfDI an Studienseminaren reiht sich nahtlos ein in seine Reaktionen auf das Strategiepapier der Kultusministerkonferenz (KMK) zur Medienbildung vom Dezember 2016. Im dem Beschluss der KMK ist im Abschnitt 2.2.1 der klare Anspruch formuliert, dass Lehrende in der Lage sein müssen, „durch ihre Kenntnisse über Urheberrecht, Datenschutz und Datensicherheit sowie Jugendmedienschutz den Unterricht als einen sicheren Raum zu gestalten und die Schülerinnen zu befähigen, bewusst und überlegt mit Medien und eigenen Daten in digitalen Räumen umzugehen …“ (Zitat „Bildung in der digitalen Welt“, Strategie der Kultusministerkonferenz, S. 26, KMK Berlin, 2016). Ein Konzept des TLfDI mit Datenschutz-Themen, die Gegenstand der Zweiten Phase der Lehrerbildung sein sollten, liegt bereits seit Ende 2015 im Thüringer Bildungsministerium.

Der Vermittlung datenschutzrechtlicher Grundlagen und die Sensibilisierung angehender Lehrerinnen und Lehrer für die Wahrnehmung des Grundrechts auf informationelle Selbstbestimmung gehören zweifelsfrei in die Lehrerausbildung. Am Rand eines „Runden Tisches Medienkompetenz“ vereinbarten TLfDI und eine Fachleiterin des Erfurter Studienseminars eine Veranstaltung zum Thema „Datenschutz und Schule“, das sich speziell an Lehramtsanwärter des Studienseminars für Regelschulen richtete. Dabei wurden schulpraktische Probleme aufgegriffen und Tipps für rechtskonformes Handeln in der Schule gegeben. Der TLfDI bot Folgeveranstaltungen an, die auch angenommen wurden.

16.12 Online-Klassenbuch

Moderne Kommunikation zwischen Schule und Eltern gehört mehr und mehr zum Alltag, auch in Thüringen. Da es hierfür leider keine einheitliche landesweite, datenschutzgerechte Lösung für die staatlichen Schulen gibt, auf die die Schulen ohne eingehende Prüfungen vertrauen könnten, suchen diese nach individuellen Lösungen, die natürlich ebenso datenschutzgerecht gestaltet sein müssen. Das macht die Sache für die Schulen als Daten verarbeitende Stellen nicht einfach. Naturgemäß sind bei der Datenverarbeitung in pädagogischem Kontext regelmäßig auch personenbezogene Informationen im Spiel. Heutige Softwarelösungen erlauben beispielsweise, Fachnoten und Fehlzeiten einzelner Schüler aus dem Datenbestand der Schule online abzurufen. Damit ist es Eltern jederzeit möglich, Einsicht zu nehmen. Das, was in der Schule passiert, wird transparenter. Die Frage ist nur, für wen. Klar ist, dass Eltern nur Zugriff auf Informationen über das eigene Kind, Lehrer nur über Schüler ihrer Klassen, Schulleitungen nur über Schüler ihrer Schule haben dürfen. Hier sind technische Weichen zu stellen, damit mitunter sensible personenbezogene Daten nicht auf Abwege geraten können. Nicht von ungefähr sind entsprechende automatisierte Verfahren und Softwareprodukte, die zum Einsatz kommen sollen, zu prüfen und vorab freizugeben. Gemäß § 34 Thüringer Datenschutzgesetz (ThürDSG) fällt diese Aufgabe dem Bildungsministerium bzw. dem jeweiligen staatlichen Schulamt zu.
Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) wurde von einem Elternteil mit einer

besorgten Anfrage kontaktiert, die ein „Online-Klassenbuch“ betrifft. Freilich war sein Zugang durch Anmeldenamen und Passwort geschützt. Seine Vermutung war, dass dennoch Dritte Zugang zu seinen und den persönlichen Daten seines Sohnes hätten. Der TLfDI hat sich daraufhin durch Kontakt mit der Schule und dem Schulamt um Klärung bemüht. Dabei wurde deutlich, dass für das in Rede stehende „Online-Klassenbuch“ bislang kein Eintrag im Verfahrensverzeichnis nach § 10 ThürDSG bestand. Auch eine entsprechende Freigabe durch das Schulamt nach § 34 ThürDSG fehlte. Die Schule besserte auch mit Unterstützung des Softwareherstellers und des Schulträgers entsprechend nach. Der TLfDI prüfte und gab Änderungshinweise, sodass das Schulamt schließlich die notwendige Freigabe des Verfahrens erteilen konnte. Insoweit war der Hinweis des sorgeberechtigten Vaters an den TLfDI hilfreich, um eine rechtskonforme Situation herzustellen. In diesem Zusammenhang wurde auch nachgewiesen, dass der vom Vater vermutete Datenabfluss an Dritte ausgeschlossen werden kann. Besonders über diese Mitteilung des TLfDI war der besorgte Vater verständlicherweise sehr froh.

Die Verarbeitung von Schülerdaten und deren Online-Bereitstellung für Berechtigte setzt entsprechend technisch sichere Verfahren voraus, die vor Freigabe in einem Verfahrensverzeichnis nach § 10 ThürDSG dokumentiert sein müssen. Aufgrund eines Hinweises eines Vaters überprüfte der TLfDI den Fall eines „Online-Klassenbuchs“. Infolgedessen wurde nachgebessert und die datenschutzrechtlichen Anforderungen wurden umgesetzt. Erfreulich: Das eingesetzte Verfahren an sich erwies sich als datenschutzrechtlich unbedenklich.

16.13 Schulserver: geklaut!

Im Februar 2016 informierte der behördliche Datenschutzbeauftragte (bDSB) des Landratsamtes Nordhausen den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) darüber, dass in das Schulgebäude in einer Regelschule eingebrochen und der Schulserver entwendet wurde. Nach Angaben des bDSB hat der Schulserver im abgeschlossenen Sekretariat gestanden. Der oder die Täter hatten in der Nacht eine Schultür und die Tür des Sekretariats aufgebrochen. Außer dem Schulserver waren keine

weiteren Geräte bei dem Einbruch entwendet worden, obwohl materiell wertvolle Geräte im Sekretariat gestanden haben.
Nach Angaben des bDSB war auf dem Server das Schulprogramm Winschool aufgespielt. Dieses Programm enthielt alle Schüler- und Elterndaten, Noten, Zeugnisse sowie die Schulchronik mit Fotos. Nach Information des bDSB war der Server mit einem Passwort geschützt; die Daten hingegen waren nicht verschlüsselt, sodass diese bei Kenntnis des Passwortes ohne besondere Schwierigkeit ausgelesen werden konnten. Für die Schule waren die Daten wiederherstellbar, da täglich Backups erstellt wurden. Aus dem Zeitpunkt des letzten Backups war auf die nächtliche Tatzeit geschlossen worden. Noch vor der eingehenden Prüfung des Sachverhalts empfahl der TLfDI dem bDSB, sofort Kontakt mit der Schulleitung aufzunehmen, damit diese die betroffenen Schüler und Eltern über den Diebstahl informieren kann.
Im Rahmen der Bearbeitung des Sachverhalts stellte der TLfDI fest, dass das Landratsamt als Schulträger den Schulserver und die entsprechende Software für die Schulen im Zuständigkeitsbereich bereitstellt und auch die erforderlichen Wartungsarbeiten durchführt (§ 13 Abs. 2 Thüringer Schulgesetz i. V. m. § 3 Thüringer Schulfinanzierungsgesetz). Die Schule selbst ist jedoch Daten verarbeitende Stelle gemäß § 3 Abs. 5 Thüringer Datenschutzgesetz (ThürDSG) und somit grundsätzlich verantwortlich für einen datenschutzgerechten Umgang mit Schüler-, Eltern- und Lehrerdaten. Beispielsweise erhebt die Schule gemäß § 136 Thüringer Schulordnung zahlreiche Daten der Schüler und der Eltern. Dabei sind personenbezogene Daten, die automatisch verarbeitet werden, durch geeignete Maßnahmen zu sichern. Die Schule ist also im Rahmen ihrer Möglichkeiten für die Einhaltung der datenschutzrechtlichen Bestimmungen verantwortlich. Dementsprechend muss die Schule sich davon überzeugen, dass die vom Landratsamt getroffenen technischen und organisatorischen Maßnahmen eingehalten werden. Im Hinblick darauf legte der TLfDI dar, dass eine Verschlüsselung der auf der Festplatte gespeicherten Daten erforderlich gewesen wäre, um die Vertraulichkeit der auf der Festplatte gespeicherten Daten zu gewährleisten. Nach Auffassung des TLfDI wog die Nicht-Verschlüsselung der Daten umso schwerer als der Server im Sekretariat untergebracht war und nicht in einem extra gesicherten Serverraum.
Der bDSB des Schulträgers informierte den TLfDI darüber, dass für die Schule ein neuer Server angeschafft worden sei. Mit dem neuen

Betriebssystem sei es nun möglich, eine Verschlüsselung mit „BitLocker“ zu aktivieren und zu nutzen.
Daraufhin teilte der TLfDI dem bDSB mit, dass nach § 9 Thüringer Datenschutzgesetz (ThürDSG) alle technischen und organisatorischen Maßnahmen getroffen werden müssen, die erforderlich sind, um die Sicherheit der zu schützenden Daten zu gewährleisten. Im vorliegenden Fall sind dies die personenbezogenen Daten auf dem Schulserver. Dies bedeutet, dass gemäß § 9 Abs. 2 Nr. 1 und 2 ThürDSG nur Befugte personenbezogene Daten zur Kenntnis nehmen können (Vertraulichkeit) und personenbezogene Daten während der Verarbeitung unversehrt, vollständig und aktuell bleiben (Integrität).
Die notwendigen technischen und organisatorischen Maßnahmen sind auf der Grundlage eines Sicherheitskonzeptes zu ermitteln und darzulegen. Im Hinblick darauf wies der TLfDI den bDSB darauf hin, dass mit dem erneuten Aufstellen des Servers im Schulsekretariat kein hinreichend hoher Schutz gegen Einbruch gewährleistet ist.
Die zu treffenden technischen und organisatorischen Maßnahmen müssen sich am Schutzzweck der jeweiligen personenbezogenen Daten orientieren. Server, die personenbezogene Daten von Schülern, Eltern und Lehrern speichern, haben immer „hohen“ Schutzbedarf hinsichtlich der Anwendungen (Programme), der IT-Systeme (Hardware), der Kommunikationsverbindungen und der Räumlichkeiten. Genauere Informationen hierzu bieten die Veröffentlichungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI): https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzSchulung/WebkursITGrundschutz/Schutzbedarfsfeststellung/schutzbedarfsfeststellung_node.html;jsessionid=C31F01A0C90256862837BF4D17C8340E.1_cid091.
Der TLfDI führte aus, dass aufgrund des hohen Schutzbedarfs entsprechende Sicherheitsmaßnahmen für die Aufstellung der IT-Systeme (Server-Hardware) getroffen werden müssen. Sofern kein besonders geschützter Raum für den Server zur Verfügung steht, müssen andere Maßnahmen getroffen werden, die dem Schutzzweck genügen. Beispielhaft benennt der TLfDI einen verschließbaren

Serverschrank, der mit tragenden Gebäudeteilen so verbunden ist, dass selbst der Schrank nur mit großem Aufwand entwendet werden kann. Der TLfDI bat den bDSB um eine Stellungnahme zu den getroffenen Schutzmaßnahmen und um Übersendung der entsprechenden Dokumentation (Auszug aus dem IT-Sicherheitskonzept). Inzwischen hat sich der Landkreis erneut an den TLfDI gewandt und darauf hingewiesen, dass derzeit ein Konzept erarbeitet wird, bei dem die Schulverwaltungssoftware statt auf einzelnen Servern in jeder Schule in einer zentralisierten Serverumgebung für alle Schulen des Landkreises betrieben werden soll. Alle Schulen sollen über gesicherte Verbindungen auf ihre dort verarbeiteten Daten zugreifen können. Nach Fertigstellung des Konzepts wird der TLfDI dieses aus datenschutzrechtlicher Sicht prüfen und darüber berichten.

Nach § 9 Thüringer Datenschutzgesetz (ThürDSG) müssen alle technischen und organisatorischen Maßnahmen getroffen werden, die erforderlich sind, um die Sicherheit der zu schützenden Daten zu gewährleisten. Dies bedeutet, dass gemäß § 9 Abs. 2 Nr. 1 und 2 ThürDSG nur Befugte personenbezogene Daten zur Kenntnis nehmen können (Vertraulichkeit) und personenbezogene Daten während der Verarbeitung unversehrt, vollständig und aktuell bleiben (Integrität). Diese Bestimmungen gelten auch für personenbezogene Daten auf dem Schulserver. Diese Daten unterliegen einem hohen Schutzbedarf; sie müssen verschlüsselt werden und für die Aufstellung des Schulservers sind besondere Schutzmaßnahmen zu treffen.

16.14 Schulnoten für kommunale Sozialplanung – nur anonymisiert

Im November 2015 wandte sich das Landratsamt Unstrut-Hainich-Kreis an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und bat um die datenschutzrechtliche Bewertung einer statistischen Erfassung der Schülerübertritte von der Grundschule auf das Gymnasium und der Nichtübertritte trotz bestehender Notenvoraussetzung.
Das Landratsamt hatte im Sommer 2015 alle staatlichen und freien Grund- und Gemeinschaftsschulen des Landkreises angeschrieben und um Auskünfte der sozial- und planungsraumbezogenen individuellen Lebenslagen von Schülerinnen und Schülern gebeten. Ebenso hatte das Landratsamt alle freien Schulen um entsprechende Aus-

künfte gebeten. Das Landratsamt legte dar, diese Auskünfte als Grundlage zu benötigen, um raum- und zielgruppenspezifische soziale Maßnahmen beispielsweise in der Jugendhilfe anzubieten. Diesen Zweck und den entsprechenden Umgang mit dem Datenmaterial hatte das Landratsamt auch im Anschreiben an die Schulen erläutert.
Im Hinblick auf die sozial- und planungsraumbezogene Schülererfassung hatte eine Schule jedoch Bedenken zur Individualisierung der Daten geäußert und das Landratsamt gebeten, die Zulässigkeit des Auskunftsersuchens vom TLfDI bewerten zu lassen.
Der TLfDI prüfte den Sachverhalt datenschutzrechtlich und gelangte zu folgender Bewertung: Die geplante Bestandsaufnahme von Schülerinnen und Schülern in der vorgelegten Form stellt eine Erhebung personenbezogener Daten dar, die nach § 4 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) einer Rechtsgrundlage oder der Einwilligung der betroffenen Schüler (bzw. der gesetzlichen Vertreter) bedarf. Da weder eine Rechtsgrundlage noch eine Einwilligung der Betroffenen vorlag, war die geplante Erhebung nur in anonymisierter Form zulässig. Daraus ergibt sich, dass das Landratsamt die Grundschulen bei bestehenden Bedenken wegen fehlender Anonymisierung der Daten nicht zur Teilnahme an dem Erhebungsverfahren verpflichten kann.
Gemäß § 3 Abs. 9 ThürDSG ist Anonymisieren „das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.“ Das bedeutet, wenn eine Bestimmung von Personen dadurch möglich ist, dass innerhalb des gesamten Datenbestands der betroffenen Schülerinnen und Schüler eine bestimmte Merkmalsausprägung nur bei einem Schulkind vorliegt, dann müssen diese Angaben gelöscht oder durch allgemeiner gehaltene Aussagen ersetzt werden (vgl. Dammann, in: Simitis- BDSG, 7. Aufl., zu § 3, Rdnr. 207). Dies wäre beispielsweise der Fall, wenn es in einer Schule oder in einem bestimmten Planungsraum nur ein Kind gibt mit einer bestimmten erfragten Konstellation. Um eine solche Konstellation zu vermeiden, könnten beispielsweise Grundschulen in freier und in kirchlicher Trägerschaft als nicht-staatliche Grundschulen zusammengefasst werden. Ebenso könnten zwei Planungsräume

zusammengelegt und somit die Daten aggregiert und damit anonymisiert werden.
Der TLfDI teilte dem Landratsamt des Unstrut-Hainich-Kreises mit, dass das Auskunftsersuchen zum Zweck der kommunalen Sozialplanung zulässig ist, sofern die empfohlene Art der anonymisierten Durchführung beachtet wird.

Die Erhebung von Schulnoten zur kommunalen Sozialplanung ist nur in anonymisierter Form gemäß § 3 Abs. 9 Thüringer Datenschutzgesetz zulässig. Das heißt, personenbezogene Daten und Angaben über persönliche oder sachliche Verhältnisse müssen derart geändert werden, dass eine Zuordnung zu einer bestimmten Person nicht möglich ist.

16.15 Notenspiegel in Facebook: mangelhaft!

Im Dezember 2015 beschwerte sich eine Familie aus dem Saale-Holzland-Kreis beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) über eine Lehrerin der Regelschule Stadtroda. Der Vorwurf lautete, dass die Lehrerin personenbezogene Daten der Schülerin über das soziale Netzwerk Facebook kommuniziert und damit das Persönlichkeitsrecht der Schülerin verletzt habe. Die Lehrerin habe sich auf Facebook mit anderen Schülern über die schulischen Leistungen der betroffenen Schülerin ausgetauscht. Hintergrund für den Austausch war die Anfrage einer Mitschülerin, wieso bei einer gemeinsam erledigten Arbeit eine Schülerin mit Note 4, die andere Schülerin jedoch mit Note 6 bewertet worden sei. Die Familie übergab dem TLfDI eine Kopie der betreffenden Facebook-Korrespondenz.
Da die Lehrerin in ihrer Funktion als Lehrkraft einer staatlichen Schule handelte, muss ihr Handeln den Vorgaben des Thüringer Schulgesetzes und des Thüringer Datenschutzgesetzes (ThürDSG) entsprechen. Die Veröffentlichung von Leistungen von Schülern im Internet – und um eine solche handelt es sich bei diesem Chat, in dem Noten genannt wurden – stellt eine Übermittlung von personenbezogenen Daten an nicht-öffentliche Stellen dar. Jeder, dem die Einstellungen auf der Facebook-Seite dies erlauben, erfährt die Noten der Schüler und die Stellungnahme der Lehrerin dazu.
Die Übermittlung personenbezogener Daten muss zunächst datenschutzrechtlich die Anforderungen des § 9 ThürDSG erfüllen. Da-

nach haben die öffentlichen Stellen die notwendigen technischen und organisatorischen Maßnahmen zu treffen, um die Ausführungen der Datenschutzbestimmungen zu gewährleisten. Dazu zählen insbesondere die Vertraulichkeit der übermittelten personenbezogenen Daten und die Transparenz des genutzten Verfahrens. Viele soziale Netzwerke können diese Kriterien jedoch nicht erfüllen. Bei Facebook ist davon auszugehen, dass die Daten nicht unter der alleinigen Kontrolle der Schule verarbeitet werden. Die Schulen können nicht garantieren, dass Inhaltsdaten von Lehrern und Schülern vertraulich bleiben. Daher bewertet der TLfDI jegliche dienstliche Kommunikation über solche sozialen Netzwerke zwischen Lehrkräften sowie zwischen Lehrkräften und Schülern als Verstoß gegen § 9 ThürDSG.

Hinzu kommt, dass gemäß § 57 Abs. 4 Thüringer Schulgesetz eine Übermittlung personenbezogener Schülerdaten an Dritte nur unter den dort genannten Voraussetzungen zulässig ist, die allesamt nicht vorlagen. Die Übermittlung einer Schulnote einschließlich einer entsprechenden Begründung über eine Schülerin an eine andere Schülerin stellt eine Übermittlung von personenbezogenen Daten an eine dritte Person dar, die weder für die Aufgabenerfüllung der Schule erforderlich war, noch im rechtlichen Interesse der dritten Person unerlässlich war. Eine rechtswirksame Einwilligung der betroffenen Schülerin lag ebenfalls nicht vor.

Daher war die Lehrerin nicht befugt, über eine Note und deren Hintergründe einer anderen Schülerin via Facebook Auskunft zu erteilen. Dies teilte der TLfDI im Januar 2016 der Regelschule mit und bewertete das Verhalten der Lehrerin als eine „nicht unerhebliche Verletzung von Vorschriften über den Datenschutz, die gemäß § 39 Abs. 1 ThürDSG beanstandet wird“.

Der TLfDI forderte das Schulamt auf zu klären, warum die Lehrerin über Facebook sowohl mit der betroffenen Schülerin als auch mit Dritten korrespondiert hat. Weiterhin forderte der TLfDI, die entsprechende Unterhaltung umgehend aus dem Facebook-Account zu löschen und das Lehrerkollegium darüber zu informieren, dass es unzulässig ist, zu dienstlichen Zwecken über private Netzwerke im Internet mit Schülern und Lehrern zu kommunizieren.

Der TLfDI forderte die betreffende Regelschule mehrmals zur Stellungnahme zum Vorgang auf; die Regelschule reagierte jedoch nicht auf diese Schreiben. Daher sprach der TLfDI eine erneute Beanstandung aus und wandte sich auf der Grundlage des § 39 Abs. 2 ThürDSG an das zuständige Schulamt Ostthüringen. Als Aufsichts-

behörde ist das Schulamt nach § 34 ThürDSG dafür zuständig, die Einhaltung des Datenschutzes im nachgeordneten Schulbereich sicherzustellen und entsprechend geeignete Maßnahmen gegen die Regelschule zu ergreifen.
Das staatliche Schulamt Ostthüringen bestätigte den Vorfall als zutreffend und erklärte, dass die betroffene Lehrerin angewiesen wurde, in Zukunft die Nutzung von Facebook zur schulischen Kommunikation zu unterlassen. Ebenso wurde das Lehrerkollegium umfassend über die Einhaltung der datenschutzrechtlichen Vorschriften informiert. Der TLfDI bat das Schulamt nochmals darum, alle Schulen im Aufsichtsbereich ausdrücklich darauf hinzuweisen, dass weder soziale Netzwerke wie Facebook, noch Messenger-Dienste für die dienstliche Kommunikation eingesetzt werden dürfen.
Gemeinsam mit dem Thüringer Ministerium für Bildung, Jugend und Sport hat der TLfDI die „Orientierungshilfe Lernplattformen“ für die Thüringer Schulen Anfang 2016 nutzerfreundlich aufbereitet. Weiterhin hat der TLfDI für die Datenschutzbeauftragten der staatlichen Schulämter und das Thüringer Institut für Lehrerfortbildung, Lehrplanentwicklung und Medien eine Informationsveranstaltung zu den datenschutzrechtlichen Problemen bei der Nutzung von sozialen Netzwerken und Messenger-Diensten im schulischen Kontext durchgeführt. Er plant nun gemeinsam mit diesen Stellen einen Leitfaden für Lehrer herauszugeben.

Gemäß § 9 ThürDSG muss die Übermittlung personenbezogener Daten vertraulich erfolgen und das genutzte Verfahren muss transparent sein. Diese Kriterien können jedoch soziale Netzwerke in der Regel nicht erfüllen. Für den Schulbereich bedeutet dies, dass persönliche Daten von Lehrern und Schülern nur unter der alleinigen Kontrolle der Schule verarbeitet werden dürfen. Daher dürfen soziale Netzwerke oder Messenger-Dienste nicht für die dienstliche Kommunikation in Schulen eingesetzt werden.

16.16 Jeder muss wissen, wenn der Kollege krank ist ... oder doch nicht?

Im Januar 2016 beschwerte sich eine Erzieherin einer Grundschule darüber, dass eine Kollegin die Beschwerdeführerin betreffende personenbezogene Gesundheitsdaten (Krankschreibung, Krankentage) an Kollegen des Lehrkörpers weitergegeben habe. Die Erzieherin

hatte sich zunächst an den Schulträger gewandt, das Landratsamt Weimarer Land (LRA WE-Land), und sich dort über die Indiskretion ihrer Kollegin beschwert. Das Landratsamt habe jedoch nichts weiter unternommen, sodass sich die Beschwerdeführerin schließlich mit der Bitte um Prüfung des Sachverhalts an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) wandte.

Der TLfDI teilte der Beschwerdeführerin zunächst mit, dass der vorgetragene Sachverhalt aus datenschutzrechtlicher Sicht eine unzulässige Nutzung ihrer personenbezogenen Daten darstellt. Da es sich um Gesundheitsdaten handelte, waren diese Daten außerdem als besonders geschützt anzusehen. Der TLfDI wies darauf hin, dass eine Arbeitsunfähigkeitsbescheinigung keine Diagnosemitteilung enthalte. Aus ihr seien lediglich die Tatsache der Arbeitsunfähigkeit, deren voraussichtliche Dauer sowie der Stempel des Arztes zu entnehmen. Dennoch sind auch diese Daten gemäß § 20 Abs. 2 Thüringer Datenschutzgesetz (ThürDSG) nur den Personen mitzuteilen, die sie zur Erledigung ihrer Aufgaben benötigen. In diesem Rahmen dürfen die zuständigen Mitarbeiter/innen weder die Daten auf der Arbeitsunfähigkeitsbescheinigung, noch weitere Daten aus möglichem Zusatzwissen (z. B.: zur Krankheitsdiagnose) an Dritte übermitteln. Damit würden sie das Datengeheimnis nach § 6 ThürDSG verletzen. Die Beschwerdeführerin hätte bei der Abgabe entsprechender Bescheinigungen auch den hierfür festgelegten Dienstweg einhalten müssen.

Darüber hinaus informierte der TLfDI die Beschwerdeführerin darüber, dass das Schulverwaltungsamt des LRA-WE-Land nicht für ihre Beschwerde zuständig war. Der Landkreis Weimarer Land ist Schulträger, d. h. er stellt das Schulgebäude, die technische Ausrüstung der Schule sowie das Verwaltungs- und Hauspersonal (Haustechniker, Sekretariat) zur Verfügung bzw. finanziert diese. Alle Lehrkräfte hingegen sind Landespersonal. Die Schulaufsicht wird von dem für das Schulwesen zuständigen Ministerium als oberster Schulaufsichtsbehörde und von den Staatlichen Schulämtern als unteren Schulaufsichtsbehörden sowie den Staatlichen Studienseminaren für Lehrerausbildung ausgeübt (§ 4 Abs. 1 Thüringer Gesetz über die Schulaufsicht (ThürSchAG)). Dabei obliegt den unteren Schulaufsichtsbehörden nach § 4 Abs. 3 ThürSchAG in ihrem Zuständigkeitsbereich die Fachaufsicht über die Schulen sowie die Dienstaufsicht über die Schulleiter, Lehrer, Fachleiter, Lehramtsan-

wärter, Sonderpädagogischen Fachkräfte und Erzieher. Für die staatliche Grundschule ist das Schulamt Mittelthüringen die zuständige Schulaufsichtsbehörde. Sofern die Kollegin, die die Daten weitergegeben hat, Mitarbeiterin der Schule war, obliegt dem Landratsamt die Dienstaufsicht. Zusätzlich ist der Schulleiter in Erfüllung eines geordneten Schulbetriebs und Unterrichts auch dem Verwaltungs- und Hauspersonal gegenüber weisungsberechtigt (§ 33 Abs. 1 Thüringer Schulgesetz). Nachfolgend bat der TLfDI die Grundschule um eine Stellungnahme zum Sachverhalt. Da die Kollegin, die die Daten weitergegeben haben soll, Mitarbeiterin des Landratsamtes war, übersandte die Schulleiterin ihre Stellungnahme zunächst an das Schulverwaltungsamt im Landratsamt. Sie legte dar, dass die betreffende Kollegin keinerlei Daten aus der Arbeitsunfähigkeitsbescheinigung der Beschwerdeführerin an das Lehrerkollegium weitergegeben hätte. Ebenso habe die Kollegin keine weiteren Daten aus möglichem privaten Zusatzwissen (beispielsweise zur Krankheitsdiagnose oder zum Hintergrund der Krankschreibung) weitergegeben. Darüber hinaus sei in der Grundschule geregelt, dass Krankenscheine innerhalb von drei Tagen im Sekretariat abzugeben sind, die Sekretärin hierüber Buch führt und eine Unterbrechungsanzeige ausstellt, die an die Zentrale Gehaltsstelle weitergeleitet werde.
Aufgrund der Ausführungen der Schulleiterin konnte der TLfDI nicht feststellen, ob bzw. dass die betreffende Kollegin Teile des Lehrerkollegiums über die Krankschreibung der Beschwerdeführerin informiert hatte oder nicht. Insofern konnte der TLfDI auch keinen datenschutzrechtlichen Verstoß zweifelsfrei erkennen und teilte dies der Beschwerdeführerin mit. Für den Fall, dass die Beschwerdeführerin eine weitere Bearbeitung ihrer Beschwerde wünschte, führte der TLfDI aus, dass er hierfür zusätzliche Unterlagen oder Angaben derjenigen Kolleginnen und Kollegen des Lehrerkollegiums benötigte, die ihre Sachverhaltsdarstellung stützten. Weiterhin informierte der TLfDI die Grundschule und wies vorsorglich auf das bestehende Datengeheimnis hin, das insbesondere bei der Entgegennahme und Bearbeitung von Krankmeldungen im Sekretariat besteht. Ebenso setzte der TLfDI das Landratsamt darüber in Kenntnis, dass er aus den vorgetragenen Informationen kein Fehlverhalten der Kollegin feststellen konnte, gegen die sich die Beschwerde richtete, und der Vorgang insofern erledigt sei. Der TLfDI wies jedoch auch darauf hin, dass der Vorgang erneut aufgegriffen werden müsse, wenn die Beschwerdeführerin Unterlagen vorlegte, die ihre Darstellung stütz-

ten, beispielsweise entsprechende Bestätigungen von anderen Lehrkräften oder den Erziehern.

Gesundheitsdaten sind als personenbezogene Daten besonders geschützt. Hierzu zählen auch ärztliche Bescheinigungen über die Arbeitsunfähigkeit, einschließlich der darin angegebenen Krankheitstage. Diese Daten dürfen nur den Personen mitgeteilt werden, die sie zur Erledigung ihrer Aufgaben benötigen (§ 20 Abs. 2 Thüringer Datenschutzgesetz) In diesem Zusammenhang dürfen auch keine weiteren Daten aus möglichem privaten Zusatzwissen (beispielsweise zur Krankheitsdiagnose oder zum Hintergrund der Krankschreibung) an andere Personen weitergegeben werden, da dies nicht zuletzt einen unzulässigen Eingriff in das Recht auf informationelle Selbstbestimmung und das allgemeine Persönlichkeitsrecht darstellt (Art. 2 Abs. 1 Grundgesetz [GG] in Verbindung mit Art. 1 Abs. 1 GG).

16.17 Lehrergespräche über schulische Leistungen: keine gute Leistung

Im September 2015 wandte sich die Mutter eines Schülers einer staatlichen Grundschule an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Sie beschwerte sich darüber, dass die Klassenlehrerin andere Personen über gemeinsam geführte Gespräche, die schulischen Leistungen ihres Sohnes betreffend, informiert habe. Die Klassenlehrerin sei zwischenzeitlich in Rente gegangen. Jedoch habe die Beschwerdeführerin einen Brief ihrer ehemaligen Schwägerin erhalten, die ebenfalls Lehrerin an der Grundschule war. Dieser Brief enthielt die gleichen, bereits von der im Ruhestand befindlichen Grundschullehrerin erhobenen Vorwürfe gegen die Beschwerdeführerin im Hinblick auf die erzieherische Einwirkung auf ihren Sohn. Daher bat die Mutter den TLfDI, den Sachverhalt zu prüfen und dafür zu sorgen, dass das Lehrpersonal der Schule das bestehende Datengeheimnis einhält.
Gemäß § 57 Abs. 1 Thüringer Schulgesetz (ThürSchulG) sind das Verarbeiten und Nutzen personenbezogener Daten der Schüler, der Eltern und der Lehrer nur zur Aufgabenerfüllung der Schulen zulässig. Eine Übermittlung personenbezogener Daten der Schule an Dritte ist nur unter den in § 57 Abs. 4 Nr. 1 bis 4 ThürSchulG aufgeführten Voraussetzungen zulässig. Darüber hinaus ist es nach § 6

Thüringer Datenschutzgesetz (ThürDSG) „den bei Daten verarbeitenden Stellen beschäftigten Personen […] untersagt, personenbezogene Daten unbefugt zu verarbeiten oder zu nutzen (Datengeheimnis). Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort." Diese Bestimmungen gelten auch für Schulen und deren Lehr- wie Mitarbeiterpersonal. Der TLfDI bat die Leitung der Grundschule zunächst um eine Stellungnahme zum vorgetragenen Sachverhalt. Die Schulleiterin legte dar, dass zu keiner Zeit ein Gespräch allein zwischen den beiden o. g. Lehrerinnen über schulische Angelegenheiten des Sohnes der Beschwerdeführerin stattgefunden habe. Jedoch habe ein Gespräch zwischen der Schulleiterin und dem Kindesvater stattgefunden, bei dem dessen Schwester (die ehemalige Schwägerin der Beschwerdeführerin) ebenfalls anwesend war. Hierbei sei es nicht um die schulischen Leistungen und das Unterrichtsverhalten des Sohnes gegangen, sondern um die Betreuungsregelung des Kindes, da die Eltern getrennt leben. Die Schulleiterin gab an, keinen Einfluss darauf zu haben, welche Informationen der Kindesvater an seine Schwester familienintern weitergebe.

Weitere Nachfragen zum Sachverhalt des TLfDI wurden von der Grundschulleitung wiederholt nicht beantwortet. Daher sprach der TLfDI gegenüber der Grundschule eine Beanstandung aus wegen des Verstoßes gegen die Unterstützungspflicht gemäß § 39 Abs. 1 ThürDSG.

In der Folge übersandten die Schulleitung sowie die zuständige Aufsichtsbehörde ergänzende Stellungnahmen an den TLfDI. Darin legte die Schulleiterin dar, dass sie nicht wissen könne, ob oder welche „Freizeitgespräche" es möglicherweise zwischen den beiden Lehrerinnen gegeben habe. Die Schulleiterin habe mehrfach aktenkundig Belehrungen zur dienstlichen Verschwiegenheit durchgeführt und die Klassenlehrerein habe entsprechend gehandelt. Da sie sich mittlerweile jedoch im Ruhestand befinde, bat die Schulleiterin den TLfDI, weitere Fragen mit ihr persönlich zu klären.

Das zuständige staatliche Schulamt legte ebenfalls schriftlich dar, dass eine ordnungsgemäß durchgeführte Belehrung zur Verschwiegenheit gemäß § 37 Gesetz zur Regelung des Statusrechts der Beamtinnen und Beamten (Beamtenstatusgesetz) erfolgt war. Über mögliche Gespräche zwischen den beiden Lehrerinnen könne keine Aussage getroffen werden. Man schlug dem TLfDI deshalb vor, sich zur weiteren Aufklärung des Sachverhalts an die im Ruhestand befindliche Lehrerin persönlich zu wenden. Hierfür besitzt der TLfDI jedoch

nicht die datenschutzrechtliche Kontrollkompetenz. Nach § 37 Abs. 1 ThürDSG unterliegt nur die öffentliche Stelle der Kontrolle des TLfDI. Einzelnes Lehrpersonal unterliegt nach § 4 Abs. 3 Thüringer Gesetz über die Schulaufsicht der Dienstaufsicht durch die staatlichen Schulämter. Dies gilt auch für Lehrpersonal, das sich bereits im Ruhestand befindet.
Wenn eine Lehrkraft unbefugt personenbezogene Daten, die nicht offenkundig sind, übermittelt, so liegt hierin eine Ordnungswidrigkeit nach § 43 Abs. 1 Nr. 1 ThürDSG. Von der Dienstaufsichtsbehörde wird diese Ordnungswidrigkeit nur auf Antrag verfolgt. Hierfür sind der Betroffene und der TLfDI antragsberechtigt.
Im Ergebnis konnte der TLfDI nicht zweifelsfrei davon ausgehen, dass die Klassenlehrerin personenbezogene Daten des Sohnes der Beschwerdeführerin an Dritte übermittelt hat. Dennoch informierte der TLfDI das Staatliche Schulamt darüber, dass auch Lehrpersonal im Ruhestand gemäß § 2 Abs. 2 Nr. 5 i. V. m. § 4 Abs. 3 Thüringer Gesetz über die Schulaufsicht der Dienstaufsicht durch die staatlichen Schulämter unterliegt. Daher kann das Schulamt im Rahmen seiner Dienstaufsicht die im Ruhestand befindliche Klassenlehrerin zum Sachverhalt befragen, um zu klären, ob sie die ihr obliegenden Pflichte schuldhaft verletzt hat.
Der TLfDI wies die Beschwerdeführerin auf § 36 Abs. 1 Nr. 2 Buchstabe a Ordnungswidrigkeitengesetz in Verbindung mit § 43 Abs. 3 Satz 2 und 3 ThürDSG hin, wonach sie die Möglichkeit hat, beim zuständigen Thüringer Ministerium für Bildung, Jugend und Sport (TMBJS) zu beantragen, dass die Tat als Ordnungswidrigkeit verfolgt wird. Voraussetzung für die Verfolgung ist, dass das TMBJS vom Verdacht einer unbefugten Übermittlung von nicht offenkundigen Daten des Sohnes ausgeht. Weiterhin forderte der TLfDI die Schulleitung auf, erneut eine datenschutzrechtliche Belehrung im Lehrerkollegium durchzuführen und dabei ausdrücklich darauf hinzuweisen, dass es untersagt ist, dienstlich erlangtes Wissen über personenbezogene Daten auch außerhalb der Schule oder im privaten Rahmen unbefugt zu verarbeiten oder zu nutzen. Dies haben auch Lehrkräfte zu beachten, die sich bereits im Ruhestand befinden.

Nach § 37 Gesetz zur Regelung des Statusrechts der Beamtinnen und Beamten (BeamtStG) haben Lehrerinnen und Lehrer über die ihnen im Rahmen ihrer amtlichen Tätigkeit bekannt gewordenen dienstlichen Angelegenheiten Verschwiegenheit zu bewahren. Diese Rege-

lungen sind für Tarifbeschäftigte analog anwendbar. Weiterhin ist es gemäß § 6 Thüringer Datenschutzgesetz (ThürDSG) den bei Daten verarbeitenden Stellen beschäftigten Personen untersagt, personenbezogene Daten unbefugt zu verarbeiten oder zu nutzen (Datengeheimnis). Das Datengeheimnis besteht auch nach Beendigung der Tätigkeit fort.

16.18 Datenschutz in der Thüringer Schulgesetzgebung

Das Thüringer Ministerium für Bildung, Jugend und Sport (TMBJS) bat den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) um eine Stellungnahme zum Gesetzentwurf zur Änderung des Thüringer Schulgesetzes (ThürSchulG) und des Thüringer Schulfinanzierungsgesetzes (ThürSchFG).
Nach rechtlicher Prüfung teilte der TLfDI dem TMBJS mit, dass aus datenschutzrechtlicher Sicht gegen den Gesetzentwurf keine Bedenken bestehen. Im Zusammenhang mit seiner Stellungnahme nahm der TLfDI jedoch die Gelegenheit war, dass TMBJS darauf aufmerksam zu machen, dass im Umgang mit personenbezogenen Daten von Schülern, Eltern und Lehrern Änderungs- und Ergänzungsbedarf im Thüringer Schulgesetz, im Thüringer Schulfinanzierungsgesetz und in weiteren schulgesetzlichen Bestimmungen besteht.
Den datenschutzrechtlichen Änderungsbedarf in der Thüringer Schulgesetzgebung legte der TLfDI gegenüber dem TMBJS folgendermaßen dar:
Im ThürSchulG sollte die Schule ausdrücklich als Daten verarbeitende und somit verantwortliche Stelle bestimmt werden. Im ThürSchFG sollte entsprechend klargestellt werden, dass der Schulträger zwar den Sachaufwand finanziert, jedoch nicht für die Verarbeitung und Nutzung personenbezogener Daten von Schülern, Eltern und Lehrern verantwortlich ist. Hier sollte auch festgelegt werden, dass der Schulträger im Rahmen der Auftragsdatenverarbeitung die erforderlichen technischen und organisatorischen Maßnahmen nach § 9 Thüringer Datenschutzgesetz (ThürDSG) für die Schulen bzw. die zuständige Schulaufsichtsbehörde trifft. Gemäß § 3 Abs. 5 ThürDSG ist zwar die „Daten verarbeitende Stelle“ definiert, in der Praxis bestehen aber Abgrenzungsschwierigkeiten zwischen den Aufgaben des Schulträgers und der Schule.
Der TLfDI legte dar, dass diese Schwierigkeiten in der Abgrenzung beispielsweise für das Abschließen von Vereinbarungen über eine

Auftragsdatenverarbeitung mit der Schule als Auftraggeber und dem Schulträger als Auftragnehmer bestehen. Sofern die Schule nach Ansicht des früheren Thüringer Ministeriums für Bildung, Wissenschaft und Kunst (TMBWK) als nicht rechtsfähige Anstalt öffentlichen Rechts keine Verträge abschließen kann, muss das Staatliche Schulamt als Aufsichtsbehörde anstelle der Schule diese Vereinbarungen mit dem Schulträger schließen. Ein weiteres Beispiel ist die Regelung der Zuständigkeit für das Erstellen eines Sicherheitskonzepts zur Ermittlung der zu treffenden technischen und organisatorischen Maßnahmen nach § 9 ThürDSG. In einigen Bereichen haben die behördlichen Datenschutzbeauftragten (bDSB) der Staatlichen Schulämter die Eigenschaft der Schulen als Daten verarbeitende Stellen jedoch anerkannt. Dies ist u. a. der Fall bei der Freigabe für in der Schule genutzte automatisierte Verfahren und bei der Aufnahme dieser Verfahren in das Verfahrensverzeichnis nach § 10 ThürDSG.

Weiterhin legte der TLfDI dar, dass die bisherigen Regelungen des § 57 Abs. 9 ThürSchulG und § 136 Abs. 9 Thüringer Schulordnung (ThürSchulO) aufgrund des technischen Fortschritts überholt und daher ergänzungsbedürftig sind. Als Datenverarbeitungsgeräte wurden die privaten stationären Computerarbeitsplätze des Lehrpersonals mittlerweile durch leistungsfähige Smartphones und Tablets abgelöst. Diese Geräte und die gespeicherte Anwendungssoftware ermöglichen jederzeit den Internetzugang und sind aus datenschutzrechtlicher Sicht weitaus kritischer einzuschätzen. Daher sind hierfür klare Verwendungsregeln erforderlich.

Deshalb sollte nach Auffassung des TLfDI in § 57 ThürSchulG eine Regelung aufgenommen werden, wonach personenbezogene Daten der Schulverwaltung grundsätzlich nur mit Datenverarbeitungsgeräten und Software des Schulträgers verarbeitet werden dürfen. Weiterhin sollte festgelegt werden, dass eine elektronische Kommunikation der Schule nur auf den Übertragungswegen erfolgen darf, die das für Schulwesen zuständige Ministerium zugelassen hat. Näheres hierzu sollte in einer Verordnung geregelt werden.

Abschließend wies der TLfDI das TMBJS noch auf ein datenschutzrechtliches Problem in der Schulgesundheitspflege hin: Nach § 8 Abs. 6 der Thüringer Verordnung über die Schulgesundheitspflege (ThürSchulgespflVO) müssen die Dokumentationsunterlagen in den Gesundheitsämtern mit Ablauf des Kalenderjahrs, in dem der Schüler keine Schule mehr besucht, gesperrt werden. Dies ist jedoch nicht

möglich, da die Gesundheitsämter von den Schulen keine entsprechende Meldung erhalten. Daher sollte eine entsprechende Meldepflicht gesetzlich geregelt werden.
Der TLfDI bot dem TMBJS seine Mitarbeit bei der Aufnahme der von ihm dargelegten datenschutzrechtlichen Regelungen an und bat um Information, inwieweit das TMBJS entsprechende Regelungen in die schulgesetzlichen Bestimmungen aufnehmen wird. Eine Antwort aus dem TMBJS liegt jedoch trotz nochmaliger Erinnerung nicht vor. Der TLfDI bleibt natürlich dran!

Gemäß § 3 Abs. 5 ThürDSG ist Daten verarbeitende Stelle jede öffentliche Stelle, die Daten in eigener Verantwortung für sich selbst verarbeitet oder nutzt oder dies im Auftrag durch andere vornehmen lässt. Um in dieser Hinsicht Abgrenzungsschwierigkeiten zwischen den Aufgaben des Schulträgers und der Schule zu vermeiden, sollte im ThürSchulG die Schule ausdrücklich als Daten verarbeitende und somit verantwortliche Stelle bestimmt werden. Im ThürSchFG sollte entsprechend klargestellt werden, dass der Schulträger zwar den Sachaufwand finanziert, jedoch nicht für die Verarbeitung und Nutzung personenbezogener Daten verantwortlich ist.

16.19 Hochschuleigene E-Mail-Adresse

In die Immatrikulationsordnung einer Thüringer Hochschule wurde ein neuer Passus eingefügt, nach dem jeder Studierende vom Universitätsrechenzentrum mit Einschreibung eine studentische E-Mail-Adresse auf dem Mailserver der Universität erhalten sollte. Der Studierendenrat der Universität bat den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) diesbezüglich um eine datenschutzrechtliche Beurteilung.
Dem Studierenden sollte die Möglichkeit eingeräumt werden, die universitären E-Mails regelmäßig unter der studentischen E-Mail abzurufen oder diese an eine andere E-Mail-Adresse weiterzuleiten. Datenschutzrechtlich zu beurteilen wäre, ob die so ermöglichte Übermittlung von personenbezogenen Daten, wie zum Beispiel Prüfungs- und Immatrikulationsangelegenheiten, per E-Mail oder Mailanhang die Erfordernisse des Landesdatenschutzrechtes erfüllt.
Eine datenschutzrechtliche Beurteilung ist nicht nötig, solange nur Informationen und Hinweise an die Studierenden versandt werden, wie Rundmails, Öffnungszeiten oder allgemein organisatorische

Hinweise, die keine personenbezogenen Daten enthalten. Sollten personenbezogene Daten übermittelt werde, bestehen aus datenschutzrechtlicher Sicht verschiedene Bedenken. Bei Schriftverkehr in Verwaltungsangelegenheiten, die personenbezogene Daten enthalten, ist fraglich, ob nicht der postalische Zugang eingeräumt werden muss. Hier würde der § 3a Thüringer Verwaltungsverfahrensgesetz (ThürVwVfG) Anwendung finden. Demnach ist die Übermittlung elektronischer Dokumente zulässig, soweit der Empfänger hierfür einen Zugang eröffnet hat. Die Zustimmung des Studierenden wäre also nötig, um elektronische Dokumente, die personenbezogene Daten enthalten, zu übermitteln. Wenn der Studierende den Zugang zur elektronischen Kommunikation nicht eröffnet hat, muss die Universität den postalischen Weg nutzen. Hat sich dagegen ein Empfänger dazu entschlossen, die elektronische Kommunikation mit der Universität zu nutzen, muss die Stelle gewährleisten, dass zwischen dem Sender und dem Empfänger die Vertraulichkeit, die Integrität und die Authentizität der übertragenden Information gewährleistet ist. Denn nach § 9 Abs. 1 Thüringer Datenschutzgesetz müssen öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten verarbeiten, die technischen und organisatorischen Maßnahmen treffen, die erforderlich sind, um die Ausführung der Bestimmungen dieses Gesetzes zu gewährleisten. Die Stelle hat die entsprechenden Verschlüsselungs- und Signaturverfahren nach § 3a Abs. 2 ThürVwVfG anzuwenden.
Dies erläuterte der TLfDI der Universität und bat um Stellungnahme, außerdem erfragte er, ob den Studierenden ein entsprechendes Verschlüsslungs- uns Signaturverfahren zur Verfügung steht. Die Universität erklärte, dass die studentischen E-Mails wichtige Hinweise und Informationen enthalten, die keine personenbezogenen Daten einschließen. Im Übrigen würde die E-Mail-Adresse von Studierenden genutzt, um von sich aus die entsprechenden Stellen der Universität zu kontaktieren. Das Akademische Studien- und Prüfungsamt der Universität verwendet die studentische E-Mail-Adresse nicht für die Bekanntgabe von Noten, kann aber Studierende gegebenenfalls zur Sprechstunde bitten. Weiterhin legte die Universität dar, dass die E-Mails vollständig als Inhouse-E-Mails verwendet werden, dadurch bestehe bereits grundsätzlich ein hohes Sicherheitsniveau. Der Zugang zum E-Mail-Dienst der Universität erfolgt über das HTTPS-Übertragungsprotokoll, der Abruf und das Versenden der E-Mails erfolgt über eine durch das SSL/TLS-Übertragungsprotokoll gesi-

cherte Sitzung. Zudem beherrscht der E-Mail-Server für die Server-Server-Kommunikation Verschlüsselung, sodass für eine gegebenenfalls erfolgende Übermittlung von personenbezogenen Daten durch die Universität eine dem Datenschutz angemessene sichere Datenübertragung gewährleistet ist.
Zudem merkte die Universität an, dass § 3a ThürVwVfG die Möglichkeit der rechtswirksamen Übermittelung elektronischer Dokumente im Verwaltungsverfahren regelt. Für die Übermittelung elektronischer Dokumente außerhalb eines förmlichen Verwaltungsverfahrens enthält § 3a ThürVwVfG keine bindenden Regularien. Insofern kann die Universität durch Satzung für ihre Mitglieder eine Zugangsmöglichkeit für nicht formbedürftige Dokumente schaffen, ohne dass die Anforderungen des § 3a Abs. 2 ThürVwVfG vorliegen müssen, folglich können Dokumente formfrei per E-Mail versendet werden. Verwaltungsakte werden von der Hochschule nach Maßgabe der §§ 37 und 41 ThürVwVfG erlassen und bekanntgegeben, es wird seitens der Universität nicht beabsichtigt, diese elektronisch zuzustellen.
Aufgrund des Satzungsrechts nach § 3 Thüringer Hochschulgesetz kann die Universität für ihre Mitglieder in einer hochschuleigenen Ordnung die ausschließliche Zugangsmöglichkeit per E-Mail für nicht formbedürftige Dokumente vorschreiben. Ein Verstoß gegen datenschutzrechtliche Vorschriften liegt hier somit nicht vor.
Wenn eine Weiterleitung der E-Mails von der studentischen E-Mail-Adresse an eine weitere E-Mail-Adresse erfolgt, liegt die Sicherstellung des Datenschutzes auf Seite des Studierenden. Dies teilte der TLfDI so dem Studierendenrat mit und schloss damit die datenschutzrechtliche Prüfung ab.

Unter Voraussetzung, dass die E-Mails keine personenbezogenen Daten beinhalten, ist es zulässig, dass eine Universität ihren Studierenden eine E-Mail-Adresse auf ihren Mailserver einrichtet. Sollte eine Übermittlung von elektronischen Dokumenten mit personenbezogenen Daten erfolgen, muss der Mailverkehr durch ausreichende technische und organisatorische Maßnahmen vor dem Zugriff Unbefugter gesichert sein.

16.20 Wie geht Datenschutz? – Da fragen wir doch den TLfDI!

Immer wieder erreichen den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) Anfragen von verschiedenen, vor allem öffentlichen Stellen in Thüringen, die darum bitten, dass ihre behördlichen Datenschutzbeauftragten vom TLfDI in Fragen des Datenschutzes geschult werden. Nach § 10a Abs. 1 des Thüringer Datenschutzgesetzes (ThürDSG) haben Daten verarbeitende Stellen, die personenbezogene Daten mithilfe automatisierter Verfahren verarbeiten oder nutzen, einen ihrer Beschäftigten zum Beauftragten für den Datenschutz schriftlich zu bestellen. Da mittlerweile die gesamte Verwaltung im Freistaat Thüringen mittels automatisierter Verfahren geschieht, ist davon auszugehen, dass alle öffentlichen Stellen einen behördlichen Datenschutzbeauftragten zu bestellen haben. Zum behördlichen Datenschutzbeauftragten bestellt werden darf nach § 10a Abs. 1 Satz 3 ThürDSG nur, wer die notwendige Fachkenntnis in Fragen des Datenschutzes und der Datensicherheit hat. Bei den bestellten Personen handelt es sich in aller Regel nicht von vornherein um ausgewiesene Datenschutzfachleute, da immer ein Beschäftigter der jeweiligen Stelle bestellt werden muss, sondern um Personen, die eine gewisse Affinität zu dem Thema haben und sich darin fortbilden müssen. Diesen Fortbildungsbedarf kann der TLfDI allerdings mit dem ihm zur Verfügung stehenden Personal nicht abdecken. Auch kann der TLfDI, wie das oft gewünscht wird, keine Bildungsträger empfehlen, weil er dann gegen das Gebot der wettbewerbsrechtlichen Neutralität verstoßen würde. Den Anfragenden wird in solchen Fällen vorgeschlagen, auf den Internetseiten der Berufsverbände (BvD und GDD) nach Fortbildungsangeboten zu schauen. Eine weitere Möglichkeit, geeignete Schulungsangebote zu finden ist, sich bei den behördlichen Datenschutzbeauftragten anderer öffentlicher Stellen zu erkundigen.

Zum behördlichen Datenschutzbeauftragten bestellt werden darf nach § 10a Abs. 1 Satz 3 ThürDSG nur, wer die notwendige Fachkenntnis in Fragen des Datenschutzes und der Datensicherheit hat. Die betreffenden Personen benötigen daher oft Schulungen im Bereich des Datenschutzes. Auf den Internetseiten der Berufsverbände BvD und GDD finden sich zahlreiche Fortbildungsangebote.

16.21 Sitzpläne mit Matrikelnummern – zulässig?

Eine Universität bat den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), die Zulässigkeit einer von ihr angewandten Verfahrensweise zu prüfen. Die Universität verwendet für die ausgehängten Sitzpläne, mittels derer über die während der Klausuren vorgesehenen Sitzplätze informiert wird, die Matrikelnummern der Studierenden.
Der TLfDI erklärte nach entsprechender Prüfung, dass aus datenschutzrechtlicher Sicht die Erstellung von Sitzplänen unter Nennung der Matrikelnummern nicht zulässig ist, da hierdurch für Dritte die Möglichkeit besteht, die Matrikelnummer einer konkreten Person zuzuordnen. Schon vor Beantwortung der Anfrage des TLfDI stellte die Universität das System für die Erstellung der Sitzpläne um. Die Matrikelnummer wurde durch die laufenden Nummern auf der Unterschriftenliste ersetzt.
Allerdings machte die Universität gegenüber dem TLfDI geltend, dass die neue Darstellung für die Hochschulverwaltung organisatorisch schwerer zu bewältigen sei. Deshalb bat die Universität den TLfDI um eine detailliertere Begründung für die Unzulässigkeit der Verwendung der Matrikelnummern zu. Der TLfDI verwies in seiner Antwort die Hochschule darauf, dass ursprünglich die Matrikelnummern den Studierenden in allen Hochschulen als Pseudonym zugewiesen wurden, um den Namen und andere Identifikationsmerkmale durch diese Zahlenkombination zu ersetzen und so die Bestimmung des Betroffenen ohne Nutzung der Zuordnungsfunktion auszuschließen. Die Matrikelnummer sollte daher nur der Universität und dem Studierenden bekannt sein. Durch die eindeutige Zuordnung zu Sitzplätzen wäre es nun jedoch unter Umständen möglich, die Matrikelnummer desjenigen Studenten, der sich auf einem bestimmten Platz befindet, ohne Schwierigkeit in Erfahrung zu bringen.
Die Universität versicherte dem TLfDI, dass die Matrikelnummern an dieser Hochschule zu keinen anderen Zwecken als zur Bestimmung der Platzwahl öffentlich genutzt werden, also z. B. weder für den Aushang von Noten noch für Seminarzuteilungen am schwarzen Brett. Dritte könnten also mit den Matrikelnummern keine personenbezogenen Daten verknüpfen.
Da die Matrikelnummern von der Hochschule ausschließlich als Pseudonym für die Erstellung der Sitzpläne während einer Klausur

zur Vereinfachung von Verwaltungsvorgängen veröffentlicht werden, bestehen für den TLfDI in diesem speziellen Fall aus datenschutzrechtlicher Sicht keine Bedenken gegen die beschriebene Anwendung.

Auch bei der Matrikelnummer eines Studierenden handelt es sich im Regelfall um ein personenbezogenes Datum. Die personenbezogene Zuordnung sollte nur der Universität und dem Studierenden bekannt sein. Im hier vorliegenden Ausnahmefall kann die Verwendung von Matrikelnummern zulässig sein, wenn Dritte aufgrund der einzigen öffentlichen Verwendung der Matrikelnummer als Sitzplatzzuweisung keine personenbezogenen Daten mit Studierenden verknüpfen können. Sollten beispielsweise Notenlisten mit Matrikelnummern veröffentlicht werden, wäre eine Verwendung der Matrikelnummern für den genannten Zweck unzulässig.

16.22 Online-Gremienwahlen an der Friedrich-Schiller-Universität Jena

Studierende der Friedrich-Schiller-Universität fragten beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) an, ob bei den an der Universität durchgeführten Online-Wahlen für die Vertretungen in den universitären Gremien (Senat, Fakultätsräte, Beirat für Gleichstellungsfragen) das Wahlgeheimnis und weitere Aspekte des informationellen Selbstbestimmungsrechts der Stimmberechtigten im erforderlichen Maße gewahrt werden.
Der TLfDI wandte sich daraufhin an das Wahlamt der Universität und bat dort um Auskunft, auf welcher rechtlichen Grundlage Online-Gremienwahlen durchgeführt werden dürfen, welche Hard- und Software hierbei eingesetzt wird und welche nach § 9 Thüringer Datenschutzgesetz (ThürDSG) erforderlichen technischen und organisatorischen Maßnahmen von der Universität ergriffen wurden, um die Ausführung der Bestimmungen des ThürDSG zu gewährleisten. Die Universität teilte dem TLfDI mit, dass die Wahlen gemäß § 37 Abs. 1 Satz 1 Hochschulrahmengesetz in Verbindung mit § 22 Thüringer Hochschulgesetz (ThürHG) und in der Wahlordnung der Universität geregelt sind. Zusätzlich wurde auf eine Entscheidung des Thüringer Oberverwaltungsgerichts vom 30. Mai 2013 (Az. 1 N 240/12) verwiesen, in der die Durchführung von Online-Wahlen

in Hochschulen grundsätzlich für rechtlich zulässig erachtet wird und die Hochschule aufgrund der Zuweisung nach § 22 Abs. 7 ThürHG die Möglichkeit zum Erlass einer Wahlordnung und zur Einführung von Online-Wahlen hat. In der Gerichtsentscheidung wurde aber auch die damalige konkrete Durchführung der Online-Wahlen für nicht ausreichend angesehen.
Die Universität hatte auf der Grundlage der Gerichtsentscheidung bereits einen Monat später ihre Wahlordnung angepasst. Dabei wurde der TLfDI auf einen Artikel der Zeitschrift „Datenschutz und Datensicherheit“ (Roßnagel/Richter; Internetwahlen an Hochschulen, Rechtliche Anforderungen an die technische und rechtliche Gestaltung, DuD 2/2014, 93 ff.) verwiesen, in dem der FSU Jena nicht nur die Umsetzung der gerichtlichen Anforderungen bestätigt wird, sondern die ergriffenen Maßnahmen teilweise hierüber noch hinausgehen. Die FSU Jena führt die Online-Wahl mit einem auch von anderen Hochschulen und Einrichtungen eingesetzten Verfahren eines Wahldiensteanbieters durch. Das Wahlverzeichnis wird auf einem universitätseigenen Server am Universitätsrechenzentrum betrieben. Dieses besteht aus einer laufenden Nummer, die vom Wahlamt der FSU Jena vergeben wird sowie einem numerischen zehnstelligen Code, der die Stimmzettel der einzelnen Wahlbereiche definiert. Ein Rückschluss auf konkrete Wähler sei zu keinem Zeitpunkt möglich, da die wahre Identität nur dem Wahlamt bekannt sei. Die Wahlberechtigten erhalten eine Wähleridentifikationsnummer und ein einmal gültiges Passwort, mit dem sich diese am System anmelden können. Vor der eigentlichen Stimmabgabe muss der Wahlberechtigte eine von der FSU Jena zuvor per E-Mail versendete, zufällig generierte achtstellige PIN und zusätzlich eine per Brief zugeschickte zehnstellige TAN eingeben. PIN und TAN verlieren nach Ablauf der Wahlfrist ihre Gültigkeit und werden bei jeder Wahl neu konfiguriert.
Nachdem der TLfDI die von der FSU Jena angegebenen Rechtsgrundlagen sowie den o. g. Fachartikel und die Prozedurenbeschreibung geprüft hatte, bestanden aus datenschutzrechtlicher Sicht keine Bedenken gegen das von der FSU Jena verwendete Verfahren zur Durchführung von Online-Wahlen. In der Folge wurde den Beschwerdeführern dieses Ergebnis mitgeteilt. Sie wandten sich nochmals an den TLfDI und wiesen auf ein weiteres Verfahren hin, welches von der FSU Jena verwendet wird und baten auch hierzu um eine datenschutzrechtliche Stellungnahme.

Das Wahlamt der FSU Jena teilte dem TLfDI auf dessen erneute Nachfrage mit, dass neben dem beschriebenen Wahlverfahren seit dem Sommersemester 2016 ein zweites Anmeldeverfahren eingesetzt wird. Hierbei wird nicht mehr das o. g. PIN- und TAN-Verfahren verwendet, sondern alle Wahlberechtigten, die über einen Benutzer-Account (E-Mail-Adresse) des Universitätsrechenzentrums verfügen, können sich aus dem Service-Portal des Universitätsrechenzentrums durch Anmeldung am Wahlsystem legitimieren. Der Account-Zugriff erfolgt dabei mit Nutzernamen und dem individuell festzulegenden Passwort. Inzwischen wird dieses Verfahren überwiegend eingesetzt, da alle Studierenden über einen Benutzer-Account verfügen. Soweit die Beschwerdeführer bei diesem Anmeldeverfahren geltend machen, dass die Vergabe des Passwortes nicht als ausreichend sicher anzusehen sei, stellte der TLfDI allerdings fest, dass systemseitig nur nicht einfach zu erratende Passwörter, die bestimmte Bedingungen erfüllen müssen, gewählt werden dürfen. Die Geheimhaltung des jeweils ausgewählten Passworts liegt ebenso in der Verantwortung der Studierenden wie die Änderung des zunächst bei Anmeldung generierten Passworts. Hierauf werden die Studierenden gemäß § 3 Abs. 2 Nr. 5 der Nutzerordnung des URZ auch ausdrücklich hingewiesen. Als technische Plattform wird ein Wahlsystem von der FSU Jena eingesetzt, welches nach Aussage des Wahlamtes der FSU Jena nach Maßgabe der Anforderungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) als sicher beurteilt wird. Die Beschreibung des Verfahrens der internetbasierten Online-Wahlen würde den Rahmen dieses Tätigkeitsberichts sprengen, ist aber ausführlich z. B. im Internetauftritt der FSU Jena unter https://www.unijena.de/unijenamedia/Downloads/einrichtungen/wahlamt/Wahl+2017/Sicherheitshinweise_2017.pdf dargestellt. Nach datenschutzrechtlicher Prüfung dieses Anmeldeverfahrens zur Online-Wahl konnte der TLfDI keinen Verstoß gegen Vorschriften über den Datenschutz feststellen. Die Beschwerdeführer wurden hierüber abschließend unterrichtet.

Hochschulen dürfen Online-Wahlen unter Beachtung der rechtlichen Anforderungen und der entsprechenden technischen und organisato-

rischen Umsetzung der gemäß § 9 ThürDSG zu ergreifenden erforderlichen Maßnahmen durchführen. Auch die Verwendung der E-Mail-Accounts der Studierenden für die Online-Wahl ist aus datenschutzrechtlicher Sicht grundsätzlich zulässig. Die Verantwortung für die Änderung des bei der ersten Anmeldung generierten Passwortes sowie die Geheimhaltung des Passworts liegt in der Verantwortung der Studierenden.

16.23 Immatrikulation – welche Speicherfrist gilt denn nun?

Die Beauftragte für den Datenschutz (bDSB) einer Thüringer Universität ist auf folgende Problematik gestoßen: Die Thüringer Immatrikulationsordnung (ThürImO) und die internen Immatrikulationsordnungen einiger Thüringer Hochschulen beziehen sich in verschieden Paragrapfen auf die Thüringer Verordnung zur Erhebung personenbezogener Daten der Studienbewerber, Studierenden und Prüfungskandidaten der Hochschulen des Landes vom 10. November 1992. Diese Verordnung ist jedoch mit Inkrafttreten der Thüringer Hochschul-Datenschutzverordnung (ThürHDatVO) im April 2012 außer Kraft getreten. Nun weiß die Betroffene nicht, wie der Datenschutz für die Studierenden geregelt ist, ob die Vorschriften in der ThürImO noch gelten, weil kein neuer Bezug hergestellt wurde oder auch diese ihre Gültigkeit verloren haben. Besonders interessierte sie die generelle Regelung zur maximalen Speicherfrist von personenbezogenen Daten von Studierenden an den Hochschulen.
Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) bedankte sich bei der bDSB der Hochschule und merkte an, dass bei offensichtlichen Fehlern der Wille des Gesetzgebers bzw. für die Hochschulordnung der Wille der Hochschule maßgebend für die Auslegung der einschlägigen Vorschriften ist. Generell hat eine außer Kraft getretene Verordnung ihre Gültigkeit auch dort verloren, wo diese in einer gültigen Vorschrift zitiert wird. So ist in der ThürImO die entsprechende Regelung aus der ThürHDatVO anzuwenden. Bei hochschulinternen Immatrikulationsordnungen gelten ebenfalls die Regelungen der ThürHDatVO.
Im Bezug zur Anfrage hinsichtlich der Speicherfrist von personenbezogenen Daten von Studierenden an Thüringer Hochschulen gab der TLfDI der Anfragenden folgende Information: Da gemäß § 1 ThürHDatVO das Thüringer Datenschutzgesetz (ThürDSG) dann

Anwendung findet, soweit in dieser Verordnung nicht anderes geregelt, gilt gemäß § 16 Abs. 1 Nr. 2 ThürDSG, dass personenbezogene Daten zu löschen sind, wenn ihre Kenntnis für die Daten verarbeitende Stelle zur Erfüllung ihrer Aufgaben nicht mehr erforderlich ist. Die Hochschulen haben unter Berücksichtigung dessen Aufbewahrungsfristen von personenbezogenen Studierendendaten festzulegen. Dabei sind nicht irgendwelche beliebigen Speicherfristen zu benennen, sondern diese sind anhand der tatsächlichen Erforderlichkeiten festzulegen. Vor einer Vernichtung solcher Daten ist zu prüfen, ob die Unterlagen dem zuständigen Staatsarchiv zur Entscheidung über die Archivierung angeboten werden müssen, § 11 in Verbindung mit § 3 Thüringer Archivgesetz. Möglicherweise erhalten die hochschuleigenen Immatrikulationsordnungen oder andere Datenschutzordnungen entsprechende Speicher- bzw. Löschfristen.

Daraufhin wies der TLfDI das dafür zuständige Thüringer Ministerium für Wirtschaft, Wissenschaft und Digitale Gesellschaft (TMWWDG) auf den entsprechenden Änderungsbedarf in der ThürImO hin. Darüber hinaus bat der TLfDI das TMWWDG, alle Hochschulen anzuschreiben, um diese zu einer Überarbeitung der Angabe der Rechtsgrundlage in ihren Ordnungen zu veranlassen.

Das TMWWDG bedankte sich bei dem TLfDI für den Hinweis auf den Aktualisierungsbedarf der Immatrikulationsordnungen im Hinblick auf die Inkraftsetzung der ThürHDatVO. Hinzufügend teilte es mit, dass die Thüringer Verordnung zur Erhebung personenbezogener Daten der Studienbewerber, Studierenden und Prüfungskandidaten der Hochschulen des Landes vom 10. November 1992 inhaltlich in der ThürHDatVO aufging und mit deren Inkrafttreten zum 28. April 2012 außer Kraft trat.

Die ThürImO, die die Verweise auf die außer Kraft gesetzte Datenschutzverordnung enthält, ist zwar formal noch in Kraft, entfaltet jedoch keine Rechtswirkungen mehr. Insoweit sei auf § 14 Satz 2 der ThürImO zu verweisen, wonach diese für die jeweilige Hochschule zu dem Zeitpunkt außer Kraft tritt, an dem eine vom Ministerium genehmigte eigene Immatrikulationsordnung in Kraft tritt. Alle Thüringer Hochschulen haben inzwischen eigene Immatrikulationsordnungen erlassen, die auf Grundlage des § 65 Abs. 5 Thüringer Hochschulgesetz (ThürHG) durch das TMWWDG genehmigt worden sind. Deshalb beabsichtigt das TMWWDG, die ThürImO demnächst aufzuheben.

Die meisten Immatrikulationsordnungen der Hochschulen verwiesen bereits auf die Vorschriften der geltenden ThürHDatVO, teilweise jedoch noch auf die außer Kraft gesetzte Datenschutzverordnung. Da die Regelungen der ThürHDatVO unmittelbare Anwendung finden, d. h. keiner Umsetzung in den Hochschulsatzungen bedürfen (§ 10 Abs. 2 ThürHG), hätten die datenschutzrechtlichen Verweise in den Immatrikulationsordnungen lediglich deklaratorischen Charakter. Die entsprechenden Vorschriften stehen nicht im Widerspruch zu den Regelungen der ThürHDatVO. Der bestehende Anpassungsbedarf wäre damit rein redaktioneller Natur. Nach Auskunft der betroffenen Hochschulen sollten die redaktionellen Anpassungen im Zusammenhang mit geplanten oder in Arbeit befindlichen inhaltlichen Änderungen der Immatrikulationsordnung vorgenommen werden.

Grundsätzlich gilt, dass eine außer Kraft getretene Verordnung ihre Gültigkeit auch dort verloren hat, wo auf diese in einer gültigen Vorschrift verwiesen wird. Thüringer Hochschulen besitzen eine eigene interne, vom TWWDG genehmigte Immatrikulationserklärung. Da die Regelungen der ThürHDatVO unmittelbare Anwendung finden und darin auch abschließend die zu verarbeitenden Daten aufgeführt sind, haben die Verweise auf den Datenschutz in den Immatrikulationsordnungen lediglich deklaratorischen Charakter.

16.24 Adresslisten mit personenbezogenen Daten in Papiermüllcontainern einer Universität?

Ein besorgter Bürger sprach in den Geschäftsräumen des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) vor und berichtete unter anderem, dass er beim Durchsuchen von Papiermüllcontainern einer Thüringer Universität nicht geschredderte Adresslisten mit Namen von Studenten, Adressen sowie Telefonnummern und E-Mail-Adressen gefunden habe. Es käme immer wieder zu solchen Funden. Belege für seine Aussage, z. B. durch Fotos des Containers oder eine gefundene Adressliste, legte er dem TLfDI nicht vor. Obwohl somit keine Nachweise vorlagen, wandte sich der TLfDI umgehend an den Kanzler der Universität, informierte über die Aussagen des Bürgers und bat um Recherche in dieser Sache. Der Kanzler antwortete, dass er zum Vorgang leider nicht dezidiert Stellung nehmen könne, da die dargestellten

Fakten nicht einzuordnen seien. Es sei nicht erkennbar, ob es sich um Dokumente aus dem Dienstbetrieb der Universität oder des Studierendenwerkes handele. Auch die Umstände des Auffindens seien unklar. Schließlich sei auch eine gezielte Falschmeldung nicht auszuschließen. Auf Anfrage des TLfDI nach Vorschriften der Universität für die Vernichtung von Papierunterlagen mit personenbezogenen Daten informierte der Kanzler über den Ablauf der Aktenentsorgung und die beteiligten Fachfirmen. Er informierte auch, dass im Zusammenhang mit dem Fall offenbar wurde, dass eine allgemeine Dienstanweisung für den Umgang mit Datenabfall noch nicht vorhanden sei. Eine entsprechende Dienstanweisung werde derzeit erarbeitet. Im Vorgriff auf die Dienstanweisung seien alle Mitarbeiter der Universität über die Beachtung der datenschutzrelevanten Gebote bei der Entsorgung von Datenträgern sensibilisiert worden. Nach entsprechender Anfrage erwartet der TLfDI noch die Übermittlung dieser Dienstanweisung der Universität an die Landesdatenschutzbehörde.
Der Fall zeigt, dass datenschutzrechtliches Bewusstsein bei Verantwortlichen durchaus vorhanden, aber nicht immer präsent ist. Nach Befassung des TLfDI mit der Sache reagierte die Universität umgehend und konstruktiv.

Einer Information eines Bürgers folgend befasste sich der TLfDI mit dem Vorwurf, dass eine Universität Akten mit personenbezogenen Daten von Studenten unsachgemäß in öffentlich zugänglichen Papiercontainern entsorgen würde. Obwohl Belege für die Richtigkeit des vorgetragenen Sachverhaltes fehlten, reagierte die Universität auf Bitte des TLfDI umgehend durch Erläuterung ihrer Entsorgungspraxis. Mit einem Rundschreiben sensibilisierte die Universität ihre Mitarbeiter vorsorglich über den datenschutzgerechten Umgang mit Datenmüll. Die Erarbeitung einer entsprechenden Dienstanweisung wurde veranlasst. Leider wird offen bleiben, ob die Vorwürfe an die Universität überhaupt zutrafen, da Belege für den vermeintlichen Datenschutzverstoß fehlten.

16.25 Kontoauszüge – welche darf das Amt sehen?

Ein Auszubildender wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und beschwerte sich über das Amt für Ausbildungsförderung (AfA) einer

Stadt in Thüringen. Der Beschwerdeführer hatte nach eigenen Angaben beim AfA einen Folgeantrag auf Ausbildungsförderung gestellt und dem Amt die erforderlichen Nachweise übersandt. Das AfA forderte vom Beschwerdeführer die Vorlage sämtlicher Kontoauszüge von November 2015 bis Juli 2016. Dies sah der Beschwerdeführer als groben Verstoß gegen das Datenschutzgesetz an und bat den TLfDI um Bewertung.

Der TLfDI forderte das AfA zunächst zur Stellungnahme zum vorgetragenen Sachverhalt auf. Das AfA legte dar, dass es im Grundsatz um die Höhe der Vermögensanrechnung des Beschwerdeführers ginge. Aus den eingereichten Nachweisen des Beschwerdeführers sei die Gutschrift eines Bausparguthabens auf seinem Girokonto ersichtlich gewesen und das AfA habe prüfen müssen, wie hoch das Vermögen des Beschwerdeführers zum Zeitpunkt der Antragstellung auf finanzielle Unterstützung nach dem Bundesausbildungsförderungsgesetz (BAföG) war. Aus den eingereichten Nachweisen sei es jedoch nicht möglich gewesen, diesen Sachverhalt hinreichend aufzuklären, sodass das AfA weitere Belege abfordern musste. Aufgrund des vom Beschwerdeführer angegebenen Vermögensverbrauchs konnte das AfA einen Rechtsmissbrauch nach eigner Darlegung nur über die Vorlage von lückenlosen und ungeschwärzten Kontoauszügen vollständig prüfen. Es wollte feststellen, ob der Beschwerdeführer Vermögensanteile an Dritte (Eltern, Geschwister) übertragen hatte.

Das AfA räumte in seiner Stellungnahme ein, gegenüber dem Beschwerdeführer das Prüfungsanliegen nicht eindeutig formuliert zu haben, was möglicherweise zu Irritationen geführt habe. Daraus ergab sich, dass der vom Beschwerdeführer geschilderte Sachverhalt weniger ein bewusster datenschutzrechtlicher Verstoß durch das AfA war, als vielmehr ein Missverständnis aufgrund mehrdeutiger Formulierungen. Daher hatte sich das AfA zwischenzeitlich auch mit dem Beschwerdeführer ins Benehmen gesetzt und einen Abhilfebescheid erlassen. Das AfA hatte die Verwertung eines Teilvermögens als Zufluss auf das Sparkonto des Beschwerdeführers anerkannt und den Vermögensgesamtwert entsprechend geändert, sodass sein Guthaben durch den Vermögensfreibetrag nach § 29 Abs. 1 Nr. 1 BAföG anrechnungsfrei blieb.

Aufgrund der Stellungnahme des AfA teilte der TLfDI dem Beschwerdeführer mit, dass er keinen datenschutzrechtlichen Verstoß

feststellen konnte und der vorgetragene Sachverhalt auf Missverständnissen aufgrund der Formulierungen des AfA beruhte.
Um entsprechende Missverständnisse in Zukunft zu vermeiden, empfahl der TLfDI dem AfA, die schriftliche Anforderung von Unterlagen stets so zu formulieren, dass beim Antragsteller nur Unterlagen abgefordert werden, die für eine Sachverhaltsklärung auch tatsächlich notwendig sind. Außerdem informierte der TLfDI die Behörde darüber, dass er eine pauschale Anforderung von Kontoauszügen, die einen längeren Zeitraum betreffen, für datenschutzrechtlich bedenklich erachtet. Der Antragsteller muss genau darüber aufgeklärt werden, welche Kontoauszüge zu welchen Zwecken zur Einsichtnahme erforderlich sind. In diesem Sinne dürfen gemäß § 19 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) immer nur die zur Aufgabenerfüllung erforderlichen Daten des Betroffenen erhoben werden. Daher müssen bei Anforderung der vorzulegenden Unterlagen so genau wie möglich beschrieben dementsprechend eindeutige Formulierungen verwendet werden.
Weiterhin teilte der TLfDI dem AfA mit, dass dem Antragsteller nicht generell untersagt werden kann, einzelne Buchungen zu schwärzen. Aus welchen Zeiträumen Kontoauszüge angefordert werden dürfen und was in den einzelnen Buchungen geschwärzt werden darf, muss im Einzelfall geprüft werden. Die Behörde muss den Betroffenen über die Gründe informieren, wenn sie eine Schwärzung für unzulässig hält. In diesem Zusammenhang wies der TLfDI das AfA darauf hin, dass besonders geschützte Daten nach dem Sozialgesetzbuch (§ 67 Abs. 12 Sozialgesetzbuch SGB X, u. a. Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen) und § 4 Abs. 5 ThürDSG grundsätzlich teilweise geschwärzt werden können, wenn die Höhe der Überweisung noch lesbar bleibt.

Das Erheben personenbezogener Daten ist gemäß § 19 Abs. 1 ThürDSG nur zulässig, wenn ihre Kenntnis zur Erfüllung der Aufgaben der erhebenden Stelle erforderlich ist. Besonders geschützte Daten nach dem Sozialgesetzbuch (§ 67 Abs. 12 Sozialgesetzbuch SGB X) und § 4 Abs. 5 ThürDSG können grundsätzlich teilweise geschwärzt werden.

16.26 Beschwerde über BAföG-Stelle

Ein Bürger beschwerte sich beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) über ein Amt für Ausbildungsförderung (AfA), weil von dort seine personenbezogenen Daten an einen fremden Antragsteller von Leistungen nach dem Bundesausbildungsförderungsgesetz (BAföG) übermittelt wurden. Der TLfDI wandte sich daraufhin an das AfA und forderte dieses zu einer Stellungnahme auf. Das AfA erläuterte in seiner Antwort, dass die in Rede stehenden Daten dem Antragsteller im BAföG-Verfahren in der Begründung eines Bescheids zur Kenntnis gegeben wurden. Bei dem Beschwerdeführer handelte es sich um den zweiten Ehemann der Mutter des BAföG-Antragstellers. Der Beschwerdeführer selbst habe in keiner Vater-Kind-Beziehung zum Antragsteller gestanden. Für die Berechnung des Förderungsanspruchs des BAföG-Antragstellers habe deshalb das Einkommen des Beschwerdeführers nach § 11 Abs. 2 BAföG grundsätzlich keine Rolle gespielt, die Höhe des Einkommens ermittelte sich entsprechend den Regelungen der §§ 21 ff. BAföG. Allerdings habe die Mutter des Antragstellers bei der Berechnung ihres eigenen Einkommens die Berücksichtigung außergewöhnlicher Belastungen ihres Ehemanns, also des Beschwerdeführers, geltend gemacht. Da diese nach Auffassung des AfA nicht angerechnet werden konnten, reichte die Mutter weitere Unterlagen ein, die auch den Beschwerdeführer betrafen. Somit habe nicht das AfA, sondern die Mutter personenbezogene Daten des Beschwerdeführers in das Verfahren eingebracht. Das AfA sei nach § 35 Sozialgesetzbuch (SGB) Zehntes (X) Buch in Verbindung mit § 50 Abs. 2 BAföG verpflichtet, einen Bescheid über Leistungen nach dem BAföG zu begründen und müsse dabei die wesentlichen tatsächlichen und rechtlichen Gründe mitteilen, die das AfA zu seiner Entscheidung über die Förderhöhe bewogen haben. Nach Prüfung der vom AfA genannten Rechtsgrundlagen und unter Berücksichtigung des Verfahrensablaufs kam der TLfDI zur Auffassung, dass die erfolgte Datenübermittlung der Daten des Beschwerdeführers an den Antragsteller zur Erfüllung der gesetzlichen Aufgaben der AfA nach § 69 Abs. 1 Nr. 1 SGB X grundsätzlich zulässig waren.
Der Beschwerdeführer wandte sich daraufhin nochmals an den TLfDI, da er es nicht für erforderlich hielt, dem Antragsteller in der Begründung mitzuteilen, welche Tatsachen keine Anrechnung auf

das Einkommen der Mutter gefunden hatten. Der TLfDI teilte diese Einschätzung des Beschwerdeführers und forderte das AfA auf, im vorliegenden Fall zukünftig bei erneut zu erteilenden Auskünften auf die Mitteilung von nicht für die Berechnung relevanten Informationen zu verzichten. Das AfA sagte dem TLfDI abschließend zu, die Darstellung der Gründe, ob ein Freibetrag für den Beschwerdeführer berücksichtigt werden kann, aus dem Bescheid zu entfernen. Der TLfDI informierte den Beschwerdeführer abschließend über das erreichte Ergebnis.

Die Ämter für Ausbildung müssen ausführlich prüfen, welche Informationen unbedingt erforderlich sind, damit ein Antragsteller die sachliche und rechtliche Richtigkeit eines Bescheids über Leistungen nach dem BAföG prüfen kann. Die schutzwürdigen Interessen von nur mittelbar Betroffenen sind dabei zu berücksichtigen.

16.27 Plagiatsprüfung

Ein Studierender schilderte dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), dass an einem Institut der Friedrich-Schiller-Universität Jena (FSU Jena) ein Plagiatsverfahren zur Anwendung kommt und er nicht von der datenschutzrechtlichen Zulässigkeit dieses Verfahrens überzeugt sei. Wie der Homepage des Anbieters des Verfahrens zu entnehmen war, müssen die Studierenden ihre Haus- und Abschlussarbeiten an eine spezielle vom Anbieter zur Verfügung gestellte E-Mail-Adresse senden. Dort werden die Arbeiten von einem schwedischen Anti-Plagiatsservice einer Plagiatsprüfung unterzogen.
Um das Verfahren einer näheren datenschutzrechtlichen Beurteilung zu unterziehen, wandte sich der TLfDI mit zahlreichen Fragen zum Plagiatsverfahren an die FSU Jena. Wie die Hochschulleitung in ihrer Stellungnahme mitteilte, werde das Verfahren als Pilotprojekt von einem Institut und einer Professur zunächst auf zwei Jahre befristet eingesetzt. Daher seien hierzu bisher keine Regelungen in einer Studien- oder Prüfungsordnung aufgenommen worden. Die Studierenden werden auf der Homepage des Instituts über das Plagiatsprüfungsverfahren informiert, während der Lehrstuhl in einem Erstgespräch zur Anfertigung einer schriftlichen Arbeit auf die Plagiatsprüfung hinweist. Die Plagiatsprüfung werde nicht bei jeder abgegebenen Arbeit, sondern nur anlassbezogen im Einzelfall ange-

wandt. Zur Durchführung des Verfahrens müssen Studierende ihre Haus- oder Abschlussarbeiten in Papierform verschicken und zusätzlich als digitale Datei an eine eigens hierfür eingerichtete E-Mail-Adresse der Prüfer senden. Die Übersendung erfolge als unverschlüsselte E-Mail. Das Einholen einer Einwilligung bei den Betroffenen sei nicht erforderlich, da die Daten gemäß § 8 Thüringer Datenschutzgesetz (ThürDSG) im Auftrag der FSU Jena verarbeitet werden. Daraufhin wandte sich der TLfDI erneut an die FSU Jena und bat um Darlegung, ob die Hochschule eine entsprechende schriftliche Vereinbarung unter Berücksichtigung der in § 8 ThürDSG geforderten Festlegungen mit dem Anti-Plagiatsservice abgeschlossen hat (sogenannter Auftragsdatenverarbeitungsvertrag), und um Zusendung dieser Vereinbarung, zu der keine datenschutzrechtlichen Bedenken bestanden. Wie sich im Verlauf der weiteren datenschutzrechtlichen Prüfung zeigte, werden die Studierenden ausdrücklich darauf hingewiesen, das Deckblatt ihrer Arbeiten zu anonymisieren, indem alle Daten außer dem Titel der Arbeit zu löschen sind. Der TLfDI geht daher beim Versenden der Hausarbeiten durch die Studierenden über die E-Mail-Adresse der Dozenten bzw. Prüfer an das Anti-Plagiatsprüfungsunternehmen im Regelfall von einer nicht personenbezogenen Übermittlung aus. Das Unternehmen, welches die Plagiatsprüfung durchführt, kann aus dem Inhalt der Arbeit nicht ohne Weiteres auf die Autorenschaft schließen. Dies ist somit aus datenschutzrechtlicher Sicht nicht bedenklich. In allen anderen Fällen, in denen sich aus Hausarbeiten ohne großen Aufwand für das Unternehmen als Auftragnehmer die Autorenschaft einer bestimmten oder bestimmbaren Person ergibt, ist dies ebenfalls zulässig, da der gemäß § 8 ThürDSG zwischen der FSU Jena als Auftraggeber und dem Anti-Plagiatsunternehmen als Auftragnehmer in englischer Sprache geschlossene Vertrag über die Auftragsverarbeitung personenbezogener Daten als ausreichend anzusehen ist. Der TLfDI hatte zusätzlich geprüft, dass das Unternehmen sich im alleinigen Besitz eines schwedischen Unternehmens befindet und ausdrücklich nicht dem USA PATRIOT Act unterliegt. Werden personenbezogene Daten von einem EU-Unternehmen auf Servern von US-Tochterunternehmen gespeichert, so sind diese, unabhängig von den geltenden Gesetzen des Sitzlandes, nach diesem Gesetz verpflichtet, Zugriff auf ihre Server durch US-Behörden zu gewähren. Dies aber verstößt gegen EU-Datenschutzrecht. Ein solches Unternehmen dürfte daher nicht als Auftragnehmer gewählt werden. Al-

lerdings kritisierte der TLfDI die FSU Jena für die nicht nach § 8 Abs. 6 Satz 2 ThürDSG erfolgte Unterrichtung über die Beauftragung des Unternehmens, auf das die Bestimmungen des ThürDSG nicht anwendbar sind. Der Beschwerdeführer wurde abschließend über das Ergebnis unterrichtet.

Wenn eine Hochschule Plagiatsprüfungen von Haus- und Abschlussarbeiten von einem hierauf spezialisierten Unternehmen durchführen lässt, muss eine schriftliche Vereinbarung über die Auftragsdatenverarbeitung abgeschlossen werden. Dabei sind alle in § 8 ThürDSG aufgeführten Festlegungen vertraglich sicherzustellen. Die Hochschule darf nach dem Grundsatz der Datensparsamkeit nach § 1 Abs. 2 ThürDSG nur die hierfür unbedingt erforderlichen personenbezogenen Daten an den Auftragnehmer weitergeben.

16.28 Mediendatenbank für Thüringer Schulen 2.0

Es ist längst kein Geheimnis mehr: Die Medienbildung in Thüringer Schulen ist dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) ein besonderes Anliegen. Dass er nicht nur redet, sondern handelt, geht schon aus dem Tätigkeitsbericht 2014/2015 hervor. Dort ist beispielsweise von der Mediendatenbank (https://medien.tlfdi.de) die Rede (vgl. z. B. 14.2 des 11. Tätigkeitsberichts im öffentlichen Bereich von 2014/2015). Inhaltlich wurde sie zuletzt im Dezember 2017 aktualisiert und mit Links zu aktuellen Videos und Unterrichtsmaterialien rund um den Privatsphärenschutz ergänzt. Das muss auch weiterhin so sein, denn die Medienwelt und mit ihr der Datenhunger von Wirtschaft und Sicherheitsorganen wachsen ständig. So gilt es beispielweise auch Material zur Verfügung zu stellen, das Schülern die politische Dimension von Profiling und mögliche Anwendungsfälle zeigt. Für ein überzeugendes Beispiel konnte der TLfDI die Rechte für die Nutzung eines Videos in Thüringer Schulen erwerben und mit deutschen Untertiteln versehen. Im Video (siehe unter https://www.schulportal-thuerin-

gen.de/web/guest/media/detail?tspi=6453) spricht der Chief Executive Officer der britischen Datenanalysefirma Cambridge Analytica eindrucksvoll von den Datenverarbeitungsmöglichkeiten seiner Firma und der Einflussnahme auf die politische Profilierung von Präsidentschaftskandidaten im US-Wahlkampf 2015/2016. Unabhängig vom Wahrheitsgehalt seiner Worte ist klar: Was technisch geht, wird versucht: heute, morgen, spätestens übermorgen. Der TLfDI sieht seine Aufgabe auch darin, vor allem junge Menschen zu sensibilisieren, positive und negative Auswirkungen von Big Data-Anwendungen zu erkennen und Position zu beziehen – bestenfalls durch kritische Reflexion des eigenen Verhaltens, z. B. in sozialen Netzwerken.
Neben der inhaltlichen Weiterentwicklung soll auch die Handhabung der Mediendatenbank verbessert werden. Hierzu hat der TLfDI Kontakt zu Informatik-Studenten der Erfurter Fachhochschule gesucht, die mit ihren Programmierkenntnissen bereit sind, die technische Weiterentwicklung der Software voranzutreiben. So ist geplant, dass Anfang 2018 auch eine Version 2.0 der Mediendatenbank online gehen kann.

Der Schutz der Privatsphäre im Medienzeitalter muss ein wesentlicher Bildungsbestandteil in der Schule sein. Mit der Mediendatenbank stellte der TLfDI ein wichtiges Werkzeug für Lehrkräfte zur Unterstützung der Medienkompetenzentwicklung ihrer Schüler ins Netz. Die Internetseite https://medien.tlfdi.de wurde 2017 inhaltlich aktualisiert und auch technisch weiterentwickelt. Zu Beginn des Jahres 2018 soll eine Version 2.0 online gehen.

16.29 Nutzung sozialer Netzwerke und Messenger-Dienste in Schulen oft problematisch

Wie in diesem Tätigkeitsbericht unter Punkt 16.15 ausführlich dargestellt, sprach der Thüringer Landesbeauftragte für den Datenschutz

und die Informationsfreiheit (TLfDI) einer Schule gemäß § 39 Thüringer Datenschutzgesetz (ThürDSG) eine Beanstandung aus, weil dort eine Lehrkraft eine Schülerin auf Facebook bloßgestellt hatte. Bei dieser Gelegenheit wies der TLfDI die Schule auf die datenschutzrechtliche Unzulässigkeit einer Nutzung der weit verbreiteten sozialen Netzwerke und Messenger-Dienste zu dienstlichen Zwecken der Schule hin.

Einige Zeit später wandte sich die Thüringer Staatskanzlei an den TLfDI, weil dessen Hinweis zum Umgang mit den einschlägigen sozialen Netzwerken und Messenger-Diensten, welcher über das Thüringer Ministerium für Bildung, Jugend und Sport (TMBJS) an alle staatlichen Schulen des Freistaats Thüringen kommuniziert worden war, zu Aufregungen in mehreren Schulen geführt habe. Aus diesem Grund schlug die Thüringer Staatskanzlei dem TLfDI die Durchführung einer gemeinsamen Fachveranstaltung zur dienstlichen Nutzung von sozialen Netzwerken und Messenger-Diensten in der Schule mit dem TMBJS, dem Thüringer Institut für Lehrerfortbildung, Lehrplanentwicklung und Medien (ThILLM) sowie den staatlichen Schulämtern vor. Der TLfDI griff den Vorschlag gerne auf und lud die Gesprächspartner zu einer Fachberatung in seine Dienststelle ein. In einem Einführungsvortrag legte der TLfDI nochmals ausführlich dar, dass mit seinem Hinweis an die Schulen, weder die einschlägigen sozialen Netzwerke, noch Messenger-Dienste für die dienstliche Kommunikation einzusetzen, diejenigen Produkte angesprochen sind, die üblicherweise eine hohe Verbreitung haben und deshalb vorzugsweise für den Kommunikationsaustausch verwendet werden. Es handelt sich bei diesen sozialen Netzwerken und Messenger-Diensten um Telekommunikationsdienste, die geltende europäische und deutsche Rechtsvorschriften nicht beachten oder zumindest das Verfahren nicht ausreichend dokumentieren. Eine Nutzeranalyse zu Zwecken der Werbung, bei der z. B. Standortdaten, Daten darüber, wer mit wem, wann und wie lange kommuniziert, ist bei einer dienstlichen Nutzung aus datenschutzrechtlicher Sicht nicht hinnehmbar. Von diesen Messenger-Diensten ist darüber hinaus bekannt, dass nach einer erfolgten Anmeldung alle in dem verwendeten Smartphone gespeicherten Kontaktdaten abgeglichen werden. Die Verwendung solcher Kommunikationsdienste zu dienstlichen Zwecken ist aus datenschutzrechtlicher Sicht als eine Datenverarbeitung im Auftrag nach § 8 ThürDSG anzusehen. Nach § 8 Abs. 1 ThürDSG bleibt die Schule als Auftraggeber für die Ein-

haltung der Bestimmungen dieses Gesetzes und anderer Vorschriften über den Datenschutz verantwortlich. Diese Verantwortung kann die Schule jedoch nicht wahrnehmen, da kein Einfluss auf die Datenverarbeitung bei den Messenger-Diensten geltend gemacht werden kann. Dies bedeutet jedoch nicht, dass pauschal eine Verwendung von modernen Kommunikationsdiensten zu dienstlichen Zwecken in der Schule datenschutzrechtlich grundsätzlich unzulässig ist. Kann ein Kommunikationsdienst einen datenschutzgerechten Kommunikationsaustausch gewährleisten, darf dieser auch in der Schule eingesetzt werden. Ergänzend stellte der TLfDI klar, dass selbstverständlich keine Einwände gegen eine Behandlung von sozialen Netzwerken und Messenger-Diensten als Unterrichtsgegenstand bestehen.

Als Ergebnis der Fachveranstaltung konnte der TLfDI positiv überrascht feststellen, dass sich alle Gesprächspartner über die Unzulässigkeit der Nutzung von den angesprochenen sozialen Netzwerken und Messenger-Diensten durch Lehrkräfte für die Kommunikation zu dienstlichen Zwecken einig waren. Einige Gesprächspartner hatten die ihrer Auffassung nach begründete Vermutung, dass einige Lehrkräfte soziale Netzwerke oder Messenger-Dienste aus Unwissenheit oder aus Unüberlegtheit für den Kontakt untereinander oder mit Schülern und Eltern einsetzen. Es gebe auch Elternsprecher, die die Lehrkräfte ausdrücklich zur Nutzung von WhatsApp auffordern.

Im Rahmen der Vermittlung von Medienkompetenz können soziale Netzwerke oder Messenger-Dienste zum Unterrichtsgegenstand gemacht werden. Dies sollte aber nur auf schuleigenen Rechnern bzw. mobilen Geräten und unter Verwendung von fiktiven personenbezogenen Daten erfolgen.

Der TLfDI wird mit Beratung und Unterstützung der Teilnehmer der Fachveranstaltung ein Informationsblatt für Schulleiter und Lehrkräfte zur Nutzung von sozialen Netzwerken und Messenger-Diensten erstellen und auf seiner Homepage veröffentlichen. Die Verteilung der Informationsschrift soll dann bei Veranstaltungen für Schulleiter und Lehrkräfte verteilt werden.

Zusätzlich ist die Erstellung einer FAQ-Liste geplant, die datenschutzrechtliche Fragen von Schulleitern und Lehrkräften sammelt und diese auch beantwortet.

Der TLfDI hatte alle an der beschriebenen Fachveranstaltung beteiligten Institutionen um eine entsprechende Zuarbeit gebeten. Da die Rückmeldungen bisher sehr schleppend erfolgten, wurden die Stellen nochmals um eine entsprechende Zuarbeit gebeten.

Lehrkräfte dürfen soziale Netzwerke und Messenger-Dienste für die dienstliche Kommunikation nur dann nutzen, wenn die Schule sich von der datenschutzrechtlichen Zulässigkeit des Dienstes überzeugt hat. Die derzeit am häufigsten vertretenen und mutmaßlich auch für Schulzwecke verwendeten Produkte erfüllen diese Anforderungen nicht.

16.30 Zweites Gesetz zur Änderung des Thüringer Erwachsenenbildungsgesetzes

Werden in speziellen Gesetzen konkrete Regelungen zum Datenschutz getroffen, dann gehen diese Festlegungen dem Thüringer Datenschutzgesetz (ThürDSG) bzw. dem Bundesdatenschutzgesetz (BDSG) vor oder ergänzen diese. Dieser Grundsatz ist sinnvoll, weil ThürDSG und BDSG zwangsläufig allgemein gehalten sind und keinesfalls alle Fälle zum Schutz der Privatsphäre des einzelnen Bürgers abdecken können, die gegenwärtig relevant sind oder zukünftig relevant werden könnten. Der Gesetzgeber und die Ressorts, die ein Gesetz oder eine Verordnung zur Verabschiedung im Landtag vorbereiten, sind deshalb gut beraten, wenn sie im Zuge der Erarbeitung von Rechtsgrundlagen den Schutz der Privatsphäre jener Personen „mitdenken“, die von den Regelungen betroffen sein werden. Gut beraten sind auch jene Ressorts, die den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) in die Prüfung von Gesetzentwürfen einbeziehen, so, wie das im Zuge der Novellierung des Thüringer Erwachsenenbildungsgesetzes im Jahr 2016 geschehen ist. Das für die Erarbeitung zuständige Ministerium für Bildung, Jugend und Sport (TMBJS) leitete dem TLfDI den Entwurf des Zweiten Gesetzes zur Änderung des Thüringer Erwachsenenbildungsgesetzes im Rahmen der öffentlichen Anhörung zu und bat den TLfDI um Stellungnahme. Der TLfDI regte in seiner Stellungnahme eine ergänzende Formulierung an, die auf die Berücksichtigung des Datenschutzrechtes im Zusammenhang mit der Durchführung von Qualitätsmanagementverfahren abstellt.
Bei der Erarbeitung der zugehörigen Verordnung unterstützte der TLfDI das TMBJS bei Festlegungen zur Aufbewahrungsdauer von Unterlagen im Zusammenhang mit der staatlichen Anerkennung von Erwachsenenbildungseinrichtungen durch das zuständige Ministerium. Derartige Unterlagen enthalten regelmäßig personenbezogene

Daten, die nach Erfüllung einer Aufgabe – hier durch das TMBJS selbst – zu löschen sind.
Beide Fälle zeigen Weitblick und datenschutzrechtliche Sensibilität des TMBJS. Der TLfDI begrüßt derartige Anfragen ausdrücklich, da mit frühzeitiger Beratung durch die Datenschutzbehörde spätere Probleme inkl. Rechtsstreitigkeiten vermieden werden können.

Spezielle Rechtsgrundlagen – hier für den Erwachsenenbildungsbereich – können Regelungen zum Datenschutz enthalten, die dem Thüringer Datenschutzgesetz bzw. dem Bundesdatenschutzgesetz vorgehen oder diese ergänzen. An der Gesetzgebung beteiligte Institutionen (z. B. Ministerien) können die datenschutzrechtliche Beratung des TLfDI durch Prüfung von Gesetz- und Verordnungsentwürfen in Anspruch nehmen, wie im Fall des TMBJS geschehen. Der TLfDI begrüßt dies ausdrücklich.

16.31 PISA-Feldtest 2017

Wenn Politik steuern soll, braucht es Fakten, statt Vermutungen. Schulleistungstests und Befragungen, vor allem internationale, liefern solche Entscheidungsgrundlagen. Nicht zuletzt profitieren die Schulen selbst vom Spiegelbild ihrer Bildungsarbeit. Dass dabei praktisch immer personenbezogene Daten von Lehrern, Schülern und Eltern mit im Spiel sind, leuchtet ein. Umso wichtiger ist, dass der Schutz der Privatsphäre aller Betroffenen von Anfang an in derartige Evaluationen „eingebaut“ wird. Das Thüringer Schulgesetz (ThürSchulG) stellt hierzu klare Weichen. Im § 57 ThürSchulG ist die Zulässigkeit über die Verarbeitung und Nutzung personenbezogener Daten in Schulen, bei Schulträgern und Schulaufsichtsbehörden geregelt, auch für wissenschaftliche Forschungsvorhaben (Absatz 5) und internationale, nationale und regionale Vergleichsuntersuchungen (Absatz 6). Im Frühjahr 2017 stand nun ein Feldtest im Rahmen der internationalen PISA-Studien (Programme for International Student Assessment) auch in Thüringen Schulen an. So war es notwendig und folgerichtig, dass das für die Durchführung zuständige Institut vor derartigen Erhebungen beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) prüfen lässt, ob die erforderlichen Datenschutzhinweise in den Unterlagen für den PISA-Feldtest sowie die begleitende Elternbefragung enthalten und deutlich erkennbar sind. Die Prüfung ergab, dass die enthal-

tenen Hinweise, z. B. zur Teilnahme-Freiwilligkeit an der Elternbefragung, zur Einwilligung der Eltern und zur Möglichkeit ihres Widerrufs ausreichend sind. Außerdem wurden die erhobenen Daten anonymisiert. Deshalb bestanden aus Sicht des TLfDI keine Bedenken gegen die Erhebung. Dies wurde dem Institut sowie dem Thüringer Ministerium für Bildung, Jugend und Sport mitgeteilt.

Das für die internationale PISA-Studie zuständige Institut wandte sich im Zusammenhang mit dem PISA-Feldtest 2017 an den TLfDI und bat um datenschutzrechtliche Prüfung der Erfassungsunterlagen, die an Lehrer, Schüler und Eltern gerichtet werden sollten. Im Ergebnis hatte der TLfDI keine datenschutzrechtlichen Bedenken. Die enthaltenen Hinweise, z. B. zur Freiwilligkeit der Teilnahme an der Elternbefragung, zur Einwilligung und zum Widerruf derselben, waren ausreichend und verständlich.

16.32 Gesundheitsvorsorge in der Schule: Welche Daten darf die Schule dem Gesundheitsamt im Vorfeld übermitteln?

Der Schulleiter einer freien Ganztagsgrundschule und freien Gesamtschule bat den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) um eine Information zur Datenübermittlung im Rahmen der schulischen Gesundheitsvorsorge. Der Schulleiter legte dar, dass das Gesundheitsamt im Vorfeld der turnusmäßigen Schuluntersuchung darum gebeten habe, von Schülern mit sonderpädagogischen Förderbedarfen die individuellen Bedarfe zu übermitteln. Der Schulleiter bat um Information, ob mit dieser Übermittlung ggf. berechtigte Interessen der betreffenden Schüler bzw. deren Sorgenberechtigten verletzt werden könnten oder ob es unbedenklich sei, wenn diese Information schriftlich oder per Mail (Datei-Anhang) an das Gesundheitsamt gesandt werde.
Der TLfDI prüfte den vorgetragenen Sachverhalt anhand der entsprechenden Regelungen in der Verordnung über die Thüringer Schulgesundheitspflege (ThürSchulgespflVO) auf seine datenschutzrechtliche Zulässigkeit. Grundsätzlich konnte der TLfDI aus den Vorschriften der ThürSchulgespflVO keine ausdrückliche Ermächtigung entnehmen, dass die Schulen dem Gesundheitsamt im Rahmen von schulärztlichen Vorsorgeuntersuchungen für jeden Schüler die konkreten Förderbedarfe übermitteln müssen. Unabhängig davon hielt der TLfDI das Erheben der sonderpädagogischen Förderbedarfe

bei den Schulen durch die Thüringer Gesundheitsämter grundsätzlich für zulässig. Der TLfDI begründete seine Auffassung zur Übermittlungspflicht damit, dass § 1 Abs. 4 ThürSchulGespflVO keine konkreten Mitwirkungspflichten der Schulen enthält. Auch fehlt eine Regelung, wonach die Schulen die konkreten sonderpädagogischen Förderbedarfe von Schülern zur Vorbereitung der Vorsorgeuntersuchungen übermitteln müssen. Aus dem Gebrauch des Wortes „insbesondere“ in § 2 Abs. 1 Satz 2 ThürSchulGespflVO ergibt sich lediglich ein Hinweis darauf, dass die Aufzählung der Modalitäten von Vorsorgeuntersuchungen nicht als abschließend anzusehen ist, eine präzise Anordnung fehlt hingegen.

Dennoch ist die Kenntnis der genauen Förderbedarfe zur Erfüllung der schulärztlichen Vorsorgeuntersuchung erforderlich, insbesondere, um den zeitlichen Umfang der Untersuchung und die notwendigen Untersuchungsmaterialien einzuschätzen und entsprechend bereitzuhalten. Bei Kindern mit besonderem Förderbedarf (beispielsweise geistige Retardierung mit oder ohne körperliche Behinderung) dauert die schulärztliche Untersuchung bedeutend länger, da diese Kinder nicht in der Form kooperieren (können) wie nicht-behinderte Kinder. Aus der Art der Behinderung ergibt sich der Förderbedarf, der auf die Kooperationsfähigkeit der Kinder im Rahmen der Untersuchung hinweist und sich insofern auf die Dauer, den Umfang und die Art der Untersuchung auswirkt. Somit ist das Erheben der sonderpädagogischen Förderbedarfe bei den Schulen durch die Thüringer Gesundheitsämter in diesem Zusammenhang zulässig, da gemäß § 19 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) das Erheben personenbezogener Daten zulässig ist, wenn ihre Kenntnis zur Erfüllung der Aufgaben der erhebenden Stelle erforderlich ist.

Im Hinblick darauf wies der TLfDI den Schulleiter darauf hin, dass aus Datenschutzgründen jedoch weder die Schülerlisten noch die einzelnen sonderpädagogischen Förderbedarfe ohne Weiteres per E-Mail von den Schulen an das Gesundheitsamt übermittelt werden dürfen. Im Sinne von § 9 Abs. 2 ThürDSG ist die Übertragung unverschlüsselter E-Mails im Hinblick auf die Vertraulichkeit, die Integrität und die Zugriffsmöglichkeit durch Dritte als unsicher einzuschätzen. Daher müssen personenbezogene Daten entweder konventionell auf postalischem Wege oder als verschlüsselte E-Mails versendet werden.

Über das Ergebnis seiner Prüfung informierte der TLfDI auch das Gesundheitsamt. Weiterhin wies der TLfDI darauf hin, dass das

Gesundheitsamt gemäß § 19 Abs. 4 ThürDSG die Schulen in freier oder kirchlicher Trägerschaft auf die Freiwilligkeit der Angaben bzw. auf die Rechtsvorschrift hinweisen muss, die zur Auskunft verpflichtet. Jedoch ist der ThürSchulGespflVO keine Auskunftspflicht zu entnehmen.

Gemäß § 19 Abs. 1 ThürDSG ist das Erheben personenbezogener Daten zulässig, wenn ihre Kenntnis zur Erfüllung der Aufgaben der erhebenden Stelle erforderlich ist. Das Erheben der sonderpädagogischen Förderbedarfe bei den Schulen durch die Thüringer Gesundheitsämter zur Vorbereitung von Vorsorgeuntersuchungen ist grundsätzlich zulässig, insbesondere, um den zeitlichen Umfang der Untersuchung und die notwendigen Untersuchungsmaterialien einschätzen zu können. Werden personenbezogene Daten statt beim Betroffenen bei einer nicht-öffentlichen Stelle erhoben, so ist die Stelle auf die Rechtsvorschrift, die zur Auskunft verpflichtet, sonst auf die Freiwilligkeit ihrer Angaben hinzuweisen (§ 19 Abs. 4 ThürDSG).

16.33 Erweiterte Sozialdatenerhebung im Rahmen der Schuleingangsuntersuchung – Ausforschung von Kind und Eltern durch den Gesundheitsdienst oder sinnvolle Ergänzung zur Gesundheitsvorsorge der Bevölkerung?

Im Rahmen der Schuleingangsuntersuchung müssen die Eltern des Kindes einen Erhebungsbogen ausfüllen, der zahlreiche Fragen zu bekannten und durchgestandenen Krankheiten des Kindes, aber auch derjenigen der Großeltern, Eltern und Geschwister, dem Geburts- und Entwicklungsverlauf sowie Gesundheitsstörungen des Kindes enthält. Bereits in der Vergangenheit hatte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) zu einigen personenbezogene Daten, die mit dem Bogen erhoben werden, infrage gestellt, ob deren Erhebung im Einklang mit den Regelungen der Thüringer Verordnung über die Schulgesundheitspflege (ThürSchulgespflVO) steht. Daraufhin wurde die Beantwortung einiger Fragen ausdrücklich als freiwillig gekennzeichnet. Hierzu gehört die Angabe des Berufs und zum Migrationshintergrund der Eltern.
Der Fachdienst Gesundheit eines Landratsamtes trat mit der Bitte um eine datenschutzrechtliche Beurteilung einer Erweiterung des Anamnese-Fragebogens an den TLfDI heran. Dabei soll der auf freiwilli-

ger Basis auszufüllende Ergänzungsbogen zum Migrationshintergrund des einzuschulenden Kindes um weitere Fragen zum familiären Hintergrund des Kindes ergänzt werden. Der TLfDI teilte dem Fachdienst Gesundheit mit, dass aus datenschutzrechtlicher Sicht gemäß § 4 Abs. 1 Thüringer Datenschutzgesetz die Verarbeitung und Nutzung personenbezogener Daten nur zulässig ist, wenn dieses Gesetz oder eine andere Rechtsvorschrift sie erlaubt oder anordnet oder soweit der Betroffene eingewilligt hat. Nach § 8 Abs. 1 ThürSchulgespflVO darf das Gesundheitsamt zur Erfüllung der ihm aufgrund dieser Verordnung zugewiesenen Aufgaben die dafür erforderlichen Daten verarbeiten und nutzen. Diese Aufgaben sind insbesondere in den in § 1 ThürSchulGespflVO Grundsätzen allgemein beschrieben. Diesen Vorschriften ist nicht unmittelbar zu entnehmen, ob die Erfassung des Migrations- und Familienhintergrunds für die Aufgabenerfüllung der Gesundheitsämter erforderlich ist. Der Zusatzfragebogen dient nicht der Feststellung des Gesundheitszustandes des einzuschulenden Kindes, sondern der Klärung eines gesundheitspolitischen Sachverhalts.

Im Ergebnis hielt der TLfDI die Ergänzung des bereits zusätzlichen Fragebogens „Einheitliche Erfassung Migrationshintergrund“ um vier weitere Fragestellungen (zum Familientyp, zur Sprachanwendung im Elternhaus, zum höchsten Berufsabschluss der Eltern und zur anteiligen Erwerbsbeteiligung der Eltern) nur dann für zulässig, wenn das Ausfüllen dieses Zusatzbogens auf freiwilliger Basis erfolgt und die Eltern hierauf sowie auf den Zweck der Verarbeitung ausdrücklich hingewiesen werden. Das als Fachaufsichtsbehörde für die Gesundheitsämter zuständige Thüringer Landesverwaltungsamt wurde über die Auffassung des TLfDI ebenfalls unterrichtet. Zusätzlich wies der TLfDI darauf hin, dass der ausführlichere Fragebogen-Entwurf in keiner Weise die datenschutzrechtlichen Anforderungen, auf welche Weise auf die Freiwilligkeit der Preisgabe von Daten hingewiesen werden muss, erfüllt. Auf dem Erhebungsbogen muss darauf hingewiesen werden, dass eine Auskunftspflicht nicht besteht und der Betroffene auch die Auskunft verweigern kann, ohne dass ihm hierdurch Nachteile entstehen. Als Vorschlag für einen Mustertext verwies der TLfDI auf die, allerdings inzwischen nicht mehr gültigen Hinweise des Thüringer Innenministeriums zum Thüringer Datenschutzgesetz (ThürDSG) – Fassung des ThürDSG vom 10. Oktober 2001 zu § 19 unter 19.1 Nr. 3: „… *wenn keine Rechtsvorschrift den Betroffenen zur Angabe verpflichtet und die Daten*

nicht zur Bearbeitung eines Antrages des Betroffenen erforderlich sind: Hinweis nach § 19 Abs. 3 des Thüringer Datenschutzgesetzes: Die Angaben (in Nummer ... dieses Vordrucks) sind freiwillig. Sie werden benötigt, um ... Die Daten werden an ... übermittelt. Sie können von diesen Angaben absehen, ohne Rechtsnachteile befürchten zu müssen.“ Keinesfalls genügt es, die auf Freiwilligkeit beruhende Beantwortung von Fragen lediglich mit zwei Sternchen ** zu kennzeichnen und vermutlich in einer Fußnote hierauf hinzuweisen. Nach Kenntnis des TLfDI verzichten die Gesundheitsämter der Landkreise und kreisfreien Städte bisher auf den erweiterten Bogen zur einheitlichen Erfassung des Migrationshintergrunds.

Die Gesundheitsämter dürfen für die Schuleingangsuntersuchung im Rahmen der Schulgesundheitspflege personenbezogene Daten bei den Erziehungsberechtigten mit einem Fragebogen erheben. Fragen, die nicht der Erfassung des Gesundheitszustands und der Bewertung der Schulfähigkeit des Kindes dienen, sondern bei dieser Gelegenheit zur Erledigung gesundheitspolitischer Sachverhalte erhoben werden, sind als freiwillige Angaben zu kennzeichnen.

16.34 Schulaufsichtliche Prüfung – doppelt hält besser?

Die Überprüfungen von Schulen, die Forderung von Berichten, Nachweisen, Statistiken gehören zum normalen Aufgabenspektrum von Schulaufsichtsbehörden, auch der staatlichen Schulämter in Thüringen. Für die betroffenen Schulen sind das zusätzliche Belastungen, die neben der Gewährleistung des Unterrichtsbetriebs zu bewältigen sind. Nicht jede dieser Maßnahmen ist den Schulen immer plausibel, zumal, wenn sich Prüfungen in einer bestimmten Schule häufen oder/und nicht ausreichend begründet werden.
Dass auch datenschutzrechtliche Aspekte durch schulaufsichtliche Überprüfungen berührt sein können, beweist der Fall einer Thüringer Grundschule. Der Schulleiter wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) mit datenschutzrechtlichen Bedenken: Eine erneute Sprachstandserhebung bei den Schülern solle durchgeführt werden, obwohl eine solche bereits im gleichen Schuljahr wenige Monate zuvor stattgefunden habe und die Ergebnisse beim Schulamt vorlägen. Doppelte Arbeit also und zudem ein Verstoß gegen den Grundsatz der Datensparsamkeit nach Ansicht des Schulleiters. Zudem beklagte der

Schulleiter, dass er Unterlagen des Fördervereins, dessen Vorsitzender er war, sowie Unterlagen zur Haushaltsführung an das Schulamt übergeben sollte. Hierfür sah er keine Rechtsgrundlage. Der TLfDI nahm mit dem zuständigen Schulamt Kontakt auf und bat um Stellungnahme. Insbesondere war hier zu prüfen, ob die vom Schulamt angeforderten Unterlagen personenbezogene Daten enthielten. Falls dies zuträfe, sei deren Erforderlichkeit nachzuweisen, um die Zulässigkeit der Datenübermittlung gemäß § 21 Thüringer Datenschutzgesetz (ThürDSG) zu belegen. Das war insbesondere im Zusammenhang mit den Unterlagen vom Schulförderverein von Interesse.
Die Angelegenheit verlor erfreulicherweise an Brisanz, weil das zuständige Schulamt die schulaufsichtliche Prüfung kurzfristig absagte. Es wurden keine Unterlagen an das Schulamt übergeben, sodass schon deshalb keine datenschutzrechtlichen Verstöße entstehen konnten.
Was wäre, wenn die Überprüfung stattgefunden hätte? Aus den Aussagen des Schulamtsleiters kam der TLfDI zu dem Schluss, dass eine nochmalige Überprüfung der Sprachstände keinen datenschutzrechtlichen Verstoß darstellen würde. Eine solche Maßnahme liegt im Rahmen der gesetzlich geregelten Fachaufsicht des Schulamtes und kann erforderlich sein, um festzustellen, ob bestimmte Förderleistungen korrekt vergeben werden. Anders bei der Übermittlung von Fördervereinsunterlagen. Hier stellte der TLfDI gegenüber dem Schulamtsleiter unmissverständlich klar, dass eine Trennung zwischen der Schulleitertätigkeit einer Person und ihrer Tätigkeit im Förderverein geboten ist. Im Ergebnis sei es aus datenschutzrechtlicher Sicht weder erforderlich noch zulässig gewesen, den Schulleiter zur Erteilung von Auskünften über seine Tätigkeit als Vorsitzender des Schulfördervereins aufzufordern. Der TLfDI bat das Schulamt um zukünftige Beachtung.

Im Zusammenhang mit einer Prüfung einer Schule durch das zuständige Schulamt war für den TLfDI zu klären, ob eine wiederholte Erfassung und Übermittlung von personenbezogenen Daten – hier von Sprachständen von Schülern – erforderlich ist. Darüber hinaus prüfte der TLfDI, ob es datenschutzrechtlich zulässig ist, wenn ein Schulamt vom Schulleiter Unterlagen fordert, die seine Tätigkeit im Schulförderverein betreffen. Im ersten Fall bestand kein datenschutzrechtlicher Verstoß. Im zweiten Fall stellte der TLfDI klar, dass eine

Anforderung von Unterlagen des Fördervereins durch das Schulamt datenschutzrechtlich weder erforderlich noch zulässig ist.

16.35 Schule stellt Schülern E-Mail-Adressen zur Verfügung – Klasse, oder?

Unter den Thüringer Lehrern gibt es etliche, die sehr kreative Wege suchen, um den Schülern Kompetenzen im Bereich von Medienkunde zu vermitteln. So wandte sich ein Lehrer an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), der darüber nachdachte, dass den Schülern ab der 7. Klasse im Rahmen des Medienkundeunterrichts eine eigene E-Mail-Adresse von der Schule eingerichtet werden soll. Dabei sollte der Internetprovider genutzt werden, den auch alle Lehrer verwenden. Er fragte, ob hiergegen aus datenschutzrechtlicher Sicht Bedenken bestehen.
Der TLfDI teilte zunächst mit, dass ihm grundsätzlich keine rechtlichen Altersbeschränkungen bei der Nutzung von E-Mail-Adressen bekannt sind. Falls die E-Mail-Adressen ausschließlich zu Unterrichtszwecken vergeben und nur schuleigene Rechner verwendet werden, ist darüber hinaus auch keine Einwilligung der Erziehungsberechtigten erforderlich. Am wenigsten problematisch ist es, wenn die Schule die E-Mail-Accounts selbst auf einem eigenen Mailserver verwaltet. Im Missbrauchsfall hat die Schule unmittelbaren Zugriff auf den Server und kann den Zugang löschen bzw. deaktivieren. Außerdem ist damit die technische Trennung von schulischen Belangen und privater Kommunikation für die Schüler besser gewährleistet.
Aus datenschutzrechtlicher Sicht als bedenklich einzuschätzen ist hingegen die schulische Nutzung von privaten E- Mail-Diensten. Hier findet eine Datenverarbeitung im Auftrag (gemäß § 8 Thüringer Datenschutzgesetz) statt, die von der Schule vertraglich zu regeln ist. Die Schule bleibt hierbei für die Einhaltung datenschutzrechtlicher Vorschriften verantwortlich. Die E-Mail-Accounts können nur individuell verwaltet werden und unterliegen somit nicht der Kontrolle der Schule. Daher kann die Nutzung durch die Schule nicht kontrolliert werden. Im Missbrauchsfall kann die Schule den Zugang nicht löschen bzw. deaktivieren.
Im vorliegenden Fall war vorgesehen, dass die E-Mail-Adressen der Schüler aus dem Schülervor- und -nachnamen sowie aus der Domain der Schule gebildet werden. Diese Domain gehört dem Träger der

Schule, wird aber durch ein privates Telekommunikationsunternehmen gehostet.
Somit ergibt sich für die E-Mail-Account-Verwaltung Folgendes: Die Schule verwaltet die E-Mail-Accounts nicht unmittelbar auf einem eigenen Server, da die Verwaltung seitens des Trägers erfolgt. Es ist der Schule aber möglich, über vertragliche Vereinbarungen mit dem Träger bei Missbrauchsverhalten einzelner Schüler die E-Mail-Adresse zu löschen oder zu deaktivieren. Außerdem hat das Telekommunikationsunternehmen seinen Geschäftssitz und Serverstandort in Deutschland. Es kann darauf vertraut werden, dass die verfassungsrechtlichen, telekommunikationsrechtlichen und datenschutzrechtlichen Regelungen befolgt werden.
Im Ergebnis bestanden in diesem Fall keine grundsätzlichen datenschutzrechtlichen Bedenken gegen die Vergabe von E-Mail-Adressen an alle Schüler der Klassenstufe 7 zu schulischen Zwecken, also insbesondere zur Vermittlung von Medienkompetenz.
Dabei wurde davon ausgegangen, dass es den Schülern nur möglich ist, auf den Computern der Schule auf das E-Mail-Programm zuzugreifen und E-Mail-Nachrichten nur dort zu versenden und zu empfangen. Die Schüler sind darüber zu unterrichten, dass das Nutzen der vergebenen Accounts nur schulischen Zwecken dient und eine private E-Mail-Nutzung ausgeschlossen ist. Ebenso sind die Schüler über die Gefahren aufzuklären, die sich aus der E-Mail-Kommunikation ergeben können (z. B. hinsichtlich der Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität usw. von E-Mail-Nachrichten). Der Zugriff auf das eigene E-Mail-Postfach sollte jedem Schüler nur mit der Benutzerkennung und einem ausreichend sicheren Passwort möglich sein. Was ein sicheres Passwort ist, wird in der Maßnahme M 2.11 „Regelung des Passwortgebrauchs“ des Bundesamtes für Sicherheit in der Informationstechnologie (BSI) näher beschrieben
(vgl:
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02011.html;jsessionid=0FCD22A55BF5A85596880FAED25BFE5F.2_cid368?nn=6610622).

Es kann die Medienkompetenz von Schülern fördern, wenn ihnen von der Schule eigene Mail-Adressen zur Verfügung gestellt werden, die auf schulischen Rechnern zu schulischen Zwecken verwendet werden. Wichtig ist dabei, dass es der Schule möglich ist, in den Fällen einzugreifen, in denen Missbrauch mit den Mail-Adressen betrieben wird.

16.36 Klassenbuch und Co.

Fragen kann nicht schaden! Der Austausch von Rechtspositionen und Erfahrungen zwischen Sachverständigen – hier zu Fragen des Datenschutzes – sind insbesondere dann sinnvoll, wenn es länderübergreifend um ähnliche Probleme geht. Da kann der Blick in die Praxis eines anderen Bundeslandes schon mal hilfreich im Hinblick auf weitgehend einheitliches Handeln sein, sofern Landesrecht dem nicht entgegensteht. So wandte sich eine Datenschutz-Beratungsfirma aus Bayern an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) mit zwei Fragen, die den Datenschutz in Schulen betreffen und bat um fachliche Einschätzung. Beschrieben wurde der Fall, dass in Schulen Schülerlisten mit Schülernamen, Klassenstufe und Raumnummern in Fenstern des Schulgebäudes so angebracht werden, dass von außen jedermann Zugang zu diesen Informationen erlangen kann. Die Beratungsfirma fragte an, ob in Thüringen Festlegungen hierzu im Thüringer Schulrecht bzw. im Landesdatenschutzgesetz beständen. Der TLfDI antwortete hierzu, dass es in Thüringen weder eine erlaubende Rechtsgrundlage gibt, noch eine Einwilligung von Schülerinnen, Schülern bzw. Erziehungsberechtigten eine hinreichende Rechtsgrundlage hierfür bietet. Ergänzend teilte der TLfDI mit, dass seinerseits keine datenschutzrechtlichen Bedenken für den Fall beständen, wenn die Veröffentlichung innerschulisch und zeitlich begrenzt erfolge und sie nicht ohne Weiteres von unberechtigten Personen einsehbar wäre. Die Veröffentlichung müsse zudem der Organisation des Schulbetriebs dienen.
Der zweite Fall der Anfrage betraf das altbekannte Klassenbuch und dessen Transport im Schulalltag durch Schüler. Klar, dass die Verantwortung bei der jeweiligen Lehrkraft liegt. Zumeist würde jedoch doch die Obhut bei Schülerinnen oder Schülern aus der Klasse liegen. Der Beratungsfirma sei häufig zugetragen worden, dass dabei Klassenbücher zeitweise oder gänzlich verloren gingen. Die Bera-

tungsfirma legte dem TLfDI ihre Rechtsauffassung dar, dass es sich dabei um eine potenzielle Offenlegung sensibler Daten an Dritte handelt, aus welcher zudem „schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen“ nach § 42a Bundesdatenschutzgesetz (BDSG) resultieren könnten. Zudem bewegte die Beratungsfirma die Frage, ob für es für öffentliche Schulen (gemeint sind hier staatliche Schulen in Thüringen, für die das Thüringer Schulgesetz in Verbindung mit dem Thüringer Datenschutzgesetz [ThürDSG] einschlägig ist) eine Informationspflicht analog zu den Festlegungen von § 42a BDSG gibt. Der TLfDI antwortete, dass das ThürDSG eine entsprechende Informationspflicht nicht enthält. Somit müssen die öffentlichen Stellen in Thüringen eine unrechtmäßige Kenntniserlangung nach derzeit geltendem Recht nicht melden. Das eigentliche Problem mit dem Klassenbuchtransport durch Schüler stellt aus datenschutzrechtlicher Sicht einen Verstoß der Schule gegen die datenschutzrechtlichen Bestimmungen dar. Nach § 9 Abs. 1 ThürDSG hat sie die erforderlichen technischen und organisatorischen Maßnahmen zu treffen, um die datenschutzrechtlichen Vorgaben zu erfüllen. Keine Frage, dass das im Zusammenhang mit sensiblen Schülerdaten besonders bedeutsam ist. Transportieren Schüler das Klassenbuch von einem Klassenraum in einen anderen oder geben diese das Klassenbuch nach Stundenende an der dafür vorgesehenen Stelle ab, so kann die Schule nicht gewährleisten, dass nur Befugte die im Klassenbuch gespeicherten personenbezogenen Daten zur Kenntnis nehmen können, die Daten nicht manipuliert werden oder sogar ein Verlust des Klassenbuchs erfolgt. Die Schule hat aber gemäß § 9 Abs. 2 ThürDSG insbesondere die Vertraulichkeit, die Integrität, die Verfügbarkeit und die Authentizität der personenbezogenen Daten zu gewährleisten.

Es ist unzulässig, wenn in Schulen Schülerlisten mit Schülernamen, Klassenstufe und Raumnummern in Fenstern des Schulgebäudes so angebracht werden, dass von außen jedermann Zugang zu diesen Informationen erlangen kann. Keine datenschutzrechtlichen Bedenken bestehen hingegen, wenn die Veröffentlichung innerschulisch und zeitlich begrenzt erfolgt und sie nicht ohne weiteres von unberechtigten Personen einsehbar ist.
Der Transport von Klassenbüchern hat durch die Lehrkräfte zu erfolgen. Schüler dürfen nicht zu dieser Aufgabe herangezogen werden.

16.37 Big Brother in der Schule? Unterrichtsvideografie in der Lehrerausbildung

Ein Institut für Erziehungswissenschaften wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und bat um Informationen zu den Thüringer Datenschutzregelungen der Unterrichtsvideografie in der Lehrerausbildung. Die Institutsmitarbeiter legten dar, dass sich die Universität, zu der das Institut gehört, im Rahmen der „Qualitätsoffensive Lehrerbildung" des Bundesministeriums für Bildung und Forschung (BMBF) mit verschiedenen Maßnahmen zur Verbesserung der Lehrerausbildung befasse. Im Teilprojekt „Virtuelle Hospitation" soll angehenden Lehrern erfolgreiche „Reflektierte Handlungsfähigkeit" vermittelt werden. Dazu werden als Unterrichtsdokumentationen Bild-, Ton- und Videoaufnahmen von Schülern und Lehrern angefertigt (multimediale Unterrichtsdokumentation). Diese Unterrichtsdokumentationen sollen ausschließlich zum Zweck der wissenschaftlichen Lehre und Forschung verwertet werden. Dabei ist der Einsatz der Videoaufnahmen insbesondere in der Lehrerausbildung vorgesehen. Angehenden Lehrern sollen die Unterrichtsdokumentationen als Lehrmaterialien zur Verfügung gestellt werden.
Die bestehenden bundeseinheitlichen Regelungen hinsichtlich des Allgemeinen Persönlichkeitsrechts, Urheberrechts, bürgerlichen Rechts und Datenschutzrechts wurden von Seiten der Universität bereits berücksichtigt. Darüber hinaus bestehen in den Bundesländern jedoch weitergehende unterschiedliche rechtliche Rahmenbedingungen für solche Videoaufzeichnungen in Schulen. Daher übersandten die Institutsmitarbeiter dem TLfDI einen Fragebogen, um festzustellen, wie die entsprechenden Thüringer Regelungen (Landesgesetze/Verwaltungsvorschriften, ministeriale/dienstliche Weisungen) ausgestaltet sind.
Der TLfDI beantwortete diese Fragen folgendermaßen:
Unterrichtsdokumentationen in Form von Video-,Bild- und Tonaufnahmen zu Forschungs- und Ausbildungszwecken innerhalb von Schulen sind unter bestimmten Voraussetzungen möglich: Die direkt von den Aufnahmen betroffenen Lehrer, Schüler und Eltern müssen gemäß § 4 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) ihr Einverständnis zu den Aufnahmen erklären. Weiterhin müssen folgende Stellen ebenfalls ihr Einverständnis erklären: das Thüringer Ministe-

rium für Bildung, Jugend und Sport (TMBJS) gemäß § 57 Abs. 5 Thüringer Schulgesetz (ThürSchulG) sowie der oder die jeweilige/n Schulleiter/in gemäß § 56 Abs. 1 ThürSchulG. Die Aufnahmen einsichtsfähiger oder gar volljähriger Schüler zum Zweck der Forschung oder Lehre sind grundsätzlich erlaubt, wenn deren Einverständniserklärung sowie die der Lehrer vorliegt und die o. g. Stellen nach ThürSchulG ihr Einverständnis ebenfalls erklärt haben. Aufnahmen von minderjährigen Schülern bzw. Kindern für die o. g. Zwecke sind grundsätzlich erlaubt, wenn die entsprechenden Einverständniserklärungen der Eltern vorliegen gemäß § 57 Abs. 10 ThürSchulG in Verbindung mit § 4 Abs. 1 und Abs. 2 ThürDSG. Nach § 57 Abs. 10 ThürSchulG sind ergänzend die Regelungen des § 25 ThürDSG zur Verarbeitung und Nutzung der personenbezogenen Daten durch Forschungseinrichtungen zu beachten. So müssen sich z. B. Stellen, auf die die das ThürDSG keine Anwendung findet, vertraglich zur Einhaltung der Zweckbindung verpflichten. Außerdem sind Daten zu anonymisieren, sobald dies nach dem Forschungszweck möglich ist. Auch nach dieser Vorschrift besteht eine Ausnahme von der Anonymisierungspflicht dann, wenn der Betroffene ausdrücklich in die Veröffentlichung seiner Daten eingewilligt hat.

In den Einverständniserklärungen muss darauf hingewiesen werden, dass die schriftlich erteilte Zustimmung zur Nutzung der Dokumente jederzeit widerrufen werden kann. § 4 Abs. 2 ThürDSG impliziert auch diese Widerspruchsmöglichkeit. Im Rahmen der Einverständniserklärung kann ein Recht auf die nachträgliche Bearbeitung der Aufnahmen (z. B. ergänzende Kommentierung) mit übertragen werden. Eine Klausel zur Duldung einer Weiterübertragung der Nutzungsrechte an Dritte (z. B. im Rahmen einer Publikation) ist im Rahmen der Einverständniserklärung nicht zulässig. Hierfür müsste eine gesonderte Einwilligung bzw. vertragliche Gestaltung mit den Rechteinhabern erfolgen. Eine Verwertung kann nur mit Zustimmung aller Miturheber erfolgen. Eine Widerspruchsmöglichkeit ist jedoch dann i. d. R. nicht mehr gegeben.

Für die erstellten Unterrichtsdokumentationen wird keine konkrete, inhaltliche, räumliche oder zeitliche Verwertungsoption verlangt. Ebenso bestehen keine speziellen Löschauflagen jenseits der gesetzlichen Regelungen. Die direkt oder indirekt an den Aufnahmen Beteiligten (Lehrpersonen, Eltern, einsichtsfähige Kinder) können gemäß § 4 Abs. 2 ThürDSG gegenüber der Universität ihre Einwilli-

gung in eine zeitliche, räumliche und inhaltliche Nutzung an den Unterrichtsdokumentationen geben oder einer entsprechenden Nutzung widersprechen.

Unterrichtsdokumentationen in Form von Video-, Bild- und Tonaufnahmen zu Forschungs- und Ausbildungszwecken innerhalb von Schulen sind nicht grundsätzlich unzulässig. Neben den direkt von den Aufnahmen betroffenen Lehrern, Schülern und Eltern müssen folgende Stellen ebenfalls ihr Einverständnis erklären: das Thüringer Ministerium für Bildung, Jugend und Sport (TMBJS) gemäß § 57 Abs. 5 Thüringer Schulgesetz (ThürSchulG) sowie der oder die jeweilige Schulleiter/in gemäß § 56 Abs. 1 ThürSchulG. Im Hinblick auf die Datensicherheit sind gemäß § 9 ThürDSG „die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes zu gewährleisten."

16.38 Beschwerde über eine Schule in Bezug auf die Inanspruchnahme des Bildung- und Teilhabepaketes – Die finanzielle Situation des Elternhauses geht Dritte nichts an

Die Mutter eines Schulkindes beschwerte sich beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) darüber, dass im Zusammenhang mit der Nutzung des Bildungs- und Teilhabepakets – es handelt sich hierbei um die Gewährung von Leistungen nach § 28 Zweites Sozialgesetzbuch und § 34 Zwölftes Sozialgesetzbuch im Rahmen von schulischen und außerschulischen Veranstaltungen, wie Schulausflüge, Schülerbeförderung, Lernförderung, Schulessen, Mitgliedsbeiträge in den Bereichen Sport, Kultur, Kunst usw. – das Schulpersonal im Umgang mit den personenbezogenen Daten des betroffenen Kindes dessen informationelles Selbstbestimmungsrecht verletzt habe und bat um Auskunft, welche Möglichkeiten der TLfDI habe, dieses Verhalten zu unterbinden und zu sanktionieren. Die Beschwerdeführerin trug vor, dass verschiedene Lehrer ihr Kind im Treppenhaus der Schule im Beisein von weiteren Schülern ansprechen und es z. B. auf noch nicht vom Sozialamt an die Schule überwiesene Gelder hinweisen. Hierdurch werde für eine bewusste oder unbewusste Ausgrenzung ihres Kindes gesorgt, weil seine Klassenkameraden über die finanzielle Situation des Schülers Kenntnis bekommen.

Der TLfDI teilte der Beschwerdeführerin zunächst mit, dass in dem von ihr geschilderten Sachverhalt eine Übermittlung von personenbezogenen, teilweise sensiblen Daten an Dritte vorliegt. Eine Übermittlung personenbezogener Daten an Dritte ist nur unter den in § 57 Abs. 4 Thüringer Schulgesetz genannten Bedingungen zulässig, die hier aber nicht vorlagen. Der Beschwerdeführerin wurde mitgeteilt, dass sich der TLfDI an die Schule wenden und unter Bekanntgabe des Namens des Schülers und der geschilderten Sachverhalte zu einer Stellungnahme auffordern müsse. Falls sich die Angaben des Schülers entsprechend bestätigen würden, so hat der TLfDI die Möglichkeit, das Verhalten der Schule gemäß § 39 Thüringer Datenschutzgesetz (ThürDSG) zu beanstanden und das als Aufsichtsbehörde zuständige staatliche Schulamt hierüber zu verständigen. Die Beschwerdeführerin wurde gebeten, dem TLfDI den Namen ihres Kindes, die Klassenstufe, die Namen der beteiligten Lehrkräfte und den Zeitpunkt der Vorfälle mitzuteilen. Ebenfalls wurde sie darauf aufmerksam gemacht, dass ihr Kind sich in jedem Fall mit einer eigenen Eingabe an den TLfDI wenden müsse, falls dieses bereits volljährig ist. Bei der Anrufung des TLfDI gemäß § 11 ThürDSG handelt es sich um ein Betroffenenrecht, welches höchstpersönlich vorgetragen werden muss. Die Beschwerdeführerin meldete sich zwar nicht mehr, der TLfDI hat aber die Schule angeschrieben und gebeten, alle Lehrkräfte darauf hinzuweisen, dass personenbezogene Daten, die Dritte nichts angehen, nicht laut im Schulflur oder im Rahmen einer Unterrichtsstunde besprochen werden.

Führen Lehrkräfte mit Schülern persönliche Gespräche, so muss ausgeschlossen sein, dass Dritte vom Inhalt des Gesprächs Kenntnis erlangen können. Ansonsten liegt hierin eine Verletzung von § 57 Abs. 4 Thüringer Schulgesetz, wonach eine Übermittlung personenbezogener Daten an Dritte nur unter den dort abschließend genannten Ausnahmen zulässig ist.

16.39 Wann dürfen Prüfungsunterlagen kopiert und Prüfungsergebnisse weitergegeben werden?

Eine Auszubildende beschwerte sich beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) darüber, dass ein Fachreferat des Thüringer Landesverwaltungsamtes (TLVwA) im Rahmen des Verfahrens zur Berufsanerkennung der

Auszubildenden ihre personenbezogenen Daten an einen medizinischen Weiterbildungsträger übermittelt habe. Die Beschwerdeführerin gab an, dass sie über die Datenübermittlung durch das TLVwA nicht in Kenntnis gesetzt wurde und dass die Übermittlung nicht erforderlich gewesen sei, da die Berufsanerkennung zum Zeitpunkt der Datenübermittlung noch nicht geklärt war. Weiterhin wandte sich die Beschwerdeführerin gegen die Weigerung des TLVwA, ihr eine Kopie ihrer Prüfungsunterlagen zukommen zu lassen. Die Beschwerdeführerin war der Auffassung, dass ihr die Kopie ihrer Daten zustünde. Der TLfDI bat das TLVwA um eine Stellungnahme zu dem vorgetragenen Sachverhalt.

Das TLVwA teilte mit, dass die Beschwerdeführerin sich in gleicher Angelegenheit bereits an den behördlichen Datenschutzbeauftragten (bDSB) des TLVwA gewandt und von diesem zwischenzeitlich Antwort erhalten hatte. Diese Antwort übersandte das TLVwA dem TLfDI. Darin wies der bDSB den Vorwurf der unbefugten Weitergabe von personenbezogenen Daten an ein medizinisches Weiterbildungsunternehmen zurück. Er legte dar, dass lediglich ein Gespräch mit dem Bildungswerk für Gesundheitsberufe in Erfurt stattgefunden habe. Hingegen hätten keine Gespräche zwischen Mitarbeitern des zuständigen Fachreferats vom TLVwA und dem medizinischen Weiterbildungsunternehmen stattgefunden, in denen personenbezogene Daten der auszubildenden Beschwerdeführerin mitgeteilt worden seien. Somit lag nach Darstellung des bDSB kein Verstoß gegen § 43 Abs. 1 Nr. 1 Thüringer Datenschutzgesetz (ThürDSG) vor, da keine personenbezogenen Daten „übermittelt“ wurden. Es konnte jedoch nicht ausgeschlossen werden, dass das Bildungswerk mit dem Weiterbildungsträger kommuniziert und entsprechende Daten übermittelt hat.

Die von der Beschwerdeführerin erbetene Kopie ihrer Prüfungsunterlagen hatte das TLVwA mit Verweis auf § 14 Satz 1 der Ausbildungs- und Prüfungsverordnung für Masseure und medizinische Bademeister (MB-APrV) zurückgewiesen und dies damit begründet, dass der Betroffenen schließlich die Einsichtnahme in die Prüfungsunterlagen zustehe und sich somit eine Kopie erübrige. Weiterhin wies das TLVwA darauf hin, dass der Beschwerdeführerin Prüfungsbescheide bereits schriftlich zugegangen seien.

Nach Auswertung dieser Ausführungen teilte der TLfDI der Beschwerdeführerin mit, dass durch das TLVwA keine Daten widerrechtlich weitergegeben wurden und aus datenschutzrechtlicher Sicht

für den TLfDI auch keine Anhaltspunkte dafür bestehen, diese Darlegung anzuzweifeln. Im Hinblick auf die von ihr erbetene Kopie der Prüfungsunterlagen legte der TLfDI gegenüber der Beschwerdeführerin dar, dass er die hierzu vom TLVwA gezogene Schlussfolgerung nicht teilt. Aus datenschutzrechtlicher Sicht schließt das Recht auf Einsichtnahme nach der MB-APrV die Erstellung und Aushändigung einer Kopie nicht aus (vgl. u. a. BGH Iva ARZ (VZ) 9/88 und OLG Schleswig 12 VA 6/08). Da in den Unterlagen nur für die Betroffenen bestimmte Daten enthalten sind, besteht aus datenschutzrechtlicher Sicht kein Grund, dass Ablichtungen nicht angefertigt werden dürfen. Dieses Ergebnis teilte er auch der Beschwerdeführerin mit, wies aber darauf hin, dass die Behörde von ihr die Erstattung der entstehenden Kosten verlangen kann.

Das Recht auf Akteneinsicht schließt die Erstellung und Aushändigung einer Kopie. an den Betroffenen nicht aus. Aus datenschutzrechtlicher Sicht ist es unbedenklich, wenn nur personenbezogene Daten des Betroffenen kopiert werden. Die Behörde kann allerdings die entstandenen Kosten der Fertigung der Kopien ersetzt verlangen.

16.40 Fotoaufnahmen beim Projekttag – „Entweder du lässt dich fotografieren oder du darfst nicht mitmachen!“

Eltern beschwerten sich beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) über den an einer Grundschule im Rahmen des Schulunterrichts durchgeführten Projekttag, der zum Thema Essen und Bewegung von der Stiftung einer Handelskette veranstaltet wurde. Im Vorfeld waren die Eltern um eine schriftliche Foto- und Videoerlaubnis gebeten worden, die dem TLfDI von den Beschwerdeführern in Kopie zugesandt wurde. Der TLfDI wandte sich daraufhin unter Hinweis auf § 56 Abs. 1 Nr. 2 Thüringer Schulgesetz (ThürSchulG), wonach die Zustimmung zu Bild-, Film-, Fernseh- und Tonaufnahmen bei Veranstaltungen in der Schule das schriftliche Einverständnis der Eltern nach Unterrichtung über das Vorhaben voraussetzt, an die Schulleitung. Wie die Betreuung von Kindern erfolgen sollte, deren Eltern keine Einwilligung in die Foto- Film- und Tonaufnahmen erteilt hatten, war den Betroffenen nicht bekannt. Sie fühlten sich jedenfalls unter Druck gesetzt, ebenfalls eine Einwilligung zu erteilen, damit ihr Kind von den Klassenkameraden nicht als Außenseiter angesehen wird. Die Schule

erklärte in ihrer Stellungnahme, dass es sich bei der Einwilligungserklärung um ein gemeinsames Schriftstück der Stiftung und der Schule gehandelt habe. Außerdem sei keinem Kind ein Nachteil entstanden, wenn eine entsprechende Foto- und Filmerlaubnis der Eltern nicht vorgelegen habe, da man in diesem Fall so fotografiert bzw. gefilmt habe, dass das betroffene Kind nicht mit aufgenommen wurde. Es sei grundsätzlich kein Kind von der Veranstaltung ausgeschlossen worden.
Nach erneuter Prüfung der Einwilligung unter Zugrundelegung der Stellungnahme der Schulleitung kam der TLfDI zum Ergebnis, dass inhaltlich eine schriftlich einzuholende Einwilligung die in § 4 Abs. 3 Thüringer Datenschutz (ThürDSG) festgelegten Kriterien erfüllen muss. Der Text der vorliegenden Einwilligung erfüllte nicht in ausreichendem Maße die geforderte Informationspflicht. Dies betraf z. B. die genaue Zweckbestimmung sowie die Auskunft über die voraussichtliche Dauer der Speicherung der Fotos. Da die Aufnahmen von der privaten Stiftung verarbeitet und genutzt wurden, waren darüber hinaus die Betroffenen über ihre Widerrufsmöglichkeit zu informieren. Da die Aufnahmen zumindest im weiteren Sinn für Werbemaßnahmen genutzt werden konnten und hierauf auch in der Einwilligung hingewiesen wurde, wäre nach § 3a Bundesdatenschutzgesetz in der Einverständniserklärung darauf hinzuweisen gewesen, dass die Einwilligung mit Wirkung für die Zukunft widerrufen werden kann. Einen wesentlichen datenschutzrechtlichen Verstoß der Schule sah der TLfDI aber nicht, da der Zweck der Fotoaufnahmen aufgrund des Einverständnistextes nahelag und in erster Linie die Stiftung die entsprechenden Textteile hinsichtlich der Speicherdauer und der Widerrufsmöglichkeit der Schule hätte zuarbeiten müssen. Der Beschwerdeführer wurde hierüber abschließend unterrichtet. Die datenschutzrechtliche Bewertung der inhaltlichen Gestaltung der von der Stiftung formulierten Einwilligung unterlag hingegen nicht dem TLfDI, sondern der für diese Stiftung zuständigen Aufsichtsbehörde für den Datenschutz, an die sich der Beschwerdeführer ebenfalls gewandt hatte.

Gem. § 56 Abs. 1 Nr. 2 ThürSchulG setzt die Zustimmung zu Bild-, Film-, Fernseh- und Tonaufnahmen bei Veranstaltungen in der Schule das schriftliche Einverständnis der Eltern nach Unterrichtung über das Vorhaben voraus. Die von einer privaten Stiftung erstellte entsprechende Einwilligung darf nicht von der Schule ungeprüft über-

nommen und mit dem Aufdruck des Schulstempels als gemeinsame Einwilligung den Eltern vorgelegt werden. Die Schule muss bei der Formulierung der Einwilligung die in § 4 Abs. 3 ThürDSG festgelegten Kriterien beachten.

16.41 Einschulungsuntersuchung: Datenschutz in der Schulgesundheitspflege

2016 führte das Thüringer Landesverwaltungsamt (TLVwA) eine Revision aller Formbögen des schulärztlichen Dienstes der Thüringer Gesundheitsämter durch. Anschließend übersandte das TLVwA die aktualisierten Formbögen an das Thüringer Ministerium für Arbeit, Soziales, Gesundheit, Frauen und Familie (TMASGFF) mit der Bitte um Genehmigung gemäß § 3 der Thüringer Verordnung zur Schulgesundheitspflege (ThürSchulgespflVO). Parallel dazu übersandte das TLVwA die Formbögen an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) mit der Bitte um datenschutzrechtliche Prüfung.
Die Einladung und Anamneseerhebung zur Einschulungsuntersuchung (ESU) wurden im Rahmen der Revision hinsichtlich fachlicher Gesichtspunkte aktualisiert. Der Formbogen „Standardisierte Erhebung Migrationshintergrund“ sollte vorrangig im Rahmen der ESU angewendet werden, ist aber auch für alle anderen Untersuchungen des Kinder- und Jugendärztlichen Dienstes (KJÄD) nutzbar. Er wurde im Hinblick auf datenschutzrechtliche Vorgaben und fachliche Aspekte überarbeitet.
Der TLfDI prüfte die Formbögen und sah nur im Hinblick auf einen Umstand Änderungsbedarf: In Thüringen erfolgt die Erfassung des Migrationshintergrundes zur Einschulungsuntersuchung auf freiwilliger Basis bereits seit dem Schuljahr 2015/16. Im ESU-Erhebungsbogen zum Migrationshintergrund wird hinsichtlich der freiwilligen Teilnahme auf § 4 Thüringer Datenschutzgesetz (ThürDSG) verwiesen. Dies ist jedoch nicht richtig. Die speziellere Regelung zur Erhebung findet sich in § 19 Abs. 3 ThürDSG. Im Sinne des § 19 Abs. 3 ThürDSG könnte und sollte folgender Hinweis im Formbogen formuliert werden: *„Wir bitten um Kenntnisnahme des Hinweises nach § 19 Abs. 3 Thüringer Datenschutzgesetz: Die Angaben im Vordruck sind freiwillig. Sie werden benötigt, um … Die Daten werden an … übermittelt. Sie können von diesen Angaben absehen, ohne Rechtsnachteile befürchten zu müssen.“*

Der TLfDI bat das TLVwA um eine entsprechende Korrektur des Fragebogens zur Erfassung des Migrationshintergrundes und um die Übersendung des geänderten Formbogens. Das TLVwA informierte im Oktober 2016 das TMASGFF über die vorgenommenen Änderungen des Formbogens zur Erhebung des Migrationshintergrunds und setzte auch den TLfDI entsprechend in Kenntnis.
Der TLfDI bestätigte die nunmehr datenschutzrechtlich korrekte Fassung des Formbogens. Daraufhin wurden die Formbögen vom TMASGFF gemäß § 3 ThürSchulgespflVO genehmigt. Im November 2016 übersandte das TLVwA die Formbögen an den KJÄD der Landratsämter. Die Nutzung sollte bereits ab der Einschulungsuntersuchung des Schuljahres 2016/17 erfolgen.

Die Verordnung zur Schulgesundheitspflege in Thüringen sieht vor, dass im Rahmen der Einschulungsuntersuchung eine Erhebung zum Gesundheitszustand der Schulanfänger erfolgt. Dabei wird auch der Migrationshintergrund erfasst. In die entsprechenden Formbögen zur Einschulungsuntersuchung ist gemäß § 19 Abs. 3 ThürDSG der Hinweis zur Freiwilligkeit der Angaben aufzunehmen und darzulegen, wofür die Daten erhoben bzw. benötigt werden und an wen sie übermittelt werden.

16.42 Einbehalten von Klassenarbeiten von Schülern der 9. und 10. Klasse

In einer Eingabe beschwerten sich Eltern beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) darüber, dass einige Lehrkräfte korrigierte Klassenarbeiten an die Kinder nicht aushändigen, sondern die Kinder lediglich einen Blick in die Arbeit und auf die erhaltene Zensur bekommen. Auch das Anfertigen von Kopien der Klassenarbeiten oder das Abfotografieren mit dem Handy sei den Kindern nicht erlaubt worden. Die Eltern erhalten damit keine Rückmeldung darüber, welche Themen abgefragt wurden und welchen Leistungsstand die Kinder haben. Die Eltern baten um Klärung, ob mit dieser Verfahrensweise nicht gegen datenschutzrechtliche Bestimmungen verstoßen wird, da es sich bei den Arbeiten um personenbezogene Daten der Kinder handele. Es war den Eltern auch unklar, wo und wie lange die Klassenarbeiten in der Schule aufbewahrt werden müssen und aus welcher Rechtsgrundlage sich dies ergibt.

Der TLfDI schrieb zur Klärung des Sachverhalts das Thüringer Ministerium für Bildung, Jugend und Sport (TMBJS) an und bat um Mitteilung, welche Regelungen dort zur Rückgabe von Klassenarbeiten und schriftlichen Tests sowie zur Aufbewahrung von Klassenarbeiten im Kultusbereich erlassen wurden. In seiner Antwort verwies das Ministerium auf § 31 Abs. 2 Thüringer Schulgesetz (ThürSchulG), wonach die Eltern gegenüber der Schule ein Recht auf Auskunft über die schulische Entwicklung und den Leistungsstand des Schülers haben. Um diesem Auskunftsanspruch nachzukommen, seien die Klassenarbeiten den Eltern zur Kenntnisnahme vorzulegen. Weiterhin sind gemäß § 6 Abs. 3 Satz 2 der Dienstordnung für Lehrer, Erzieher und Sonderpädagogische Fachkräfte an den staatlichen Schulen Klassenarbeiten für zwei Jahre in der Schule aufzubewahren. Aus diesem Grund müssen die Klassenarbeiten nach der Kenntnisnahme durch die Eltern von den Fachlehrerinnen und -lehrern wieder eingesammelt und verwahrt werden. Hintergrund für diese Regelung sei, dass bei möglichen Streitigkeiten über nachfolgende Versetzungsentscheidungen deren Rechtmäßigkeit sich im Wesentlichen nur anhand der Überprüfung der Klassenarbeiten belegen lasse. Falls in Einzelfällen zur Kenntnisnahme ausgegebene Klassenarbeiten von Schülern nicht wieder an die Schule zurückgegeben werden, könne die Schule aber zur Erfüllung ihrer Dokumentationspflicht entscheiden, bis auf Weiteres die Einsichtnahme von Klassenarbeiten des betroffenen Schülers für ihn und für die Eltern nur noch in der Schule zu ermöglichen. Ausdrücklich wies das TMBJS auf das Recht der Eltern hin, gemäß § 29 Thüringer Verwaltungsverfahrensgesetz Klassenarbeiten auch bildlich, sei es durch Anfertigen einer Kopie oder durch Abfotografieren, festzuhalten. Das TMBJS bat den TLfDI für eine schulaufsichtliche Aufarbeitung um Mitteilung, welche Schule die Kenntnisnahme von Klassenarbeiten gegenüber den Kindern und den Eltern verweigerte. In der Antwort an die Beschwerdeführer bat der TLfDI diese um Benennung der betroffenen Schule, um dies an das Ministerium weiterzureichen. Der TLfDI unterrichtete das TMBJS abschließend darüber, dass der Name der Schule von den Beschwerdeführern trotz Nachfrage nicht genannt wurde und daher eine konkrete Verfolgung des Sachverhalts für das TMBJS nicht möglich ist. Der TLfDI bat deshalb das TMBJS, alle Schulen entsprechend darüber zu unterrichten, dass es zulässig ist, wenn Schüler sich Kopien oder Fotos von ihren Klassen- bzw. Kursarbeiten anfertigen.

Eltern und Schüler haben gegenüber der Schule das aus § 31 Abs. 2 ThürSchulG abzuleitende Recht auf Einsichtnahme in die korrigierten Klassenarbeiten. Dies schließt die Erstellung von Kopien oder Fotos der Arbeiten ein. Die ausgegebenen Arbeiten werden von der Schule wieder eingesammelt und für zwei Jahre dort aufbewahrt. Lediglich in Fällen, in denen sich Schüler oder Eltern weigern, die Klassenarbeiten wieder zurückzugeben, kann die Schule von einer Ausreichung der Arbeiten absehen und den Schülern und Eltern die Einsichtnahme lediglich in der Schule ermöglichen.

16.43 Unterstützung von Amtsärzten durch niedergelassene Ärzte verstößt grundsätzlich nicht gegen den Datenschutz

Im Zusammenhang mit der geplanten Verbeamtung von Lehrern in Thüringen berichtete eine Thüringer Zeitung darüber, dass rund 30 niedergelassene Ärzte mit dem zuständigen Ministerium eine Vereinbarung unterzeichnet hätten, um die vorgeschriebenen ärztlichen Untersuchungen der Lehrkräfte durchzuführen. In der Regel werden diese Untersuchungen durch die örtlichen, mit sogenannten hoheitlichen Aufgaben betrauten Amtsärzte durchgeführt. Die Frage, ob bzw. wann es zulässig ist, dass niedergelassene Ärzte die Aufgaben von Amtsärzten wahrnehmen, war bereits Gegenstand im 9. Tätigkeitsbericht 2010/2011 unter Nummer 11.5 im Zusammenhang mit schulzahnärztlichen Reihenuntersuchungen. Für die Verbeamtung von Lehrkräften ist das Thüringer Ministerium für Bildung, Jugend und Sport (TMBJS) zuständig. Daher bat der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) das TMBJS um Auskunft darüber, auf welcher Rechtsgrundlage freiberuflich tätige Ärzte anstelle von Amtsärzten mit der Untersuchung betraut wurden.
Das TMBJS teilte dem TLfDI in seiner Stellungnahme mit, dass für die Verbeamtung gemäß § 8 Abs. 2 des Thüringer Laufbahngesetzes (ThürLaufbG) die gesundheitliche Eignung aufgrund einer ärztlichen Untersuchung festzustellen ist. Gemäß § 33 Abs. 1 Satz 1 Thüringer Beamtengesetz (ThürBG) können *„angeordnete ärztliche Untersuchungen“* auch von *„sonstigen von der zuständigen Stelle bestimmten Ärzten durchgeführt“* werden. Von dieser Regelung hatte das TMBJS Gebrauch gemacht und hierfür einen Pool von niedergelassenen Ärzten festgelegt. Die zur Verbeamtung vorgesehenen Lehre-

rinnen und Lehrer hatten, bezogen auf diesen Ärztepool, grundsätzlich freie Arztwahl. Nach Auffassung des TLfDI ist die durch das TMBJS getroffene Regelung datenschutzrechtlich unbedenklich, da es hier, anders als bei der schulzahnärztlichen Untersuchung, eine gesetzliche Ermächtigung gibt. Voraussetzung ist aber, dass die entsprechenden ärztlichen Untersuchungen (schriftlich) angeordnet werden.

Gemäß § 33 Abs. 1 Satz 1 Thüringer Beamtengesetz (ThürBG) können angeordnete ärztliche Untersuchungen auch von „sonstigen von der zuständigen Stelle bestimmten Ärzten durchgeführt‘ werden. Sofern die zuständige Stelle entsprechende Ärzte bestimmt und die Untersuchung zur Feststellung der gesundheitlichen Eignung gemäß § 8 Abs. 2 des Thüringer Laufbahngesetzes (ThürLaufbG) angeordnet ist, ist die Durchführung durch niedergelassene Ärzte anstelle von Amtsärzten datenschutzrechtlich grundsätzlich unbedenklich.



Online Security Technology © GKSD / Fotolia.com

17. Technische Entwicklung allgemein

17.1 Datenschutz beim Bürger-Konto (Servicekonto)

Im Juli 2017 wurde per Grundgesetzänderung u. a. dem Artikel 91 c des Grundgesetzes ein neuer Absatz 5 angefügt. Dieser regelt, dass der übergreifende informationstechnische Zugang zu den Verwaltungsleistungen von Bund und Ländern durch Bundesgesetz mit Zustimmung des Bundesrates geregelt wird (BGBl Nr. 47 vom 19. Juli 2017). Durch diese Änderung erhielt der Bund die Gesetzgebungskompetenz zur Ausgestaltung des Zugangs zu den Verwaltungsleistungen von Bund und Ländern. Nach Angaben des Bundesministeriums des Innern soll dadurch in Deutschland ein modernes E-Government Einzug halten. Die Verwaltungsportale aller Behörden in Bund und Ländern werden nun zu einem „Portalverbund“, das heißt zu einem „virtuellen Portal“ verknüpft. Das entsprechende Bundesgesetz heißt Onlinezugangsgesetz (OZG) und ist im Bundesgesetzblatt Nr. 57 vom 17. August 2017 veröffentlicht.
Damit Nutzer die Verwaltungsportale nutzen können, muss ein Nutzerkonto eingerichtet sein. Bund und Länder haben dazu jeweils eine öffentliche Stelle zu bestimmen, die den Nutzern die Einrichtung eines Nutzerkontos anbietet (§ 7 OZG). Welche Daten bei natürlichen Personen und bei juristischen Personen dazu erfasst werden

dürfen, regelt § 8 OZG. Dieses Nutzerkonto wird übrigens oft auch „Service-Konto“ oder „Bürger-Konto“ genannt.
Die 91. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder hatte bereits im April 2016 eine Entschließung „Datenschutz bei Servicekonten“ verabschiedet. Anlass war seinerzeit die Tatsache, dass sich der IT-Planungsrat in seiner 17. Sitzung im Juni 2015 für eine flächendeckende Verbreitung sogenannter Servicekonten für Bürgerinnen und Bürger und Unternehmen ausgesprochen hatte, um die Inanspruchnahme von Verwaltungsdienstleistungen zu verbessern. So wies die Konferenz u. a. darauf hin, dass dabei das Verbot einer Vorratsdatenspeicherung zu unbestimmten Zwecken sowie das grundrechtliche Prinzip der informationellen Gewaltenteilung zu beachten ist. Auch dürften Servicekonten nicht die gesetzliche Zuständigkeits- und Aufgabenverteilung der öffentlichen Verwaltung unterlaufen. Weiterhin muss den Bürgerinnen und Bürgern die Möglichkeit eingeräumt werden, sowohl einzelne im permanenten Servicekonto dauerhaft gespeicherte personenbezogene Daten als auch das Konto selbst löschen zu lassen. Wichtig war der Konferenz ebenfalls, dass Verwaltungsdienstleistungen künftig auch ohne Servicekonto in Anspruch genommen werden können. Die komplette Entschließung mit den datenschutzrechtlichen Forderungen kann in der Anlage 2 nachgelesen werden.

Mit dem Onlinezugangsgesetz wurde u. a. die rechtliche Grundlage gelegt, Verwaltungsportale aller Behörden in Bund und Ländern zu einem Portalverbund zusammenzuschließen. Die in den einzelnen Verwaltungsportalen angelegten Nutzerkonnten für die Bürgerinnen und Bürger, die oft auch als Servicekonten bezeichnet werden, müssen allerdings datenschutzrechtlichen Bestimmungen genügen.

17.2 Speicherung von IP-Adressen – Sicherheit oder Datenschutz?

Ob dynamische oder statische IP-Adressen personenbezogene Daten im Sinne des Datenschutzrechtes sind oder nicht, darüber urteilten, seitdem es Websiten gibt, die jeweiligen Gerichte in den einzelnen Bundesländern recht unterschiedlich. Die Datenschutzbeauftragten des Bundes und der Länder standen aus ihrer Sicht dabei immer auf dem Standpunkt, dass statische IP-Adressen personenbezogen sind und zumindest bei dynamischen IP-Adressen u. U. ein Personenbe-

zug herstellbar sei. Aber unter den jeweiligen Gerichten in den Bundesländern gab es hierzu keine einheitliche Rechtsauffassung.
So muss man fast von Glück reden, dass es eine Klage in dieser Sache vor ein paar Jahren bis zum Bundesgerichtshof (BGH) geschafft hatte. Herr Patrick Breyer, Parteimitglied der Piraten-Partei, hatte geklagt, dass Einrichtungen des Bundes seine Internetprotokoll-Adressen (IP-Adressen) beim Zugriff auf ihre Websites aufzeichnen und speichern. Das Amtsgericht Tiergarten wies die Klage 2008 ab (AZ 2 C 6/08), wogegen Herr Breyer Berufung einlegte. Gegen das nachfolgende Urteil aus dem Jahr 2013 vom Landgericht Berlin wurde Revision eingelegt, sodass es beim BGH landete.
Der BGH entschied in seinem Beschluss vom 28. Oktober 2014 (Beschl. v. 28. Oktober 2014, Az. VI ZR 135/13), das Verfahren auszusetzen und den Europäischen Gerichtshof (EuGH) zwecks Klärung zweier Fragen zu bitten.
Dabei war entsprechend der Informationen des EuGH Folgendes zu klären:

1.) Ob in diesem Zusammenhang auch „dynamische“ IP-Adressen für den Betreiber der Website personenbezogene Daten darstellen, sodass sie den für solche Daten vorgesehenen Schutz genießen. Eine „dynamische“ IP-Adresse ist eine IP-Adresse, die sich bei jeder neuen Internetverbindung ändert. Anders als statische IP-Adressen erlauben dynamische IP-Adressen es nicht, anhand allgemein zugänglicher Dateien eine Verbindung zwischen einem Computer und dem vom Internetzugangsanbieter verwendeten physischen Netzanschluss herzustellen. Somit verfügt ausschließlich der Internetzugangsanbieter von Herrn Breyer über die zu dessen Identifizierung erforderlichen Zusatzinformationen.
2.) Ferner wollte der BGH wissen, ob der Betreiber einer Website zumindest grundsätzlich die Möglichkeit haben muss, personenbezogene Daten der Nutzer zu erheben und zu verwenden, um die generelle Funktionsfähigkeit seiner Website zu gewährleisten. Der BGH wies insoweit darauf hin, dass die einschlägige deutsche Regelung von der deutschen Lehre überwiegend dahin ausgelegt werde, dass die Daten am Ende des jeweiligen Nutzungsvorgangs zu löschen seien, soweit sie nicht für Abrechnungszwecke benötigt würden.

Zwei Jahre später, am 19. Oktober 2016, entschied der EuGH über diese zwei Fragen (Rechtsache C-582/14):

Zu 1.) Eine dynamische Internetprotokoll-Adresse stellt ein personenbezogenes Datum für den Websiten-Anbieter dann dar, wenn er über rechtliche Mittel verfügt, die es ihm erlauben, die betreffende Person anhand der Zusatzinformationen, über die der Internetzugangsanbieter dieser Person verfügt, bestimmen zu lassen.
Dies bedeutet, er muss rechtlich die Möglichkeit haben, den Internetzugangsanbieter zwecks Zusatzinformationen abfragen zu dürfen. Diese Möglichkeit besteht beispielsweise im Fall von „Cyberattacken“, bei dem ein Strafverfahren eingeleitet werden kann.
Zu 2.) Eine Regelung eines Mitgliedsstaats, wonach IP-Adressen nur zu Abrechnungszwecken längerfristig gespeichert werden dürfen, sei in Bezug auf Art. 7 Buchstabe f der europäischen Datenschutz-Richtlinie europarechtswidrig. Eine nationale Regelung darf nicht die Verarbeitung bestimmter Kategorien personenbezogener Daten ausschließen, indem sie für diese Kategorien das Ergebnis der Abwägung abschließend vorschreibt, ohne Raum für ein Ergebnis zu lassen, das aufgrund besonderer Umstände des Einzelfalls anders ausfällt. Daher stellt sich die Frage, ob § 15 Telemediengesetz (TMG) richtlinienkonform dahin ausgelegt werden muss, dass bei der Sicherstellung der Funktion des Telemediums über die Nutzungsdauer hinaus personenbezogene Daten Verwendung finden dürfen, soweit und solange die Verwendung zu diesem Zweck erforderlich ist.
Am 15. Mai 2017 traf dann der BGH, aufgrund der Einschätzung des EuGH, folgende Entscheidung (VI ZR 135/13):
Zu 1.) Die dynamische IP-Adresse, die von einem Anbieter von Online-Mediendiensten beim Zugriff auf eine Internetseite, die dieser Anbieter allgemein zugänglich macht, gespeichert wird, stellt für den Anbieter ein personenbezogenes Datum dar.
Zu 2.) § 15 Abs. 1 TMG ist nun dahingehend auszulegen, dass Anbieter von Online-Mediendiensten personenbezogene Daten eines Nutzers dieser Dienste ohne dessen Einwilligung auch über das Ende eines Nutzungsvorgangs hinaus dann erheben dürfen, soweit ihre Erhebung und ihre Verwendung erforderlich sind, um die generelle Funktionsfähigkeit des Dienstes zu gewährleisten, wobei es allerdings einer Abwägung mit dem Interesse und den Grundrechten und -freiheiten der Nutzer bedarf.
Allerdings sieht der BGH diese notwendige Abwägung im Streitfall beim Landgericht Berlin nicht geprüft. Für diese Abwägung ist vor allem das Angriffsrisiko auf Anbieterseiten sowie die Schwere des

Eingriffs in das informationelle Selbstbestimmungsrecht des Nutzers entscheidend.
Der BGH verwies den Fall schließlich wieder zurück an das Landgericht Berlin.

Dynamische IP-Adressen stellen ein personenbezogenes Datum dar. § 15 Abs. 1 Telemediengesetz ist dahingehend auszulegen, dass Anbieter von Online-Mediendiensten personenbezogene Daten eines Nutzers dieser Dienste ohne dessen Einwilligung auch über das Ende eines Nutzungsvorgangs hinaus dann erheben dürfen, soweit ihre Erhebung und ihre Verwendung erforderlich sind, um die generelle Funktionsfähigkeit des Dienstes zu gewährleisten, wobei es allerdings einer Abwägung mit dem Interesse und den Grundrechten und -freiheiten der Nutzer bedarf.

17.3 eIDAS – was ist das?

Im 11. Tätigkeitsbericht des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit wurde unter der Überschrift „eIDAS – was ist das?“ über die eIDAS-Verordnung berichtet. Es ging darum, dass mit der am 23. Juli 2014 verabschiedeten EU-Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (910/2014)“ für alle Mitgliedstaaten die sichere elektronische Identifizierung und Authentifizierung neu festgeschrieben wurde. Diese Verordnung wird eIDAS-Verordnung genannt (electronic identification and trust services) und ist unmittelbar geltendes Unionsrecht.
Die Vorschriften bezüglich der Vertrauensdienste traten allerdings erst ab dem 1. Juli 2016 in Kraft. Vertrauensdienste definiert die eIDAS-Verordung in Artikel 3 wie folgt: Ein „Vertrauensdienst“ ist ein elektronischer Dienst, der in der Regel gegen Entgelt erbracht wird und die Erstellung, Überprüfung und Validierung von elektronischen Signaturen, elektronischen Siegeln oder elektronischen Zeitstempeln, und Diensten für die Zustellung elektronischer Einschreiben sowie von diese Dienste betreffenden Zertifikaten, anbietet. Vertrauensdienste sind aber auch Dienste, die die Erstellung, Überprüfung und Validierung von Zertifikaten für die Website-Authentifizierung oder die Bewahrung von diese Dienste betreffenden elektronischen Signaturen, Siegeln oder Zertifikaten anbietet.



Vertrauensdiensteanbieter können ihre Dienste/Produkte auch zu einem „qualifizierten Dienst“ zertifizieren lassen und dürfen dann ihre Dienste mit dem neuen EU-Vertrauenssiegel bewerben. Um der eIDAS-Verordnung bezüglich der Vertrauensdienste gerecht zu werden, trat in Deutschland am 29. Juli 2017 das eIDAS-Durchführungsgesetz mit zahlreichen Gesetzesänderungen in Kraft (BGBL Nr. 52/2017). Mit dem darin enthaltenen neuen Vertrauensdienstegesetz (VDG) wurde die wirksame Durchführung der Vorschriften über Vertrauensdienste rechtlich geregelt.
Zuständige Aufsichtsstelle für Vertrauensdienste im Bereich der Erstellung, Überprüfung und Validierung von Zertifikaten für Website-Authentifizierung ist in Deutschland das Bundesamt für Sicherheit in der Informationstechnik (BSI). Für die Aufgaben der anderen Bereiche ist die Bundesnetzagentur (BNetzA) zuständig.
Mit dem eIDAS-Durchführungsgesetz wurden zudem das Signaturgesetz und die Signaturverordnung außer Kraft gesetzt. Sämtliche Verweise auf das Signaturgesetz und die Signaturverordnung müssen nun zeitnah aktualisiert werden. Entsprechend der Übergangsvorschrift werden zudem die von der Bundesnetzagentur gemäß § 16 Absatz 1 des Signaturgesetzes ausgestellten Zertifikate mit Ablauf des 14. November 2018 gesperrt. Entsprechende akkreditierte Zertifizierungsdiensteanbieter müssen also rechtzeitig neue Zertifikate beantragen.

Mit Inkrafttreten des Vertrauensdienstegesetzes am 29. Juli 2017 werden alle von der Bundesnetzagentur gemäß § 16 Absatz 1 des Signaturgesetzes ausgestellten Zertifikate mit Ablauf des 14. November 2018 gesperrt. Sämtliche Verweise auf das Signaturgesetz und die Signaturverordnung müssen zudem nun zeitnah überarbeitet werden.

17.4 EU- und nationale Cybersicherheit

Am 5. Juli 2016 veröffentlichte die EU-Kommission eine Mitteilung unter der Überschrift: „Stärkung der Abwehrfähigkeit Europas im Bereich der Cybersicherheit und Förderung einer wettbewerbsfähigen und innovativen Cybersicherheitsbranche“. Der Mitteilung war zu entnehmen, dass einer Untersuchung zufolge mindestens

80 Prozent der europäischen Unternehmen im Jahr 2015 zumindest einmal mit einem Cybervorfall zu tun gehabt haben. Zudem nahm die Zahl der Sicherheitsvorfälle in der gesamten Wirtschaft 2015 weltweit um 38 Prozent im Vergleich zum Vorjahreszeitraum zu.
Die Europäische Kommission will deshalb eine verstärkte Zusammenarbeit sowohl über Ländergrenzen hinweg als auch zwischen allen Akteuren und allen Sektoren, die im Bereich der Cybersicherheit aktiv sind, fördern. Außerdem will sie dazu beitragen, dass in der EU innovative und sichere Technologien, Produkte und Dienste entwickelt werden.
Diese Mitteilung ist im zeitlichen Kontext der Maßnahmen zu sehen, die die Cyber-Sicherheit in Europa erhöhen sollen. Denn am Tag darauf, am 6. Juli 2016, verabschiedete das Europäische Parlament die „Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union“, kurz auch NIS-Richtlinie genannt (Richtlinie (EU) 2016/1148 vom 6. Juli 2016, http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016L1148&from=DE).
Die Mitgliedstaaten der EU müssen dem nun Rechnung tragen und die Bestimmungen der NIS-Richtlinie in nationales Recht umsetzen. Die so getroffenen Vorschriften und Umsetzungsmaßnahmen sind bis zum 9. Mai 2018 der Kommission mitzuteilen. Etwaige spätere Änderungen sind dann immer unverzüglich der Kommission zu melden.



Die Bundesrepublik Deutschland hat deshalb ein Gesetz zur Umsetzung der Richtlinie (EU) 2016/1148 beschlossen. Dieses Gesetz ist vom 23. Juni 2017 und im Bundesgesetzblatt Nr. 40 von 2017 veröffentlicht. Es ist als „Gesetz zur Umsetzung der EU-Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union“ (NIS-Richtlinien-Umsetzungsgesetz) am 30. Juni 2017 in Kraft getreten.
Das Gesetz ist ein sogenanntes Artikel-Gesetz und regelt in einzelnen Artikeln die Änderungen von verschiedenen, nachfolgend aufgeführten Gesetzen. So wurden das BSI-Gesetz (BSIG), das Telekommunikationsgesetz (TKG), das Telemediengesetz (TMG), das Energiewirtschaftsgesetz (EnWG), das Atomgesetz (AtG) und auch das Fünfte Buch des Sozialgesetzbuches in Teilen angepasst.

Gemäß BSIG müssen beispielsweise die Betreiber „Kritischer Infrastrukturen“ ihre IT-Sicherheit nach dem „Stand der Technik“ umsetzen und deren Einhaltung regelmäßig gegenüber dem BSI nachweisen. Sofern Sicherheitsmängel aufgedeckt werden, darf das BSI im Einvernehmen mit den Aufsichtsbehörden deren Beseitigung anordnen.[1]

Im TKG werden Telekommunikationsanbieter sowie auch im TMG Telemediendiensteanbieter nunmehr dazu verpflichtet, IT-Sicherheitsmaßnahmen nach dem „Stand der Technik“ zu ergreifen und zu erhalten, die nicht nur dem Schutz personenbezogener Daten dienen, sondern auch dem Schutz vor unerlaubten Eingriffen in die Infrastruktur dienen.[2]

Bezüglich der Telekommunikationsnetze erweitert sich die bereits bestehende Meldepflicht gemäß § 109 Absatz 5 TKG insofern, dass Beeinträchtigungen sowohl an die Bundesnetzagentur als auch an das BSI gemeldet werden müssen. Betreiber „Kritischer Infrastrukturen“ gemäß BSI-Kritisverordnung müssen ebenfalls eine Kontaktstelle beim BSI registrieren.

Wichtigste Änderung im Energiewirtschaftsgesetz (EnWG) ist die Tatsache, dass das Bundesamt für Sicherheit in der Informationstechnik (BSI) die Meldepflicht von IT-Störungen auf alle Energieversorgungsnetzbetreiber ausgeweitet hat. Letztere müssen hierfür eine zuständige Kontaktstelle einrichten. Beim Atomgesetz (AtG) ist dies für die Betreiber gleichlautend formuliert.[3]

Zur Stärkung der Abwehrfähigkeit Europas im Bereich der Cybersicherheit haben Mitgliedstaaten der EU die seit 2016 in Kraft gesetzte EU-NIS-Richtlinie in nationales Recht umzusetzen. Bis zum 9. Mai 2018 sind die getroffenen Vorschriften und Maßnahmen der Europäischen Kommission zu melden.

[1] weitere Details vgl. https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/IT-SiG/Neuregelungen_IT_SiG/neur_IT_SiG_node.html
[2] ebenda
[3] ebenda

17.5 Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation („Berlin Group“)

Wie bereits an anderer Stelle erwähnt, arbeiten die unabhängigen Datenschutzbeauftragten des Bundes und der Länder themenbezogen bundesweit in sehr vielen Arbeitskreisen und Unterarbeitsgruppen zusammen. Darüber hinaus gibt es auch internationale Arbeitsgruppen.

Die internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation („Berlin Group“) finalisierte im April 2016 das Arbeitspapier „Aktualisierung zu Datenschutz und Datensicherheit in der Internettelefonie (Voice over IP – VoIP) und verwandten Kommunikationstechnologien“. Das Arbeitspapier spricht diesbezügliche Empfehlungen aus, die an verschiedene Akteure gerichtet sind, so auch an die Gesetzgeber, bestehende Regelungslücken zu schließen.

Im November 2016 wurde von der internationalen Arbeitsgruppe das „Arbeitspapier zu Biometrie in der Online-Authentifizierung“ verabschiedet. Oft wird der Zugang zur Hard- oder Software schon per Fingerabdruck oder Gesichtserkennung ermöglicht. Aber auch bei dieser Methode müssen Datenschutz und Datensicherheit sichergestellt sein.

Im April 2017 wurde dann das „Arbeitspapier zum Thema E-Learning-Plattformen“ fertig gestellt. Mit dem zunehmenden Einsatz von E-Learning-Plattformen wächst die Menge an personenbezogenen Daten, die über die Lernenden zur Verfügung stehen. Diese Daten könnten beispielsweise zu Prognosen des geistigen Zustands herangezogen werden und gewollte oder ungewollte lebenslange Schlussfolgerungen nach sich ziehen. Betreiber solcher Plattformen tragen hier eine sehr hohe datenschutzrechtliche Verantwortung.

Alle drei Arbeitspapiere sind auf der Seite der Internationalen Arbeitsgruppe abrufbar http://www.berlin-privacy-group.org.

Die internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation hat die Arbeitspapiere zu Datenschutz und Datensicherheit in der Internettelefonie (Voice over IP – VoIP) und verwandten Kommunikationstechnologien, zu Biometrie in der Online-

Authentifizierung und zum Thema E-Learning-Plattformen veröffentlicht.

17.6 Canvas-Fingerprinting

Zunehmend werden bei der Darstellung von Websites Browser-Fingerprints verwendet, um Internetnutzer zu tracken, um so z. B. personalisierte Werbung zu schalten. Fingerprinting ist eine Methode, um Hersteller und Versionen von Software-Anwendungen über ein Netzwerk zu erkennen, obwohl diese Informationen nicht explizit vom System kommuniziert werden. Die Methode erlaubt es, auf Cookies oder Logins zu verzichten. Canvas-Fingerprinting ist eine solche Methode.

Wie funktioniert Canvas-Fingerprinting? Beim Aufruf einer Website werden von der Website im Hintergrund Informationen über bestimmte Software- und Hardware Merkmale ermittelt, die der Browser selbst bei Aufruf zwecks optimaler Darstellung mitliefert oder auf Anfrage nachliefert. Diese Informationen werden bei Canvas-Fingerprinting erfasst, indem sozusagen kleine Grafiken „gezeichnet“ werden. Jede Konfiguration von Hard- und Software erstellt die Grafiken mit leichten Abweichungen zueinander. Diese werden dann zur Identifizierung genutzt. Die so gesammelten Daten, wie beispielsweise der Browsertyp und Version, genutzte Schriftart, installierte Schriftarten, Bildschirmgröße, Sprache, die Art des Grafikprozessors usw. geben Aufschluss über das jeweilige Gerät. Über die gesammelten Daten entsteht somit der o. g. „Fingerabdruck“ (engl.: Fingerprinting) des jeweiligen technischen Gerätes. Je mehr Daten für die Bildung des Fingerabdrucks erfasst werden, umso genauer ist dieser Fingerabdruck und somit der Wiedererkennungswert des Gerätes.

Man kann sich vor Canvas-Fingerprinting schützen, indem man Java-Script in den Browsereinstellungen deaktiviert. Der Nachteil davon ist, dass dann allerdings viele Anzeigen von Websites nicht mehr richtig funktionieren. Auch empfehlen IT-Experten, mindestens zwei bis drei verschiedene Browser für verschiedene Suchanfragen zu verwenden. Dies erscheint für normale Nutzer zu umständlich. Weitere IT-Experten empfehlen, Anonymisierungsnetzwerke wie TOR zu nutzen. Letzteres zieht aber nur eine Anonymisierung des Netzverkehrs nach sich – die Inhalte, welche zur Identifikation herangezogen werden, werden durch TOR nicht anonymisiert. Für

das tägliche Surfen erscheint dies auch ein umständlicher Weg. Manche Browser bieten auch schon Canvas-Blocker an. Solch Canvas-Blocker als sogenanntes Add-on kann Zugriffe auf Canvas-Elemente blockieren. In den „Einstellungen“ des Add-on kann man dann das gewünschte Verhalten konfigurieren. Dieses Add-on sollte aber nur von der Online-Plattform des jeweiligen Browserherstellers geladen werden.
Es gibt demnach durchaus verschiedene Möglichkeiten, sich zu schützen. Jeder muss für sich selbst entscheiden, welchen Weg er gehen möchte.

Zunehmend werden bei der Darstellung von Websites heimlich Browser-Fingerprints verwendet, um Internetnutzer zu tracken. Damit kann z. B. personalisierte Werbung geschaltet werden. Die beschriebene Methode erlaubt es, auf Cookies oder Logins zu verzichten. Bei der Auswahl der Schutzmöglichkeiten wird empfohlen, sich auf dem Portal des jeweiligen Browseranbieters genau zu informieren und dann erst eigene Maßnahmen zu treffen.



© *Scanrail – Mobile applications concept – fotolia.com*

18. Technischer Datenschutz im Freistaat Thüringen

18.1 Angriffe auf das Netzwerk der Thüringer Landesverwaltung

Entsprechend der Thüringer Organisationsrichtlinie für E-Government vom 3. August 2015 vom Thüringer Finanzministerium ist der Beauftragte des Freistaats Thüringens für E-Government und IT u. a. auch zuständig für die zentrale Steuerung der Informationssicherheit und Cybersicherheit in der Thüringer Landesverwaltung.
Am 3. Mai 2016 informierte der Beauftragte des Freistaats Thüringen für E-Government und IT die Landesregierung zum Umsetzungsstand zur Informationssicherheit sowie zur IT-Sicherheitslage in der Thüringer Landesverwaltung. Dem Bericht waren ressortübergreifende Maßnahmen und Projekte zur Erhöhung der Informationssicherheit sowie über Art und Umfang von externen sowie internen IT-Gefährdungen für die Thüringer Landesverwaltung zu entnehmen. Die einzelnen aufgeführten internen und externen Störungen

können der entsprechenden Drucksache des Thüringer Landtages DS 6/2108 vom 3. Mai 2016 entnommen werden.
Auch war dem Bericht zu entnehmen, dass alleine im Jahr 2015 vier große Sensibilisierungs- und Schulungsmaßnahmen zu den Themen Informationssicherheit erfolgten, eine Teilnahme an den Veranstaltungen von insgesamt 600 Mitarbeitern registriert wurde.
Am 5. Januar 2017 berichtete die „Thüringer Allgemeine“ unter der Überschrift „Dauerfeuer auf Computer der Regierung“, dass im Jahr 2016 von den 13 Millionen Mails an Thüringer Landesbehörden 8,5 Millionen Mails als gefährlich herausgefiltert wurden. Dabei handelte es sich um SPAM-Mails. Zusätzlich wurden 30.000 Mails mit Schadsoftware erkannt. Dem Zeitungsbericht war zu entnehmen, dass somit fast zwei Drittel aller Mails, die im Thüringer Landesrechenzentrum gescannt wurden, als unerwünscht oder gar gefährlich für die Computersysteme eingestuft wurden. Dies sei im Vergleich zu 2015 eine deutliche Steigerung.
Wie dem o. g. Bericht aber auch zu entnehmen ist, beinhalten Angriffe via Mail zunehmend keine Schadsoftware mehr selbst, sondern beinhalten meistens Links, die auf Websiten verweisen, wo erst beim Anklicken des Links von der Website die Schadsoftware übertragen wird. Somit greifen zentrale technische Maßnahmen, die Mails mit Schadsoftware verhindern sollen, diesbezüglich nicht, da die Links aufgrund ständiger Veränderungen zudem schwer zu blockieren sind.
Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) nimmt zudem auch wahr, dass zunehmend solche E-Mails mit dienstlich aussehenden Absenderadressen versendet werden.
Solche Mails landen dann direkt beim Empfänger, also auch bei Mitarbeitern der Thüringer Landesverwaltung, von denen es laut Thüringer Landeshaushaltsplan 2016/2017 in der Thüringer Landesverwaltung über 45.000 gibt.
Aus Sicht des TLfDI gilt es daher auch, zeitnah die digitale Kompetenz bei allen Mitarbeitern zu fördern und die digitale Sorglosigkeit zu minimieren, dass das Thüringer Landesrechenzentrum ja alles abfangen würde.
Mittelfristig wird es nicht mehr ausreichen, dass das zuständige Thüringer Finanzministerium im Jahr 600 Mitarbeiter der Thüringer Landesverwaltung schult. Auch der TLfDI ist nicht in der Lage 45.000 Mitarbeiter im Jahr zu schulen. Dafür ist auf beiden Seiten schon allein die Personalausstattung unzureichend.

Auch wenn der TLfDI als Leiter des bundesweiten Arbeitskreises Datenschutz und Bildung der unabhängigen Datenschutzbeauftragten des Bundes und der Länder auf die Notwenigkeit der sozialen Medienkompetenz der Gesellschaft hingewiesen hat und in Thüringen verschiedene Akteure dafür gewinnen konnte, dass zu mindestens in den Schulen und bei Lehrern der Anfang bezüglich Medienkompetenz gemacht wird (siehe Punkt 2.2), wird dies nicht ausreichen. Die neu mit Wissen um Datenschutz und IT-Sicherheit ausgebildete Jugend wird erst in vielen Jahren in den Arbeitsmarkt Einzug halten.
Es ist unverständlich, dass Datenschutz und IT-Sicherheit noch immer nicht einer verpflichtenden Arbeitsschutzbelehrung gleichgestellt wird.
Mittelfristig wäre aus Sicht des TLfDI wünschenswert, dass wie bei einer jährlichen Arbeitsschutzbelehrung, die nachweislich dokumentiert wird, auch eine nachweisliche Belehrung für alle Mitarbeiter zum Datenschutz und zur IT-Sicherheit festgeschrieben wird. Der jeweilige Behördenleiter ist analog der Arbeitsschutzbelehrung zur Umsetzung verpflichtet.

Analog einer verpflichtenden Arbeitsschutzbelehrung muss zukünftig auch eine verpflichtende Belehrung zur IT-Sicherheit und zum Datenschutz eingeführt werden. Nur so lässt sich flächendeckend eine digitale Kompetenz in der Thüringer Landesverwaltung sicherstellen.

18.2 BSI-Richtlinie: Kryptographische Verfahren

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat im März 2017 die Technische Richtlinie „Kryptographische Verfahren“ aktualisiert (BSI TR-02102, Version 2017-1).
Diese vierteilige Richtlinie enthält:

1.) Empfehlungen zu Schlüssellängen,
2.) Empfehlungen zur Verwendung von Transport Layer Security (TLS),
3.) Empfehlungen zur Verwendung von Internet Protocol Security (IPsec) und
4.) Empfehlungen zur Verwendung von Secure Shell (SSH).

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) weist in diesem Zusammenhang darauf hin, dass die jeweils getroffenen technischen und organisatorischen

Maßnahmen damit dem Stand der Technik anzupassen sind. Somit ist diese Richtlinie zeitnah umzusetzen.
Insbesondere weist der TLfDI darauf hin, dass Websites, die personenbezogene Daten enthalten, mit einem sicheren Transportprotokoll abzusichern sind. Entsprechend der aktualisierten BSI TR 02102-2 ist dabei grundsätzlich das Transportprotokoll TLS 1.2 einzusetzen. Die Transportprotokolle SSL, TLS 1.0 und TLS 1.1 werden nicht mehr empfohlen. Das BSI hat zudem den Handlungsleitfaden „Migration auf TLS 1.2“ überarbeitet, um bei der notwendigen Umstellung auf den höheren Sicherheitsstandard TLS 1.2 die IT-Sicherheitsbeauftragten, das IT-Fachpersonal und IT-Verfahrensverantwortliche zu unterstützen.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat im März 2017 die Technische Richtlinie „Kryptographische Verfahren“ aktualisiert (BSI TR-02102, Version 2017-1). Eine Anleitung bezüglich der Umstellung auf das Transportprotokoll TLS 1.2 stellt das BSI in seinem Handlungsleitfaden „Migration auf TLS 1.2“ bereit. Der TLfDI weist daraufhin, dass die Richtlinie zeitnah umzusetzen ist.

18.3 Windows 10, Microsoft-Cloud Deutschland und Windows Office 365

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) ist per Gesetz durch das Thüringer Datenschutzgesetz (ThürDSG) verpflichtet, die Entwicklung und Nutzung der Informations- und Kommunikationstechnik, insbesondere der automatisierten Datenverarbeitung und deren Auswirkungen auf die Arbeitsweise und die Entscheidungsbefugnisse der öffentlichen Stellen, zu beobachten (§ 40 Abs. 5 ThürDSG). Gerade zu den oben genannten Themen erreichen den TLfDI auch Anfragen, und Reaktionen des TLfDI hierauf sollen kurz dargestellt werden:
Windows 10:
Für die Microsoft Deutschland GmbH ist die zuständige datenschutzrechtliche Aufsichtsbehörde das Bayerische Landesamt für Datenschutzaufsicht (BayLDA).
Da aber auch beim TLfDI Anfragen zum datenschutzgerechten Einsatz von Windows 10 eingingen, stellte der TLfDI im Juni 2016 eine

kurze Handreichung auf seiner Website zur Verfügung (siehe https://www.tlfdi.de/mam/tlfdi/themen/windows_10.pdf).

Microsoft-Cloud Deutschland:

Die Microsoft Deutschland GmbH betreibt in Deutschland zwei deutsche Rechenzentren mit der T-Systems, einer Tochter-Gesellschaft der Deutschen Telekom, als Datentreuhänder. Dies bedeutet, dass die T-Systems gegenüber dem Kunden vertraglich sicherstellt, dass Daten nicht Dritten offengelegt werden. Nach Angaben der T-Systems kann somit die Herausgabe der Daten nur der Kunde selbst verlangen oder ein Dritter aufgrund einer deutschen Rechtsgrundlage beruhen. Nach derzeitigem Stand geht die T-Systems davon aus, dass somit ausländische Behörden keine Herausgabe der Daten verlangen können.

Ziel der Microsoft-Cloud Deutschland ist es, den Kunden dieser Cloud auf Wunsch hin anzubieten, dass die Daten in den Rechenzentren in Deutschland verbleiben.

Die unabhängigen Datenschutzbeauftragten des Bundes und der Länder sind bezüglich der Microsoft-Cloud Deutschland derzeit im Gespräch, um datenschutzrechtliche Fragen zu klären. Siehe hierzu auch Nummer 2.1. Ein gemeinsamer Dialog wird sich sicherlich fortsetzen.

Microsoft-Office 365:

Der TLfDI als Vorsitzender des Arbeitskreises Bildung und Datenschutz der unabhängigen Datenschutzbeauftragten des Bundes und der Länder prüft derzeit, ob Microsoft Office 365 für Schulen datenschutzgerecht einsetzbar ist.

Am Anfang bezog sich der Prüfungsbereich auf den Einsatzbereich im rein pädagogischen Kontext. Mittlerweile steht zudem die Frage im Raum, ob nicht auch Schulen für ihre eigene Verwaltung Microsoft Office 365 nutzen dürfen. Eine Antwort auf die letzte Frage interessiert natürlich auch Verwaltungen anderer öffentlicher und nicht-öffentlicher Stellen.

Die unabhängigen Datenschutzbeauftragten des Bundes und der Länder beobachten weiterhin die Entwicklungen verschiedener Microsoftprodukte. Jegliche Anwendungen müssen zudem der DS-GVO standhalten.

18.4 Kritische Infrastruktur – Sektor Gesundheit

Im Juni 2016 legten Kriminelle per Hackerangriff das Lukas-Krankenhaus in Neuss mit einer Erpresser-Botschaft lahm. Kaum ein Nachrichtenkanal berichtete nicht davon.
Schon lange sind IT-Systeme von Krankenhäusern derartigen Angriffen ausgesetzt, in letzter Zeit häufen sich derartige Attacken.
Nach einer Meldung des WDR traf es danach weitere Krankenhäuser, unter anderem das Klinikum Arnsberg.
Der Vorteil des Einzugs der digitalen Gesellschaft ist auch im medizinischen Bereich nicht von der Hand zu weisen. Aber mit dem Einzug dieser modernen Technik werden gleichzeitig auch neue Angriffspunkte ermöglicht.
Das seit Juli 2015 gültige Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) hat zum Ziel, bei kritischen Infrastrukturen die Sicherheit informationstechnischer Systeme zu erhöhen. Im April 2016 wurde dann eine BSI-Kritisverordnung (BSI-KritisV) in Kraft gesetzt, die die Sektoren Energie, Wasser, Ernährung, Informationstechnik und Telekommunikation als kritische Infrastrukturen einstuft. Also Bereiche, deren Ausfall dramatische Folgen für Wirtschaft, Staat und Gesellschaft in Deutschland aufweisen. Im Juni 2017 wurde die BSI-KritisV dann um die Sektoren Gesundheit, Finanz- und Versicherungswesen, Transport und Verkehr erweitert.
Somit sind nun auch Betreiber dieser Sektoren angehalten, IT-Sicherheit nach dem „Stand der Technik“ umzusetzen und erhebliche IT-Sicherheitsvorfälle an das Bundesamt für Sicherheit in der Informationstechnik zu melden.

Die BSI-Kritisverordnung (BSI-KritisV) regelt, welche Sektoren derzeit als kritische Infrastruktur eingestuft sind. Bereits nach einem Jahr wurden die Sektoren Gesundheit, Finanz- und Versicherungswesen, Transport und Verkehr nachträglich aufgenommen, da diese 2016 einem hohen Gefährdungspotenzial ausgesetzt waren und deren Folgen bei Ausfall neu bewerten wurden.

18.5 Datenschleudern – vom vernetzten Auto

Vor einigen Jahren waren die Fahrzeuge nur reines Transportmittel, dessen Zweck es war, Personen von einem Ort zu einem anderen zu transportieren. Durch den Fortschritt in der digitalen Regelung und Steuerung zog zunehmend die Digitaltechnik auch in die Fahrzeuge ein. Heutzutage sind in Fahrzeugen zahlreiche Computersysteme verbaut, die die Funktion der einzelnen Komponenten überwachen (z. B. Bremsen, Motorsteuerung, Sitzverstellung, Entertainment-System, Navigationssystem) und Daten untereinander austauschen. Seit ca. 1970 können so Fehlerberichte über die einheitliche Schnittstelle ODB-II durch Werkstätten ausgelesen bzw. Speicher zurückgesetzt werden. Die Anzahl der zugriffsberechtigten Personen, die Zugriff auf die generierten Daten besaßen, war im Regelfall überschaubar.

All dies ändert sich seit einigen Jahren.

Bereits im 10. Tätigkeitsbericht (2012/2013) berichtete der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit über das europäische Vorhaben, bordeigene eCall-Systeme in allen Fahrzeugen der Mitgliedstaaten verbindlich vorzuschreiben. Schon damals war erkennbar, dass in einer weiteren Ausbaustufe neben den Basisdaten zusätzliche Angaben hinzukommen werden, die z. B. Versicherungsgesellschaften, Kraftfahrzeug-Callcenter, Gesundheitsdienste, Rechtsanwälte oder Automobilclubs interessieren werden (siehe 10. Tätigkeitsbericht, Punkt 3.2). Entsprechend der EU-Verordnung 2015/758, müssen nun ab April 2018 alle Neuwagen mit eCall-Systemen ausgestattet werden. So bereitet sich die Wirtschaft seit Jahren darauf vor.

Durch das praktisch flächendeckend verfügbare Datennetz des Mobilfunks ist nun auch eine dauerhafte mobile Erreichbarkeit der Fahrzeuge gegeben.

Die Digitalisierung hat aber auch im Fahrzeug selbst Einzug gehalten. Laptops, Handys usw. können mit dem elektronischen Multimediacenter, sogenannte Infotainmentsysteme, im Fahrzeug bestens kommunizieren, fast so, als wäre man in einer modern ausgerüsteten Wohnstube auf vier Rädern. Wer kennt dies nicht? Steigt man in ein modernes Fahrzeug ein, kann man sich heutzutage schon oft mit mobilen Geräten, z. B. mit seinem Smartphone, mit dem Multimediacenter des Fahrzeuges verbinden und alle Kontakte des Smartphones vom Fahrzeug aus anrufen oder die auf dem Smartphone gespei-

cherte Musik oder Videos abspielen. Dabei werden die Telefonkontakte oft komplett auf das Multimediacenter übertragen.
Vor einiger Zeit haben Hersteller wie Apple und Google sogar Möglichkeiten geschaffen, Apps auf dem Smartphone vom Touch-Display des Fahrzeugs bedienen zu können. Ebenso bieten nun auch schon die Automobilhersteller eigene App-Anwendungen an. Moderne Infotainmentsysteme bieten bereits Apps auf herstellerspezifischen App-Stores an und erlauben die Individualisierung des Erlebnisses Autofahren. Viele Fahrzeuge bringen auch ihre eigene Datenverbindung ins Mobilfunknetz gleich mit und können somit z. B. direkt mit dem Fahrzeughersteller kommunizieren. Das zukünftige Fahrzeug wird also ein vernetztes Fahrzeug sein – bzw. ist es zum Teil schon heute.
So komfortabel es auch ist: In den oben genannten Beispielen fallen große Mengen von Daten an. Also zum einen Daten über das Fahrzeug selbst und das Fahrverhalten und zum anderen durch den Nutzer selbst, veranlasst aufgrund des Kontaktes zum Multimediacenter. So fallen z. B. Daten an zu Motordrehzahl, Bremsverhalten, Beschleunigungsverhalten, Füllstand des Tanks, Ausschlag der Stoßdämpfer, Navigationszielen, aktuellem Standpunkt und aktueller Geschwindigkeit, Fahrtrichtung, Insassenzahl, Kamerabildern von Rückfahrt- und Frontkameras, Abstandssensoren usw. – die Liste ließe sich noch lange fortsetzen. Zum anderen können evtl. auch Daten von Nutzern erfasst werden, die sich in diesem Fahrzeug befinden und mit ihren Geräten mit dem Multimediacenter gewollt oder nicht gewollt in Kontakt stehen (z. B. indem Verbindungen gespeichert oder Gerätekennungen auch bei nicht aktiver Verbindung ausgelesen werden).
Das Problem ist, dass viele dieser Daten einen „Personenbezug“ aufweisen und durch ihre Analysen sogar ein Verhaltensprofil erstellt werden kann. Aus den Daten kann beispielsweise der Fahrstil des Fahrers (und dessen Risikobereitschaft), die Übertretung von Verkehrsregeln und natürlich auch der Verlauf von Aufenthaltsorten, wie z. B. die Route des letzten Urlaubs oder der Dienstreisen, ermittelt werden.
Die Versicherungsbranche und auch die Wirtschaft sehen bereits seit Jahren ein großes Marktpotential bezüglich der Auswertung solcher Daten. Ihre Geschäftsmodelle und die Wertschöpfung werden sich im Rahmen der digitalisierten Fahrzeuge zukünftig enorm auf den digitalen Mobilitätsbereich erweitern. Die vom Bundesministerium

für Verkehr und digitale Infrastruktur veröffentlichte Studie „‚Eigentumsordnung' für Mobilitätsdaten" vom August 2017 gibt einen ersten Eindruck, wohin die Reise zukünftig gehen könnte (siehe https://www.bmvi.de/SharedDocs/DE/Artikel/DG/studie-mobilitaetsdaten-fachkonsultation.html).
So gilt es beispielsweise dringend zu klären, welche Daten überhaupt erforderlich sind, wem eigentlich die in einem Fahrzeug anfallenden Daten gehören, wer also „Eigentümer" (oder Verfügungsberechtigter) dieser Daten und somit auch datenschutzrechtlich verantwortlich für diese ist und wer sie wann nutzen darf.



Ab dem 25. Mai 2018 tritt zudem die Europäische Datenschutz-Grundverordnung (DS-GVO) in Kraft. So regelt beispielsweise Artikel 25 DS-GVO, dass Datenschutz und Datensicherheit bereits in der Planung und Entwicklung von IT-Systemen berücksichtigt werden müssen (Data protection by design) und IT-Systeme datenschutzfreundlich so voreingestellt sein müssen, dass nur die personenbezogenen Daten verarbeitet werden, die für den verfolgten Zweck erforderlich sind (Data protection by default).
Auch auf die zukünftige Umsetzung des Artikels 6 DS-GVO, Rechtmäßigkeit der Verarbeitung, darf man gespannt sein. Die Erfassung und Weitergabe der Daten bedürfen immer einer Erlaubnisnorm oder einer Einwilligung. Auch das „Recht auf Vergessenwerden" (Artikel 17 DS-GVO) oder das Auskunftsrecht über die betreffenden Daten (Artikel 20 DS-GVO), ist umzusetzen. Man darf gespannt sein, insbesondere bei Carsharing-Lösungen.
Es gibt also noch viel zu tun, damit Daten in Fahrzeugen datenschutzgerecht verarbeitet werden. Wünschenswert ist dabei u. a., dass Fahrzeughalter oder Fahrzeugnutzer grundsätzlich über die Weitergabe und die Verwendung ihrer anfallenden Fahrzeugdaten selbst entscheiden können.
So weist auch die vom Bundesministerium für Verkehr und digitale Infrastruktur eingesetzte Ethik-Kommission zum automatisierten Fahren in ihrem Bericht im Juni 2017 darauf hin, dass Geschäftsmodelle, die sich diese anfallenden Daten zunutze machen, ihre Grenze in der Autonomie und Datenhoheit der Verkehrsteilnehmer finden. Fahrzeughalter oder Fahrzeugnutzer sollten grundsätzlich über die Weitergabe und die Verwendung ihrer anfallenden Fahrzeugdaten

entscheiden. Die Freiwilligkeit solcher Datenpreisgabe setzt das Bestehen ernsthafter Alternativen und Praktikabilität voraus. Einer normativen Kraft des Faktischen, wie sie etwa beim Datenzugriff durch die Betreiber von Suchmaschinen oder sozialen Netzwerken vorherrscht, so die Ethik-Kommission, sollte frühzeitig entgegengewirkt werden. Weiterhin führt die Ethik-Kommission in ihren 20 Ethik-Leitlinien aus, dass klar unterscheidbar sein muss, ob ein fahrerloses System genutzt wird oder ein Fahrer mit der Möglichkeit des „Overrulings“ Verantwortung behält. Dabei muss bei nicht fahrerlosen Systemen die Mensch/Maschine-Schnittstelle so ausgelegt werden, dass zu jedem Zeitpunkt klar geregelt und erkennbar ist, welche Zuständigkeiten auf welcher Seite liegen, insbesondere, auf welcher Seite die Kontrolle liegt. Für die dazu notwendige Protokollierungs- und Dokumentationspflicht ist eine internationale Standardisierung anzustreben.

Auch die 39. Internationale Konferenz der Beauftragten für den Datenschutz und die Privatsphäre forderte in ihrer Entschließung vom 25. bis 29. September 2017 die Hersteller, Behörden und Anbieter fahrzeugbezogener Dienste auf, u. a.

- sichere Datenspeicher bereitzustellen, um Zugriffe steuern zu können,
- Technologien zu entwickeln, die unzulässige Zugriffe und das Mitschneiden von persönlichen Daten bei Fahrzeugen, Infrastrukturen und Einrichtungen verhindern,
- technische Maßnahmen bereitzustellen, die Cyberangriffe verhindern,
- die Datensparsamkeit zu beachten und die Datenlöschung nach einer gewissen Zeit zu gewährleisten und z. B. auch
- eine Datenschutzfolgeabschätzung für neue, innovative oder riskante Entwicklungen durchzuführen.

Mobilität 4.0, so wird die Digitalisierung der Mobilität oft genannt, um den Komfort und die Verkehrssicherheit zu erhöhen, darf nicht auf Kosten des Rechts auf informationelle Selbstbestimmung gehen. Dieses Recht ist ein Grundrecht gemäß Artikel 2 Abs. 1 i. v. m. Art. 1 Abs. 2 Grundgesetz.

Die Ethik-Kommission weist zu Recht darauf hin, dass auch datenschutzfreundliche Innovationen (Privacy by design) gefördert werden müssen. Es gilt eben auch zu verhindern, dass es z. B. im Rahmen einer zentralen Verkehrssteuerung und der Erfassung aller

Kraftfahrzeuge, zu einer Totalüberwachung aller Verkehrsteilnehmer kommt.
Aus Sicht des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) ist es deshalb wichtig, Gelegenheiten zu nutzen, um mit der Auto-Industrie, Politikern und anderen Interessenten in Kontakt zu treten. So nutzte der TLfDI z. B. in Augsburg, Jena und Bielefeld die Möglichkeit, datenschutzrechtliche Hinweise zu geben und datenschutzrechtliche (Fehl-) Entwicklungen zu finden.

Moderne Fahrzeuge werden in naher Zukunft vollständig vernetzt sein. Die anfallenden Daten werden zukünftig Begehrlichkeiten verschiedener Wirtschaftszweige wecken. Die möglichen Daten haben das Potenzial der Verhaltenskontrolle und verraten viel über den Fahrer. Deshalb sind bei der Planung und Entwicklung von IT-Systemen Datenschutz und Datensicherheit zu berücksichtigen (Data protection by design). Die IT-Systeme müssen zudem datenschutzfreundlich so voreingestellt sein, dass nur die personenbezogenen Daten verarbeitet werden, die für den verfolgten Zweck erforderlich sind (Data protection by default).

18.6 WannaCry

Im Frühjahr 2017 wurden weltweit zehntausende Computer Opfer eines Hackerangriffs durch die Schadsoftware WannaCry. Diese Software verschlüsselt die Daten auf den jeweils gehackten Computern und zeigt dann auf dem Bildschirm des Benutzers eine Lösegeldforderung an. Das Verfahren ist nicht neu. Seit Jahren wird in diesem Zusammenhang auch davon abgeraten, auf solche Lösegeldforderungen einzugehen, denn eine Entschlüsselung der Daten nach der Zahlung ist ungewiss. Tritt ein solcher Fall jedoch auf, hilft nur eine Anzeige bei der Polizei gegen Unbekannt. Der Rechner sollte umgehend neu installiert werden, bestenfalls mit einem Sicherungs-Image neueren Datums.
Neu bei diesem Angriff war allerdings, dass er massenhaft in über hundert Ländern gleichzeitig erfolgte. Man spricht vom größten Hacker-Angriff in der Geschichte der Cyber-Angriffe. Auch in Deutschland waren Behörden, Unternehmen sowie Privatpersonen betroffen. So manche Zug-Anzeige bei der Deutschen Bahn zeigte

beispielsweise anstelle der Fahrverbindungen eine Lösegeldforderung an.
Sicherheitslücken in Betriebssystemen oder System-Anwendungen wird es allerdings wohl immer geben. Diese Lücken werden von den Herstellern zum Teil durch sogenannte Sicherheits-Updates (auch „Patches“ genannt) geschlossen. Deswegen ist es als Nutzer wichtig, immer auf die Aktualität der auf dem eigenen Computer installierten Software zu achten. In dem Fall von WannaCry waren nur Windows-Rechner älterer Versionen betroffen. Bei aktuellen Versionen der Microsoft-Betriebssysteme war zuvor schon die Sicherheitslücke durch den Hersteller geschlossen worden. Nachdem WannaCry weltweit einen so großen „Erfolg“ hatte, stellte Microsoft zusätzlich Sicherheits-Updates für ältere Betriebssysteme, deren Support-Zyklen beendet sind – das sind WindowsXP, Windows 8 als Client-Betriebssysteme und Windows Server 2003 - bereit.
Hinsichtlich der Nutzung von Rechnern mit dem Betriebssystem Windows XP warnte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) bereits in seinem 11. Tätigkeitsbericht unter Punkt 16.5. Mit der Ankündigung von Microsoft, das Betriebssystem ab dem 8. April 2014 nicht mehr mit Sicherheits-Updates zu versorgen, sah der TLfDI eine Gefahr für die Datensicherheit und somit für den Datenschutz.

Um das Sicherheitsrisiko bei Sicherheitslücken in Betriebssystemen oder System-Anwendungen zu minimieren, sind die vom Hersteller bereitgestellten Sicherheits-Updates zeitnah zu installieren. Client-Betriebssysteme, die im erweiterten Support keine Sicherheits-Updates mehr erhalten, sind daher durch neuere Client-Betriebssysteme zu ersetzen. Wo dies aus zwingenden Gründen nicht geschehen kann, müssen angemessene technische und organisatorische Sicherheitsmaßnahmen (TOM) bei den verantwortlichen Stellen getroffen werden, um die Sicherheitsrisiken auszuschließen.



© *vege – Gesetze und Paragraphen – fotolia.com*

19. Parlamentarische Anfragen gem. § 112a Geschäftsordnung des Thüringer Landtags

19.1 Parlamentarische Anfragen gem. § 40 Abs. 6 Satz 2 ThürDSG

Das Thüringer Datenschutzgesetz sieht in § 40 Abs. 6 Satz 2 vor, dass der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) parlamentarische Anfragen zu beantworten hat, die den Datenschutz im Bereich seiner Kontrollbefugnis betreffen. Ergänzend dazu regelt § 112a der Geschäftsordnung des Thüringer Landtags (GOLT) das Verfahren, wie die Anfragen an den TLfDI einzureichen und von ihm zu beantworten sind.
Im Berichtszeitraum erreichten den TLfDI insgesamt vier parlamentarische Anfragen. Der TLfDI stand einem Landtagsabgeordneten Rede und Antwort zur Videoüberwachung in öffentlich zugänglichen Bereichen in Thüringen. Im Rahmen der Beantwortung dieser parlamentarischen Anfrage konnte der TLfDI die Gelegenheit nutzen, darauf hinzuweisen, dass er über keine Übersicht/Auflistung verfügt, aus der sich eine Videoüberwachung öffentlicher Plätze in Thüringen verifizieren lässt. Dieser Mangel ist nicht etwa dem Unvermögen des TLfDI, sondern schlicht und einfach der Tatsache geschuldet, dass es

für öffentliche Stellen im Thüringer Datenschutzgesetz keine Verpflichtung gibt, den Einsatz von Videoüberwachungsanlagen dem TLfDI zu melden. Für den nicht-öffentlichen Bereich ist die Melderegelung des § 4d Bundesdatenschutzgesetz zu beachten.
Eine weitere parlamentarische Anfrage erhielt der TLfDI zu dem mittlerweile auf den Weg gebrachten Gemeinsamen Kompetenz- und Dienstleistungszentrum auf dem Gebiet der polizeilichen Telekommunikationsüberwachung (GKDZ) (siehe dazu Punkt 8.4). Dabei wies der TLfDI darauf hin, dass er im Dezember 2015 seine Stellungnahme zum damaligen Staatsvertrags-Entwurf zum GKDZ gegenüber dem TMIK abgegeben hatte.
Eine weitere parlamentarische Anfrage thematisierte die Zahl der Stellungnahmen des TLfDI gem. § 5 Abs. 2 Satz 3 Thüringer Verfassungsschutzgesetz zur erstmaligen Veröffentlichung von personenbezogenen Daten. Der TLfDI konnte hier die Antwort geben, dass er in zwei Fällen um eine solche Stellungnahme vom Amt für Verfassungsschutz gebeten worden war (siehe dazu Punkt 9.1).
Last but not least thematisierte ein Abgeordneter des Thüringer Landtags die Funktionen der von der Thüringer Polizei eingesetzten Software DeviceWatch (siehe dazu Punkt 8.3). Auch diese parlamentarische Anfrage beantwortete der TLfDI fristgerecht.
Alle parlamentarischen Anfragen und die entsprechenden Antworten des TLfDI finden Sie in den entsprechenden Landtagsdrucksachen

Das Verfahren zur Beantwortung parlamentarischer Anfragen gem. § 40 Abs. 6 Satz 2 ThürDSG in Verbindung mit § 112a GOLT hat sich mittlerweile gut zwischen dem TLfDI und der Verwaltung des Thüringer Landtags eingespielt. Der TLfDI betrachtet dieses Verfahren als sinnvolle Ergänzung, um dem parlamentarischen Fragerecht der Abgeordneten aus Artikel 53 Abs. 2 der Verfassung des Freistaats Thüringen gerecht zu werden.



update – © Marco2811 / Fotolia.com

20. Vorträge – der TLfDI ist unterwegs!

Genau am Tag des Safer Internet Days 2016 veröffentlichte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) seine Handreichung zur „Digitalen Selbstverteidigung“, https://www.tlfdi.de/mam/tlfdi/wir-ueber-uns/digitale_selbstverteidigung_broschure_3.web.pdf Ob bei Vorträgen in Schulen, Behörden, Hochschulen, Fraktionen oder Parteien, das handliche Heft begleitet ihn überall. Die von den Medien immer wieder aufgegriffenen Datenschutzskandale zeigen deutlich, dass der Datenschutz im öffentlichen Bereich immer mehr in den Fokus des öffentlichen Interesses gerückt ist. Jeder Einzelne, ob Schüler oder Lehrer, achtet mehr denn je auf einen verantwortungsvollen Umgang mit seinen Daten bei öffentlichen Stellen. Umso wichtiger ist es für den TLfDI, dass auf der einen Seite die Stellen, die mit personenbezogenen Daten arbeiten, und auf der anderen Seite die Personen, um deren Daten es geht, gut beraten und betreut sind. Täglich kommen Anfragen über die Poststelle des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit

(TLfDI) herein, ob der TLfDI nicht mit einem „Rundum-sorglos-Paket“ für Datenschutz an Materialien und Referenten die eine oder andere bereits geplante Veranstaltung mit seinen Vorträgen unterstützen kann. Der TLfDI selbst und seine Mitarbeiter haben im Berichtszeitraum abermals an mehr als 50 (!) Diskussions- und Vortragsveranstaltungen teilgenommen und dabei über zahlreiche datenschutzrechtliche Themen referiert. Eine Auswahl der Vorträge im öffentlichen Bereich finden Sie auf den folgenden Seiten:

Datenschutz als Aspekt digitaler Bildung
Initiativen des TLfDI für Thüringer Schulen

Informationen für die Intendantin des MDR

11. März 2016



Inhalt

Was Schule (nicht?) tut
Unterstützungsangebote der Landesdatenschutzbehörden auf Bundesebene
Gegenwärtige Unterstützungsangebote des TLfDI für Thüringer Schulen
Zukünftige Unterstützungsangebote des TLfDI für Thüringer Schulen

Dienstlich unterwegs in sozialen Netzwerken

7. April 2016



Inhalt:

Soziale Netzwerke

Bildung in der digitalen Welt –
Welche Rolle spielt der Datenschutz?

Runder Tisch Medienkompetenz in Nordhausen

15. September 2016



Inhalt:

Ein Stück Alltag …
Kopf in den Sand? – Was steht auf dem Spiel?
Rechtsgrundlagen
Was Thüringer Schule tut …
Gegenwärtige Unterstützungsangebote des TLfDI
für Thüringer Schulen
Zukünftige Unterstützungsangebote des TLfDI
für Thüringer Schulen
Alles in Butter????
Handlungserfordernisse aus Sicht des TLfDI

VBE Bundesvorstand

23. September 2016



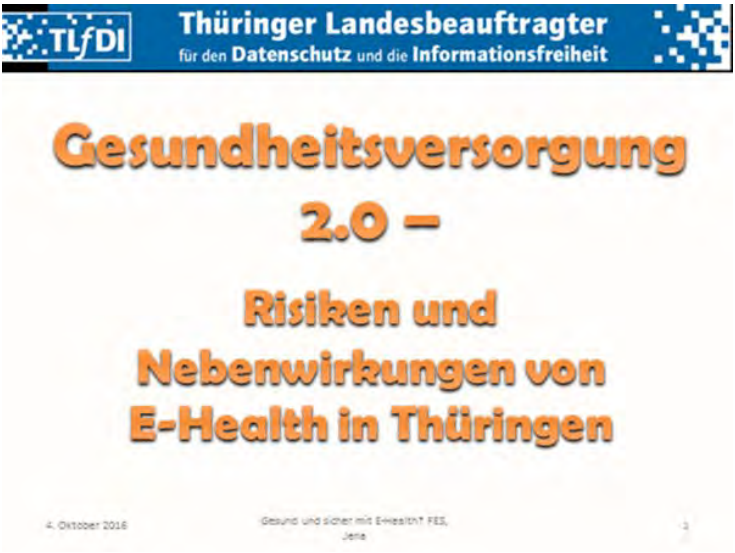
Inhalt:

Datensicherheit an Schulen
Privatsphärenschutz an Schulen

Gesundheitsversorgung 2.0 –
Risiken und Nebenwirkungen von
E-Health in Thüringen

FES – Jena

4. Oktober 2016



Inhalt:

Was ist überhaupt E-Health?
Vorteile und Gefahren
Recht
Aktuelle Beispiele
Bedrohungen des Grundrechts

Gespräch FH Erfurt, Angewandte Informatik

„Mein zweites Ich – Profilbildung und Verwertung meiner Person“
Unterstützungsangebot des TLfDI für Thüringer Schulen

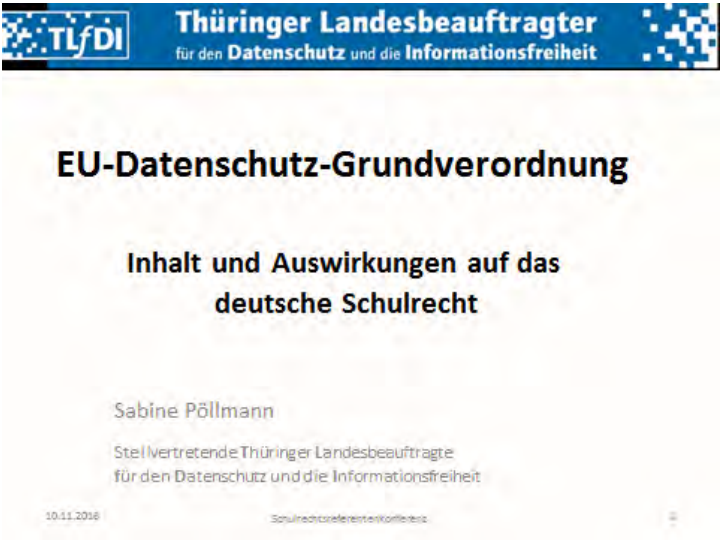
19. Oktober 2016



Inhalt:

Gesetzliche Regelungen zum Beschäftigtendatenschutz
Videoüberwachung – Was ist zulässig/unzulässig?
Erläuterung anhand von Praxisbeispielen
Technische und organisatorische Maßnahmen
Eingriffsbefugnisse und Sanktionen
Ausblick zum „Beschäftigtendatenschutzgesetz“

10. November 2016



Inhalt:

Hintergründe
Grundsätzliches
Kapitel der DS-GVO
Konsequenzen für das Schulrecht

Connected-Cars
DatenSchleuderTrauma

Tagung Autorecht
FSU Jena

11. November 2016



Inhalt:

Motivation
Das Auto der Zukunft (etwas) durchleuchtet
Rechtsgrundlagen
Rechtliche Problemfelder und die Sicht des Datenschutzes

#exitingEDU – Lehrerkongress 2016

18. November 2016



Inhalt:

Arbeitskreis „Datenschutz und Bildung“ (AK DuB)
im Kontext der Datenschutzkonferenz
Initiativen des AK DuB – Exemplarische Beispiele

Datenschutz in schulischem Kontext

Veranstaltung im Studienseminar Erfurt

1. Februar 2017



Inhalt:

Das Grundrecht auf informationelle Selbstbestimmung
Datenschutz – Zweck und Rechtsgrundlagen
Datenschutz und Thüringer Schule

Sicherheit von sozialen Netzwerken

3. Datenschutztag Stoyschule

8. März 2017



Inhalt:

Sicherheit von sozialen Netzwerken
- Sicherheit
- Soziale Netzwerke
- Was ist das überhaupt?

B90Grüne Digitaltour 2017

28. Juni 2017



Inhalt:

Struktur und Aufgaben der Behörde
Künftige Herausforderung – Datenschutz-Grundverordnung
Herausforderung Digitalisierung der Gesellschaft

Taskforce „Datenschutz in der Schulcloud“

12. Juli 2017



Inhalt:

Datenschutz in schulischem Kontext?
Gegenwärtiger und zukünftiger Rechtsrahmen
Schlussfolgerungen für die technische Gestaltung
digitaler Bildungsmedien

Tagung Autorecht „Datenschutz und Fahrzeug?“

05. Oktober 2017



Inhalt:

Informationsflüsse im Auto
Rechtsgrundlagen des Datenschutzes
Rechtliche Problemfelder und die Sicht des Datenschutzes

B90Grüne Digitaltour 2017

28. Juni 2017



Inhalt:

Struktur und Aufgaben der Behörde
Künftige Herausforderung – Datenschutz-Grundverordnung
Herausforderung Digitalisierung der Gesellschaft

Anlagen

Anlage 1

Entschließung
der 91. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 6./7. April 2016 in Schwerin

Stärkung des Datenschutzes in Europa – nationale Spielräume nutzen

Nach vier Jahren intensiver Diskussion ist der Text der Europäischen Datenschutz-Grundverordnung nun zwischen der Europäischen Kommission, dem Europäischen Parlament und dem Rat der Europäischen Union abgestimmt. Mit der Grundverordnung verfügt die EU über ein weiterentwickeltes, einheitliches Datenschutzrecht, das für Unternehmen und Behörden in Deutschland weitgehend Kontinuität gewährleistet. Überall in Europa soll künftig dasselbe Schutzniveau für das Grundrecht auf Datenschutz gelten. Ebenso wird feststehen, dass sich auch außereuropäische Anbieter, die ihre Waren und Dienstleistungen auf dem europäischen Markt anbieten, an das europäische Datenschutzrecht halten müssen.

Wichtige datenschutzrechtliche Prinzipien wie der Grundsatz des Verbots mit Erlaubnisvorbehalt, der Zweckbindungsgrundsatz und der Grundsatz der Datensparsamkeit sind in den Verhandlungen weitgehend erhalten geblieben.

Nach der Einschätzung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder ist es allerdings zur Erhaltung und Verstärkung des bestehenden Datenschutzniveaus auch im Lichte der jüngeren Entscheidungen des Europäischen Gerichtshofs geboten, die in der Grundverordnung enthaltenen Öffnungs- und Konkretisierungsklauseln zu Gunsten des Rechts auf informationelle Selbstbestimmung zu nutzen. Auch die von der Grundverordnung getroffenen Weiterentwicklungen des Datenschutzes wie beispielsweise die Grundsätze des Datenschutzes durch Technik und durch datenschutzfreundliche Voreinstellungen sowie das Erfordernis von Datenschutz-Folgeabschätzungen müssen wirksam ausgestaltet werden. Die Konferenz fordert deshalb Bundes- und

Landesgesetzgeber auf, in allen gesetzgeberischen Bereichen die nationalen Spielräume im Sinne des Grundrechts auf informationelle Selbstbestimmung zu nutzen.
Insbesondere folgenden Regelungen kommt in diesem Zusammenhang hohe Bedeutung zu:

- Schaffung eines Beschäftigtendatenschutzgesetzes, mindestens jedoch Beibehaltung der §§ 3 Abs. 11, 32 BDSG (Art. 88 i. V. m. Erwägungsgrund [EG] 155),
- Beschränkungen für die Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten (Art. 9 Abs. 4 i. V. m. EG 53, letzte beide Sätze),
- Stärkung der Befugnisse der Aufsichtsbehörden, insbesondere Schaffung von Klagebefugnissen und effektiven Sanktionen auch gegenüber Behörden (Art. 58 und 83 Abs. 7 i. V. m. EG 150, vorletzter Satz),
- jedenfalls im öffentlichen Bereich durch die Nennung der Schutzziele Datensparsamkeit, Vertraulichkeit, Integrität, Verfügbarkeit, Nichtverkettbarkeit, Transparenz und Intervenierbarkeit, um einen einfachen, flexiblen und praxistauglichen technischen und organisatorischen Datenschutz zu konkretisieren (Art. 6 Abs. 2, 25, 32),
- Begrenzung der Zweckänderung bei Videoüberwachung öffentlich zugänglicher Räume durch Private, soweit dies zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist (Art. 6 Abs. 4),
- Beibehaltung der Verpflichtung in § 4f Abs. 1 BDSG, einen betrieblichen Datenschutzbeauftragten zu bestellen (Art. 37 Abs. 4).

Anlage 2

Entschließung
der 91. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 6./7. April 2016 in Schwerin

Datenschutz bei Servicekonten

Der IT-Planungsrat hat sich in einem Beschluss in seiner 17. Sitzung im Juni 2015 für eine flächendeckende Verbreitung sogenannter Servicekonten für Bürgerinnen, Bürger und Unternehmen ausgesprochen. Über diese Konten soll es künftig möglich sein, sich einfach für die Inanspruchnahme von Verwaltungsdienstleistungen auf kommunaler, Länder- und Bundesebene zu identifizieren. Dabei soll der neue Personalausweis mit seiner eID-Funktion eine wichtige Rolle spielen. Eine Projektgruppe des IT-Planungsrates erarbeitet zurzeit die rechtlichen und technischen Rahmenbedingungen für Servicekonten.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder nimmt die Aktivitäten des IT-Planungsrates zur Kenntnis, den Zugang zu elektronischen Verwaltungsdienstleistungen zu erleichtern und möglichst medienbruchfrei auszugestalten. Sie weist darauf hin, dass insbesondere die Einrichtung von länderübergreifenden Servicekonten gewichtige verfassungsrechtliche Fragen etwa zum Bund-Länder-Verhältnis und zum Persönlichkeitsrecht aufwerfen. So ist dabei das Verbot einer Vorratsdatenspeicherung zu unbestimmten Zwecken sowie das grundrechtliche Prinzip der informationellen Gewaltenteilung zu beachten. Servicekonten dürfen die gesetzliche Zuständigkeits- und Aufgabenverteilung der öffentlichen Verwaltung nicht unterlaufen.

Hiervon abgesehen müssen jedenfalls die Datenschutzprinzipien der Datensparsamkeit, der Nichtverkettbarkeit und der Transparenz berücksichtigt werden. Für die Integration von Verwaltungsdienstleistungen heißt das insbesondere, dass auch die Schnittstellen zwischen den Systemen so definiert sein müssen, dass nur die für den vorgesehenen Zweck erforderlichen Daten übertragen werden. Dazu sind folgende Rahmenbedingungen einzuhalten:

Auch künftig muss es möglich sein, ohne Servicekonto Verwaltungsdienstleistungen in Anspruch zu nehmen.
Die einmalige Inanspruchnahme von Verwaltungsdienstleistungen muss auch ohne dauerhafte Speicherung identifizierender Daten möglich sein. Für diese Zwecke sollten temporäre Servicekonten eingerichtet werden.
Bürgerinnen und Bürgern muss die Möglichkeit eingeräumt werden, sowohl einzelne, im permanenten Servicekonto dauerhaft gespeicherte, personenbezogene Daten als auch das Konto selbst löschen zu lassen.
Soweit Daten aus dem Servicekonto übermittelt werden, müssen diese Übermittlungen durch die Bürger im Servicekonto selbst nachvollzogen werden können.
Für die Erhebung personenbezogener Daten in behördenübergreifenden Servicekonten ist eine Rechtsgrundlage erforderlich, da sie als Aufgabe verwaltungsorganisationsrechtlich einer Stelle zugewiesen werden muss. Der Staat darf personenbezogene Daten zur Erfüllung seiner gesetzlichen Aufgaben grundsätzlich nur auf der Basis einer klaren Rechtsgrundlage verarbeiten. Da zudem die Bedeutung dieser Servicekonten zunehmen wird und absehbar ist, dass den Betroffenen durch die Nutzung dieser Konten erhebliche Vorteile im Sinne von „Digital by Default“ eingeräumt werden sollen, reicht die Einwilligung als Rechtsgrundlage für die Datenerhebung nicht aus.
Vorbehaltlich weiterer verfassungsrechtlicher Prüfungen ist für die länderübergreifende Nutzung von Servicekonten eine Rechtsgrundlage erforderlich. Durch die dauerhafte Speicherung identifizierender Daten werden bundesweit nutzbare Servicekonten zu einer digitalen Meldestelle bzw. zu einer zweiten, zentralen Identifizierungsstelle neben den Meldebehörden aufgewertet. Die Rechtsgrundlage muss eindeutige Vorgaben zum Datenumfang, zu Zweckbindungsregelungen, zur Löschung und zur Transparenz der Datenverarbeitung enthalten. Daten der Betroffenen sind alleine zum Betrieb des Serviceportals und zur Erledigung der Verfahren der Nutzer zu verarbeiten. Eine Nutzung dritter Stellen zu anderen Zwecken ist gesetzlich ausdrücklich auszuschließen.
Bevor Unternehmen verpflichtet werden sollen, die eID-Funktion für Verwaltungsangelegenheiten zu nutzen, ist zu prüfen, ob und unter welchen Voraussetzungen der Einsatz privater digitaler Identifikationsnachweise zu nicht-privaten Zwecken bzw. zur Erfüllung arbeits-

vertraglicher Pflichten zulässig ist und inwieweit Arbeitnehmerinnen und Arbeitnehmer hierzu verpflichtet werden können.
Angesichts des Abhängigkeitsverhältnisses der Arbeitnehmerinnen und Arbeitnehmer im Beschäftigungsverhältnis kann die Nutzung von Servicekonten auf der Basis der privaten eID-Funktion keinesfalls auf der Einwilligungsbasis erfolgen. Auch hierfür ist eine Rechtsgrundlage erforderlich, die die Datenverarbeitung in Servicekonten vollständig erfasst. Bei der Identifizierung eines bevollmächtigten Beschäftigten dürfen nur die für diese Identifizierung erforderlichen Daten erfasst werden.

Sichere, elektronische Identifizierungsmöglichkeiten können zur Datenschutzkonformität von E-Government- und von E-Commerce-Verfahren beitragen. Die unabhängigen Datenschutzaufsichtsbehörden begrüßen daher Maßnahmen, die zur verstärkten Nutzung der eID-Funktion des neuen Personalausweises beitragen. Dennoch muss den Betroffenen die Möglichkeit gelassen werden, selbst zu entscheiden, ob sie die eID-Funktion freischalten und nutzen wollen. Die Datenschutzkonferenz lehnt daher die angedachte Änderung des Personalausweisgesetzes ab, wonach die eID-Funktion des neuen Personalausweises dauerhaft eingeschaltet wäre und nicht mehr deaktiviert werden könnte. Eine standardmäßige Aktivierung der eID-Funktion wäre allenfalls dann hinnehmbar, wenn den Bürgerinnen und Bürgern ein Opt-In mit Widerrufsmöglichkeit angeboten wird, um die eID-Funktion jederzeit gebührenfrei aktivieren und deaktivieren zu können.

Anlage 3

Entschließung
der 91. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 6./7. April 2016 in Schwerin

Wearables und Gesundheits-Apps –
Sensible Gesundheitsdaten effektiv schützen!

Die Datenschutzkonferenz tritt für einen effektiven Schutz der Persönlichkeitsrechte der Nutzerinnen und Nutzer von Wearables und Gesundheits-Apps ein. Einer repräsentativen Umfrage zufolge soll bereits knapp ein Drittel der Bevölkerung ab 14 Jahren sogenannte Fitness-Tracker zur Aufzeichnung von Gesundheitswerten und persönlichen Verhaltensweisen nutzen. Am Körper getragene Kleincomputer (sog. Wearables) und auf mobilen Endgeräten installierte Anwendungsprogramme (sog. Gesundheits-Apps) sammeln und dokumentieren auswertungsfähige Körperdaten. In der Regel werden diese Daten über das Internet an Hersteller, Internetanbieter und sonstige Dritte weitergeleitet.

Die digitale Sammlung und Auswertung der eigenen gesundheitsbezogenen Daten können durchaus interessante Informationen für Einzelne bieten, die zu einer besseren Gesundheitsversorgung und einem Zugewinn an persönlicher Lebensqualität beitragen können.

Allerdings stehen diesen Chancen auch Risiken, insbesondere für das Persönlichkeitsrecht, gegenüber. Zahlreiche Wearables und Gesundheits-Apps geben die aufgezeichneten Daten an andere Personen oder Stellen weiter, ohne dass die betroffenen Personen hiervon wissen oder dazu eine bewusste Entscheidung treffen. Darüber hinaus können Bedienungsfehler oder unzureichende technische Funktionalitäten dazu führen, dass Gesundheitsinformationen ungewollt preisgegeben werden. Einige Angebote weisen erhebliche Sicherheitsdefizite auf, sodass auch Unbefugte sich Zugriff auf die Gesundheitsdaten verschaffen können. Für bestimmte Situationen besteht überdies das Risiko, dass Einzelne aufgrund massiver gesellschaftlicher, sozialer oder ökonomischer Zwänge nicht frei über die Nutzung derartiger Technologien entscheiden können. Zum notwen-

digen Schutz von Gesundheitsdaten bei Wearables und Gesundheits-Apps weist die Datenschutzkonferenz auf folgende Gesichtspunkte hin:

Die Grundsätze der Datenvermeidung und Datensparsamkeit sind zu beachten. Insbesondere Hersteller von Wearables und Gesundheits-Apps sind aufgerufen, datenschutzfreundliche Technologien und Voreinstellungen einzusetzen (Privacy by Design and Default). Hierzu gehören Möglichkeiten zur anonymen bzw. pseudonymen Datenverarbeitung. Soweit eine Weitergabe von Gesundheits- und Verhaltensdaten an Dritte nicht wegen einer medizinischen Behandlung geboten ist, sollten Betroffene sie technisch unterbinden können (lediglich lokale Speicherung).
Die Datenverarbeitungsprozesse, insbesondere die Weitergabe von Gesundheits- und Verhaltensdaten an Dritte, bedürfen einer gesetzlichen Grundlage oder einer wirksamen und informierten Einwilligung. Sie sind transparent zu gestalten. Für das Persönlichkeitsrecht riskante Datenverwendungen, insbesondere Datenflüsse an Dritte, sollten für die Nutzerinnen und Nutzer auf einen Blick erkennbar sein. Beispielsweise könnte die Anzeige des Vernetzungsstatus' die aktuellen Weitergabe-Einstellungen veranschaulichen. Eine solche Verpflichtung zur erhöhten Transparenz sollte gesetzlich verankert werden.
Einwilligungserklärungen und Verträge, die unter Ausnutzung eines erheblichen Verhandlungsungleichgewichts zwischen Verwendern und den betroffenen Personen zustande kommen, sind unwirksam und liefern keine Rechtsgrundlage für Verarbeitungen. Das gilt namentlich für besonders risikoträchtige Verwendungszusammenhänge, etwa in Beschäftigungs- und Versicherungsverhältnissen.
Verbindliche gesetzliche Vorschriften zur Datensicherheit, insbesondere zur Integrität und Vertraulichkeit von Daten, können nicht durch Verträge oder durch Einwilligungserklärungen abbedungen werden.
Wer aus eigenen Geschäftsinteressen gezielt bestimmte Wearables und Gesundheits-Apps in den Umlauf bringt oder ihren Vertrieb systematisch unterstützt, trägt eine Mitverantwortlichkeit für die rechtmäßige Ausgestaltung solcher Angebote. In diesem Sinne Mitverantwortliche haben sich zu vergewissern, dass die Produkte verbindlichen Qualitätsstandards an IT-Sicherheit, Funktionsfähigkeit sowie an Transparenz der Datenverarbeitung genügen.

Die Datenschutzkonferenz fordert den Gesetzgeber auf zu prüfen, ob und inwieweit im Zusammenhang mit Wearables und Gesundheits-Apps die Möglichkeit beschränkt werden sollte, materielle Vorteile von der Einwilligung in die Verwendung von Gesundheitsdaten abhängig zu machen.

Anlage 4

Entschließung
der 91. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 6./7. April 2016 in Schwerin

Wahrung der Freiheits- und Persönlichkeitsrechte bei der Bekämpfung des internationalen Terrorismus

Rechtsstaat und Grundrechtsschutz – damit auch Datenschutz – stehen einer effektiven Bekämpfung des Terrorismus nicht entgegen.
Auch nach Brüssel gilt: Datenschutz verhindert nicht, Terroristen und ihre Helfernetzwerke zu erfassen und zu bekämpfen. Das geltende Datenschutzrecht erlaubt, deren Daten zu speichern und Informationen wechselseitig auszutauschen. Der Datenschutz kann jedenfalls nicht für etwaige Defizite bei der Nutzung vorhandener Eingriffsbefugnisse sowie für möglicherweise ineffiziente sicherheitsbehördliche Strukturen verantwortlich gemacht werden.
Die häufig reflexartig erhobene Forderung nach weiteren Eingriffsbefugnissen und flächendeckenden Überwachungsmaßnahmen trägt zur Bekämpfung des internationalen Terrorismus nicht bei.
Es kennzeichnet den Rechtsstaat, dass sich jeder in einem fairen Verfahren gegen unberechtigte Verdachtsbehauptungen wehren, Schutz bei Gerichten suchen und auf die Kontrolle der Datenschutzbeauftragten vertrauen darf. Die massenhafte, verdachtsunabhängige Erhebung und Speicherung von Daten widerspricht dem Grundrecht auf Datenschutz.
Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bekräftigt ihren mehrfach formulierten Appell*, dass alle neu erwogenen Maßnahmen zur Bekämpfung des internationalen Terrorismus sich daran messen lassen müssen, ob sie für dessen wirkungsvolle Bekämpfung wirklich geeignet, erforderlich und angemessen sind und damit dem Verfassungsgrundsatz der Verhältnismäßigkeit entsprechen.

*) - Entschließung der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 25./26. Oktober 2001 in Münster

- Entschließung der 72. Konferenz der Datenschutzbeauftragten des Bundesund der Länder am 26./27. Oktober 2006 in Naumburg
- Entschließung der 82. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 28./29. September 2011 in München
- Entschließung der 89. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 18./19. März 2015 in Wiesbaden

Anlage 5

Entschließung zwischen den Konferenzen 2016

Klagerecht für Datenschutzbehörden
EU-Kommissionentscheidungen müssen gerichtlich überprüfbar sein
(Umlaufentschließung vom 20. April 2016)

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz) fordert den Gesetzgeber auf, umgehend ein eigenständiges Klagerecht für die unabhängigen Datenschutzbehörden vorzusehen. Wenn die unabhängigen Datenschutzbehörden der Auffassung sein sollten, dass eine Entscheidung der EU-Kommission rechtswidrig ist, wären sie gleichwohl an diese gebunden. Sie müssten daher ggf. gegen den rechtsstaatlichen Grundsatz der Gesetzmäßigkeit der Verwaltung verstoßen. Um dies zu verhindern, sind die prozessualen Voraussetzungen dafür zu schaffen, dass die Datenschutzbehörden selbst bestehende Zweifel an der Rechtmäßigkeit einer Kommissionsentscheidung gerichtlich klären lassen können.

Anlass für die obige Aufforderung der Datenschutzkonferenz ist die zwischenzeitliche Vorlage einer Reihe von Dokumenten unterschiedlicher Repräsentanten der US-Administration durch die EU-Kommission am 29. Februar 2016, die für Unternehmen und Behörden Zusagen für den Umgang mit aus der EU übermittelten personenbezogenen Daten enthalten. Im Rahmen eines so genannten EU-US Privacy Shield sollen diese Dokumente Grundlage für eine künftige EU-Kommissionsentscheidung zur Angemessenheit des Datenschutzniveaus in den USA sein und damit als Nachfolgeregelung für die Safe Harbor-Entscheidung dienen. Letztere wurde bekanntlich am 6. Oktober 2015 durch den Europäischen Gerichtshof aufgehoben.

Gegen den „EU-US Privacy Shield“ bestehen jedoch nach Auffassung der Artikel-29-Datenschutzgruppe, dem Zusammenschluss der Datenschutzbehörden der EU-Mitgliedstaaten und des Europäischen Datenschutzbeauftragten, erhebliche Bedenken. Die Artikel-29-Datenschutzgruppe hat zum „EU-US Privacy Shield“ zuletzt am 13. April 2016 detailliert Stellung genommen. Die Datenschutzkon-

ferenz teilt diese umfassende Analyse und unterstützt die darin enthaltene Forderung an die EU-Kommission, vor einer Beschlussfassung substantielle Nachbesserungen vorzunehmen. Die Datenschutzkonferenz ist der Auffassung, dass auch der „EU-US Privacy Shield“ in seiner derzeitigen Form nicht ausreichend ist, das für die Übermittlung personenbezogener Daten in die USA erforderliche „angemessene Datenschutzniveau“ in den USA zu gewährleisten.

Der EuGH stellt in seiner o. g. Entscheidung zur Ungültigkeit von Safe Harbor ausdrücklich klar, dass nach Maßgabe der Datenschutz-Richtlinie der nationale Gesetzgeber für die Datenschutzbehörden Rechtsbehelfe vorzusehen hat, die ihnen bei rechtlichen Zweifeln über eine Angemessenheitsentscheidung die Anrufung nationaler Gerichte ermöglichen, sodass diese den EuGH um eine Entscheidung über die Vereinbarkeit mit den europäischen Grundrechten ersuchen können.

Die Datenschutzkonferenz begrüßt und unterstützt daher ausdrücklich die Bundesratsinitiative der Freien und Hansestadt Hamburg zur zeitnahen Einräumung eines Klagerechts für die Datenschutzaufsichtsbehörden von Bund und Ländern (BR-Drs. 171/16), in der nochmals deutlich gemacht wird, „dass das vom Europäischen Gerichtshof (EuGH in seinem Urteil vom 6. Oktober 2015, Rechtssache C-362/14) statuierte Klagerecht für Datenschutzaufsichtsbehörden für die Gewährleistung einer effektiven Datenschutzkontrolle von besonderer Bedeutung ist“.

Anlage 6

Pressemitteilung
Zur Entschließung der unabhängigen Datenschutzbehörden des Bundes und der Länder
vom 20. April 2016 „Klagerecht für Datenschutzbehörden“

Anlässlich der aktuellen öffentlichen Diskussion zum sogenannten EU-US Privacy Shield hat die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) am 20. April 2016 eine Entschließung verabschiedet, in der die rasche Schaffung eines Klagerechtes auch für die deutschen Datenschutzbehörden gefordert wird (abrufbar unter https://www.datenschutz-mv.de/datenschutz/themen/beschlue/ent_klagerecht.html).



Diese Forderung richtet sich an den deutschen Gesetzgeber, der erst mit der Schaffung eines solchen Klagerechtes die deutschen Datenschutzbehörden in die Lage versetzen würde, die Rechtmäßigkeit des EU-US Privacy Shields gerichtlich klären zu lassen. Hiermit würde der einschlägigen Rechtsprechung des EuGH entsprochen, der in seiner Entscheidung zur Ungültigkeit von Safe Harbor ausdrücklich klarstellte, dass der nationale Gesetzgeber für die Datenschutzbehörden Rechtsbehelfe vorzusehen hat, die ihnen bei rechtlichen Bedenken gegen eine Angemessenheitsentscheidung der Kommission (EU-US Privacy Shield) die Anrufung nationaler Gerichte ermöglichen.

Aus den genannten Gründen begrüßt die DSK ausdrücklich die aktuelle Hamburger Bundesratsinitiative (BR-Drs. 171/16), in der deutlich gemacht wird, dass der EuGH in seinem Urteil vom 6. Oktober 2015 die Notwendigkeit eines Klagerechtes der Datenschutzbehörden betont hat, weil es für die Gewährleistung einer effektiven Datenschutzkontrolle von besonderer Bedeutung ist.

Anlage 7

Entschließung zwischen den Konferenzen 2016 [4]

EU-Datenschutz-Grundverordnung
erfordert zusätzliche Ressourcen für Datenschutzbehörden
(Umlaufentschließung vom 25. Mai 2016)

Am 14. April 2016 hat das Europäische Parlament dem neuen Rechtsrahmen für den Datenschutz in Europa zugestimmt. Wesentlicher Teil des Rechtsrahmens ist die EU-Datenschutz-Grundverordnung, deren Text am 4. Mai 2016 im Amtsblatt der Europäischen Union veröffentlicht wurde. Die Verordnung ist am 25. Mai 2016 in Kraft getreten und zwei Jahre später verbindlich in allen Mitgliedstaaten der Europäischen Union anzuwenden.
Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder weist darauf hin, dass mit der EU-Datenschutz-Grundverordnung eine Reihe neuer bzw. erweiterter Aufgaben auf sie zukommen. Hierzu gehören insbesondere:
Bearbeitung von Beschwerden und Beratung Betroffener sowie datenschutzrechtliche Beratung und Kontrolle von Unternehmen nunmehr unter Beachtung des erweiterten räumlichen Anwendungsbereichs der Verordnung (Marktortprinzip),
verpflichtende Beratung von Behörden und Unternehmen bei der Datenschutz-Folgenabschätzung, insbesondere im Rahmen der vorherigen Konsultation der Aufsichtsbehörde, sowie Beratung bei der Umsetzung neuer Anforderungen wie Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen (Privacy By Design, Privacy By Default),
Aufbau und Anwendung eines Kooperationsverfahrens zwischen Datenschutzbehörden in Europa bei grenzüberschreitenden Datenverarbeitungen (One-Stop-Shop), Verpflichtung zur gegenseitigen Amtshilfe und umfassender Austausch von Informationen zwischen federführenden und betroffenen Aufsichtsbehörden jeweils mit kurzen Bearbeitungsfristen, Etablierung eines Kohärenzverfahrens zwi-

[4] Enthaltung Bayern (Bayerischer Landesbeauftragter für den Datenschutz und Bayerisches Landesamt für Datenschutzaufsicht)

schen den Datenschutzbehörden in Europa, Gewährleistung der europaweit einheitlichen Anwendung der Verordnung, Mitwirkung im Europäischen Datenschutzausschuss, europaweit einheitliche Auslegung der Grundverordnung in Bezug auf fehlende Regelungen (z. B. zur Videoüberwachung oder zum Scoring) und neue Anforderungen (z. B. Recht auf transparente Information oder Recht auf Datenübertragbarkeit), Erarbeitung von Stellungnahmen und Billigung von branchenspezifischen Verhaltensregeln zur ordnungsgemäßen Anwendung der Verordnung, Erarbeitung von Zertifizierungskriterien, ggf. Durchführung von Zertifizierungen, Erarbeitung von Kriterien für die Akkreditierung von Zertifizierungsstellen, ggf. Durchführung der Akkreditierung, Bearbeitung von gerichtlichen Rechtsbehelfen Betroffener gegen Entscheidungen von Aufsichtsbehörden, Ausübung neuer bzw. erweiterter Befugnisse der Datenschutzbehörden zur Erteilung von Anordnungen gegenüber den Verantwortlichen nunmehr auch im öffentlichen Bereich sowie Berücksichtigung zusätzlicher Tatbestände für Ordnungswidrigkeiten und eines erweiterten Bußgeldrahmens.

Die Europäische Datenschutz-Grundverordnung verpflichtet die Mitgliedstaaten, die Aufsichtsbehörden zur Gewährleistung ihrer Unabhängigkeit mit den erforderlichen personellen, finanziellen und technischen Ressourcen auszustatten (Art. 52 Abs. 4 DS-GVO). Aus Sicht der Datenschutzkonferenz ist es für die Bewältigung der neuen Aufgaben zwingend erforderlich, für die Datenschutzbehörden in Deutschland erweiterte personelle und finanzielle Ressourcen vorzusehen. Dies gilt bereits für die jetzt laufende Vorbereitungsphase, in der die Weichen für eine funktionierende Umsetzung der Datenschutz-Grundverordnung gestellt werden. Die Konferenz appelliert deshalb an die Gesetzgeber in Bund und Ländern, rechtzeitig die haushaltsrechtlichen Vorkehrungen für eine jeweils angemessene, erweiterte Ausstattung der Datenschutzbehörden zu treffen. Nur so lassen sich die zusätzlichen Aufgaben der Datenschutz-Grundverordnung von den Datenschutzbehörden in Deutschland effektiv wahrnehmen.

Anlage 8

Entschließung
der 92. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 9./10. November 2016 in Kühlungsborn

Gemeinsame Prüfung der „Falldatei Rauschgift“ deckt gravierende Mängel auf
Konsequenzen für polizeiliche Datenverarbeitung notwendig

Die Datenschutzbeauftragten des Bundes und der Länder[5] Baden-Württemberg, Bayern, Berlin, Brandenburg, Bremen, Hessen, Niedersachsen, Nordrhein-Westfalen, Rheinland-Pfalz, Sachsen-Anhalt, Schleswig-Holstein und Thüringen haben parallel die bundesweit geführte „Falldatei Rauschgift“ (FDR) datenschutzrechtlich geprüft.

Die FDR ist eine bundesweite Verbunddatei, in der Informationen über sichergestellte Drogen und Verstöße gegen das Betäubungsmittelgesetz gespeichert werden. Sie wird auf Grundlage des Bundeskriminalamtgesetzes (BKAG) zentral beim Bundeskriminalamt geführt. Die Polizeien aller Länder und die Zollfahndung haben Zugriff auf die Datei und können direkt Daten einspeichern und abrufen. Die Datenschutzbeauftragten haben im Rahmen ihrer Kontrollen sowohl die Struktur der Datei als auch Einzelspeicherungen überprüft.

Die Prüfung hat im Wesentlichen folgende Mängel aufgedeckt:

Vielfach haben die Behörden nicht ausreichend geprüft, ob die Voraussetzungen des § 2 BKAG (Straftat von länderübergreifender oder erheblicher Bedeutung) und des § 8 Abs. 2 BKAG (Negativprognose) vorliegen.
Verbreitet fehlt es an einer nachvollziehbaren Dokumentation des Vorliegens der gesetzlichen Speicherungsvoraussetzungen.
Dementsprechend fanden sich in der bundesweit abrufbaren Datei vielfach Speicherungen, die dem Bereich der Bagatellkriminalität

[5] Bei Enthaltung Hamburgs

zuzuordnen sind. Auch wurden Personen gespeichert, bei denen kein hinreichender polizeilicher Restverdacht festzustellen war.
Das Ergebnis des jeweiligen Strafverfahrens war bei vielen Einträgen nicht berücksichtigt – entweder aufgrund organisatorischer Mängel oder weil die nach § 482 Absatz 2 Strafprozessordnung (StPO) notwendige Mitteilung der Staatsanwaltschaft unterblieb.

Die Ergebnisse machen deutlich:

Es ist wichtig, die konkrete Zwecksetzung jeder Datei in einer Errichtungsanordnung festzulegen. Die Voraussetzungen, wann welche Daten für den jeweiligen Zweck erforderlich sind und welcher Personenkreis erfasst werden darf, müssen genau definiert werden.
Bagatellfälle in Verbunddateien zu speichern, ist auch im Hinblick auf die bundesweite Abrufbarkeit der Daten unverhältnismäßig.
In der Praxis ist sicherzustellen, dass in Verbunddateien alle Speichervoraussetzungen, vor allem die Negativprognose, durchgehend und gründlich bezogen auf den jeweiligen Einzelfall dokumentiert werden.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) fordert, nicht nur in der „Falldatei Rauschgift“ die Mängel zu beheben. Vielmehr fordert sie die Einhaltung der grundlegenden Standards für jedwede Speicherung in Verbunddateien der Polizei. Erst recht ist dies erforderlich vor dem Einsatz der neuen Datei zur Betäubungsmittelkriminalität im Polizeilichen Informations- und Analyseverbund (PIAV), die voraussichtlich im kommenden Jahr die FDR ablösen wird. Die Daten aus der FDR dürfen nicht pauschal übernommen werden.

Anlage 9

Entschließung
der 92. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 9./10. November 2016 in Kühlungsborn

„Videoüberwachungsverbesserungsgesetz“ zurückziehen!

Das Vorhaben des Bundesministeriums des Innern (BMI), durch ein „Videoüberwachungsverbesserungsgesetz“ Änderungen des Bundesdatenschutzgesetzes (BDSG) einzuführen, die künftig privaten Stellen den Betrieb von Videokameras zur Verhinderung von Anschlägen wie in Ansbach und Amokläufen wie in München erleichtern sollen, wird von den unabhängigen Datenschutzbehörden des Bundes und der Länder[6] abgelehnt. Der Gesetzentwurf vermag nicht zu begründen, dass die angestrebte Erleichterung der Videoüberwachung die öffentliche Sicherheit besser gewährleisten kann, als dies gegenwärtig der Fall ist. Auch die Verlagerung der Verantwortung für diese Aufgabe auf die privaten Betreiber von Einkaufszentren und öffentlichem Personennahverkehr lehnen die unabhängigen Datenschutzbehörden des Bundes und der Länder ab. Nach der nicht abschließenden Aufzählung zielt der Gesetzentwurf überwiegend auf Orte, an denen Betroffene ihre Freizeit verbringen. Gerade in diesen Bereichen, in denen sich Menschen typischerweise zur ungezwungenen Kommunikation, Erholung und Entspannung für längere Dauer aufhalten, gilt es, das Persönlichkeitsrecht in besonderem Maße zu schützen.

Gleichwohl lässt es die einschlägige Bestimmung des § 6b BDSG bereits gegenwärtig zu, die Sicherheitsbelange von Personen, die sich in öffentlich zugänglichen Bereichen aufhalten, bei der Abwägung zwischen den Rechten Betroffener und den Betreiberinteressen zu berücksichtigen. Im Rahmen der Hausrechtsausübung können auch heute Kameras installiert werden, um Personen von Straftaten

[6] Bei Enthaltung der Bundesbeauftragten für Datenschutz und Informationsfreiheit

an den Objekten abzuhalten. Darüber hinaus kann Videotechnik zur Beweissicherung eingesetzt werden und nach § 6 Abs. 3 Satz 2 BDSG können Videobilder an Polizei-, Ordnungs- und Strafverfolgungs- und Ordnungsbehörden weitergegeben werden, wenn dies zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist. Die Begründung des BMI suggeriert, die Datenschutzaufsichtsbehörden verhinderten angesichts der angespannten Sicherheitslage die Durchführung von Videoüberwachung. Dies trifft nicht zu. Tatsächlich werden gerade im Bereich der großen Einkaufszentren, aber auch an Bahnhöfen und in Fahrzeugen des Personennahverkehrs bereits heute zahlreiche Kameras mit ausdrücklicher Billigung der Aufsichtsbehörden betrieben.
Terroristen wie auch irrational handelnde Einzeltäter, vor denen die gesetzliche Regelung schützen soll, nehmen ihren eigenen Tod bei derartigen Anschlägen bewusst in Kauf. Sie werden sich daher von ihren Taten auch nicht durch Videokameras abschrecken lassen.

Hinzu kommt, dass die Betreiber von Videoüberwachungsanlagen bereits heute meistens nicht in der Lage sind, ein Live-Monitoring durchzuführen und die Bilder der vielen Kameras durch ihr eigenes Personal so auszuwerten, dass bei Gefahren direkt und schnell eingegriffen werden kann. In der Praxis bleibt die Bedeutung der Kameras daher auf eine Speicherung auf Vorrat und für die spätere Strafverfolgung beschränkt. Auch die mögliche Erhöhung eines faktisch ungerechtfertigten subjektiven Sicherheitsgefühls könnte Grundrechtseingriffe nicht rechtfertigen. Insoweit ist die Regelung, die von den privaten Betreibern eine stärkere Gewichtung des Schutzes von Leben, Gesundheit oder Freiheit der Betroffenen bei der rechtlichen Abwägung fordert, letztlich gar nicht geeignet, das Ziel der gesetzlichen Regelung zu erreichen.
Die unabhängigen Datenschutzbehörden des Bundes und der Länder betonen mit Nachdruck, dass es nicht die Aufgabe privater Stellen ist, die Sicherheit der Bevölkerung zu gewährleisten. Dies obliegt allein den Sicherheitsbehörden, die über ausreichende landes- und bundesgesetzliche Grundlagen sowohl für die Gefahrenabwehr als auch für die Strafverfolgung verfügen. Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder fordert den Bundesinnenminister auf, den Gesetzentwurf zurückzuziehen.

Anlage 10

Entschließung zwischen den Konferenzen 2016/2017

Novellierung des Personalausweisgesetzes – Änderungen müssen bürger- und datenschutzfreundlich realisiert werden!
(Umlaufentschließung vom 24. Januar 2017)

Die Bundesregierung plant grundlegende Änderungen des Personalausweisrechts. Nach dem vom Bundeskabinett beschlossenen Gesetzentwurf (BR-Drs. 787/16) werden das Recht auf informationelle Selbstbestimmung der Bürgerinnen und Bürger übergangen und Datenschutz sichernde Standards unterlaufen. Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder fordert daher, insbesondere folgende datenschutzrechtliche Anforderungen zu berücksichtigen:

- Die obligatorische Aktivierung der eID-Funktion ist dann hinnehmbar, wenn dauerhaft sichergestellt ist, dass daraus keine verpflichtende Nutzung der eID-Funktion des Personalausweises resultiert. Die Entscheidung über die Nutzung der eID-Funktion muss allein bei den Bürgerinnen und Bürgern liegen. Deren Selbstbestimmungsrecht muss gewahrt bleiben.
- An der bisherigen Verpflichtung der Ausweisbehörden, Bürgerinnen und Bürger über die eID-Funktion des Personalausweises schriftlich zu unterrichten, sollte festgehalten werden. Nur durch eine bundesweit einheitliche Vorgabe zu einer solchen Information wird sichergestellt, dass alle Bürgerinnen und Bürger in hinreichend verständlicher Form aufgeklärt werden.
- Vor einer Datenübermittlung aus dem Personalausweis müssen die Bürgerinnen und Bürger Kenntnis über den Zweck der Übermittlung erhalten; zur Wahrnehmung des Rechts auf informationelle Selbstbestimmung müssen die Betroffenen stets – wie bislang – nachvollziehen können, in welchem konkreten Kontext ihre Identitätsdaten übermittelt werden. Zudem sollte die bisherige Möglichkeit, die Übermittlung einzelner Datenkategorien auszuschließen, beibehalten werden.
- Die Einführung von organisationsbezogenen Berechtigungszertifikaten bei Diensteanbietern wird abgelehnt. Um sicherzustellen, dass Diensteanbieter nur die für den jeweiligen Geschäftsprozess erforderlichen Angaben übermittelt bekommen, sollte an

der aktuellen Rechtslage festgehalten werden, nach der der antragstellende Diensteanbieter die Erforderlichkeit der aus der eID-Funktion des Personalausweises zu übermittelnden Angaben nachweisen muss und an den jeweils festgelegten Zweck gebunden ist.

- Berechtigungszertifikate dürfen nur an Diensteanbieter erteilt werden, die Datenschutz und Datensicherheit gewährleisten. Daher sollten antragstellende Diensteanbieter nach wie vor durch eine Selbstverpflichtung die Erfüllung dieser Anforderungen schriftlich bestätigen und nachweisen müssen.
- Die maßgeblichen Regelungen für die mit der Anlegung und Nutzung von Servicekonten einhergehende Erhebung und Verarbeitung von Identitätsdaten aus dem Personalausweis sowie die sicherheitstechnischen Rahmenbedingungen sollten im Personalausweisgesetz getroffen werden.
- Die Voraussetzungen für die Erstellung und Weitergabe von Personalausweisablichtungen sollten gesetzlich konkreter normiert werden. Insbesondere das Prinzip der Erforderlichkeit ist durch eine verpflichtende Prüfung der Notwendigkeit der Anfertigung einer Ablichtung sowie durch eine Positivliste von Erlaubnisgründen zu stärken. Die Einwilligung der Betroffenen als alleinige Voraussetzung birgt die Gefahr, dass in der Praxis Ablichtungen angefertigt werden, obwohl sie nicht erforderlich sind. Zudem dürfte fraglich sein, ob betroffene Personen in eine solche Maßnahme stets informiert und freiwillig einwilligen können.
- Die zum 1. Mai 2021 vorgesehene Einführung eines nahezu voraussetzungslosen Abrufs des Lichtbildes im automatisierten Verfahren durch die Polizeibehörden des Bundes und der Länder sowie die Verfassungsschutzbehörden und Nachrichtendienste wird abgelehnt. Bisher dürfen zur Verfolgung von Straftaten und Verkehrsordnungswidrigkeiten insbesondere die Polizei- und Ordnungsbehörden Lichtbilder automatisiert abrufen, wenn die Personalausweisbehörde nicht erreichbar ist und ein weiteres Abwarten den Ermittlungszweck gefährdet. Diese gesetzlichen Einschränkungen für das Abrufverfahren sollen nun entfallen. Zudem sollen alle Nachrichtendienste künftig voraussetzungslos Lichtbilddaten abrufen können. Die bisherige Rechtslage ist völlig ausreichend.

Anlage 11

Entschließung zwischen den Konferenzen 2016/2017

Neues Bundeskriminalamtgesetz – Informationspool beschneidet Grundrechte
(Umlaufentschließung vom 16. März 2017)

Der „Entwurf eines Gesetzes zur Neustrukturierung des Bundeskriminalamtgesetzes“ (BT-Drs. 18/11326 und 18/11163; BR-Drs. 109/17) ändert das polizeiliche Datenschutzrecht grundlegend und betrifft Polizeibehörden in Bund und Ländern gleichermaßen. Er beschränkt sich nicht darauf, die Vorgaben des Bundesverfassungsgerichts aus dem Urteil vom 20. April 2016 zum Bundeskriminalamtgesetz und aus der neuen EU-Richtlinie zum Datenschutz im Bereich Justiz und Inneres umzusetzen. Tatsächlich nimmt er sogar wichtige Datenschutzregeln und Verfahrenssicherungen zurück, die der Gesetzgeber nach dem Volkszählungsurteil des Bundesverfassungsgerichts geschaffen hatte.
Der Entwurf ändert den bisherigen Informationsverbund für alle Polizeibehörden grundlegend. Dieser ist nicht mehr nach Dateien untergliedert und führt zu unverhältnismäßig weitreichenden Speicherungen. In dieser Form ist dies weder durch das Urteil des Bundesverfassungsgerichts zum BKAG noch durch die EU-Richtlinie zum Datenschutz im Bereich Justiz und Inneres veranlasst. Das Urteil des Bundesverfassungsgerichts fordert, den Zweck der jeweiligen Ermittlungsmaßnahmen bei allen weiteren Schritten zu berücksichtigen, bei denen die ermittelten Daten verwendet werden. Nicht im Einklang damit steht es, Verfahrenssicherungen und datenschutzrechtliche Rahmenbedingungen aufzugeben.
Abzulehnen ist insbesondere der vorgesehene Verzicht auf Errichtungsanordnungen. Diese sind bislang Ausgangspunkt sowohl für datenschutzrechtliche Kontrollen als auch die Selbstkontrolle der Polizeibehörden. In ihnen wird festgelegt, zu welchen Zwecken personenbezogene Daten gespeichert sind. Dies ist eine wesentliche verfassungsrechtliche Vorgabe. Die neuen Regeln führen zu umfassenden themenübergreifenden Verknüpfungen und Abgleichen aller gespeicherten Personen. Sie verkürzen die Kontrollmöglichkeiten der Datenschutzaufsichtsbehörden von Bund und Ländern.

Ebenso sind die künftig durch die geplante „Mitziehautomatik“ erheblich längeren Speicherfristen abzulehnen. Die geplante Neuregelung hat zur Folge, dass alte Speicherungen – auch zu Personen, die lediglich im Verdacht standen, eine Straftat begangen zu haben und die nicht verurteilt wurden – bei jedem neuen Speicheranlass ungeprüft weiter fortgeschrieben werden. Dafür soll es schon genügen, wenn die betroffene Person als Zeuge oder Kontaktperson erneut in Erscheinung tritt. Auch dies verstößt gegen das durch die ständige Rechtsprechung des Bundesverfassungsgerichtes bekräftigte Übermaßverbot.
Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder fordert daher, den Gesetzentwurf in der parlamentarischen Beratung datenschutzkonform zu überarbeiten!

Anlage 12

Entschließung zwischen den Konferenzen 2016/2017

Gesetzesentwurf zur Aufzeichnung von Fahrdaten ist völlig unzureichend!
(Umlaufentschließung vom 16. März 2017)

Die Bundesregierung hat im Januar 2017 einen Entwurf zur Novellierung des Straßenverkehrsgesetzes (BT Drs. 18/11300) vorgelegt, um die Nutzung automatisierter Fahrfunktionen auf Deutschlands Straßen zu erlauben. Dabei sollen Fahrdaten aufgezeichnet werden, anhand derer bewertet werden kann, zu welchem Zeitpunkt das Auto jeweils durch den Fahrer oder durch eine „automatisierte Fahrfunktion“ gesteuert wurde und wann ein Fahrer die Aufforderung zur Übernahme der Steuerung erhalten hat. Ebenfalls aufgezeichnet werden sollen Daten zu technischen Störungen automatisierter Fahrfunktionen. Mit den Daten soll sich nach einem Unfall klären lassen, ob die Technik und damit der Hersteller oder der Fahrer für einen Unfall verantwortlich war. Welche Daten dies sind und wie das Speichermedium ausgestaltet werden soll, regelt der Gesetzentwurf nicht. Auf Verlangen der nach Landesrecht für Verkehrskontrollen zuständigen Behörden müssen die Fahrdaten diesen Behörden übermittelt werden. Die Fahrdaten sind auch Dritten zu übermitteln, wenn diese glaubhaft machen können, dass sie die Fahrdaten zur Geltendmachung, Abwehr oder Befriedigung von Rechtsansprüchen aus Unfällen benötigen. Unklar ist, wer die Daten übermitteln muss. Es bleibt ebenfalls unbestimmt, ob ggf. auch die Behörden Fahrdaten übermitteln dürfen.

Im Gesetzesentwurf sind außerdem weder die Zwecke noch die zu übermittelnden Daten hinreichend konkretisiert. Weiterhin geht nicht hervor, wie die Integrität, Vertraulichkeit und Verfügbarkeit bei der Aufzeichnung und Übermittlung der Fahrdaten sichergestellt werden soll.

Sollte der Entwurf in der vorgelegten Form in Kraft treten, besteht in Kraftfahrzeugen mit hoch- oder vollautomatisierter Fahrfunktion die Gefahr elektronischer Fahrtenschreiber, die personenbezogene Profile bilden.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder fordert den Gesetzgeber zu einer dem datenschutz-

rechtlichen Bestimmtheitsgebot genügenden Novellierung des Straßenverkehrsgesetzes und zur Stärkung der Datenschutzrechte der Fahrer auf.
Sofern man eine Datenverarbeitung überhaupt für erforderlich hält, ist Folgendes zu regeln:

- die abschließende Aufzählung derjenigen Daten, die aufgezeichnet und gespeichert werden dürfen,
- die Bestimmung des für die Verarbeitung Verantwortlichen,
- die Ergänzung einer Übermittlungs-/Zugriffsregelung für den Fahrer/Halter,
- die Konkretisierung der Daten, die den nach Landesrecht zuständigen Behörden zu übermitteln sind,
- die datenschutzgerechte Ausgestaltung des Speichermediums, insbesondere die Festlegung einer angemessenen Speicherdauer anhand der Erforderlichkeit und des Zwecks der Beweisführung für die Haftung,
- eindeutige Festlegungen für die Trennung der Daten von den in den Fahrzeugdatenspeichern der Fahrzeuge gespeicherten Daten,
- die Konkretisierung der Zwecke für die Übermittlung der gespeicherten Daten,
- die Nennung des Adressaten für das Übermittlungsverlangen,
- die abschließende Nennung berechtigter Übermittlungsempfänger und ihrer jeweiligen Verarbeitungsbefugnisse mit im Übrigen strikter Zweckbindung und
- die Konkretisierung des Löschzeitpunkts der übermittelten Daten.

Anlage 13

Entschließung
der 93. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 29./30. März 2017 in Göttingen

Einsatz von Videokameras zur biometrischen Gesichtserkennung birgt erhebliche Risiken

In Pilotprojekten wird derzeit der Einsatz von Videoüberwachungssystemen erprobt, die erweiterte Möglichkeiten der Verhaltensauswertung und der Identifizierung von Beobachteten bieten. Neben der Mustererkennung steht besonders die biometrische Gesichtserkennung im Fokus dieser Projekte. Dies verschärft die ohnehin schon vorhandene Problematik derartiger neuer Überwachungsverfahren, mit denen „abweichendes Verhalten“ erkannt werden soll.[7]
Der Einsatz von Videokameras mit biometrischer Gesichtserkennung kann die Freiheit, sich in der Öffentlichkeit anonym zu bewegen, gänzlich zerstören. Es ist kaum möglich, sich solcher Überwachung zu entziehen oder diese gar zu kontrollieren.
Anders als bei konventioneller Videoüberwachung könnten Passanten mit dieser Technik nicht nur beobachtet und anhand bestimmter Muster herausgefiltert werden, sondern während der Überwachung anhand von Referenzbildern (Templates) automatisiert identifiziert werden. Damit wird eine dauerhafte Kontrolle darüber möglich, wo sich konkrete Personen wann aufhalten oder bewegen und mit wem sie hierbei Kontakt haben. Ermöglicht wird so die Erstellung von umfassenden Bewegungsprofilen und die Verknüpfung mit anderen über die jeweilige Person verfügbaren Daten.
Neben den genannten massiven gesellschaftspolitischen Problemen bestehen auch erhebliche rechtliche und technische Bedenken gegen den Einsatz solcher Überwachungstechniken. Biometrische Identifizierung arbeitet mit Wahrscheinlichkeitsaussagen; bei dem Abgleich zwischen ermitteltem biometrischen Merkmal und gespeichertem

[7] Siehe auch Entschließung der 83. Konferenz der Datenschutzbeauftragten des Bundes und der Länder „Öffentlich geförderte Forschungsprojekte zur Entdeckung abweichenden Verhaltens im öffentlichen Raum – nicht ohne Datenschutz“.

Template sind falsche Identifizierungen keine Seltenheit. Beim Einsatz dieser Technik durch Strafverfolgungsbehörden kann eine falsche Zuordnung dazu führen, dass Bürgerinnen und Bürger unverschuldet zum Gegenstand von Ermittlungen und konkreten polizeilichen Maßnahmen werden. Dieselbe Gefahr besteht, falls sie sich zufällig im öffentlichen Raum in der Nähe von gesuchten Straftätern oder Störern aufhalten.

Es gibt keine Rechtsgrundlage für die Behörden von Bund und Ländern für den Einsatz dieser Technik zur Gefahrenabwehr und Strafverfolgung. Die bestehenden Normen zum Einsatz von Videoüberwachungstechnik erlauben nur den Einsatz technischer Mittel für reine Bildaufnahmen oder -aufzeichnungen, nicht hingegen für darüber hinausgehende Datenverarbeitungsvorgänge. Aufgrund des deutlich intensiveren Grundrechtseingriffs, der durch Videotechnik mit erweiterter Auswertung einhergeht, können die bestehenden gesetzlichen Regelungen nicht analog als Rechtsgrundlage herangezogen werden, da sie für einen solchen Einsatz verfassungsrechtlich zu unbestimmt sind.

Nach der Rechtsprechung des Bundesverfassungsgerichts sind Maßnahmen mit großer Streubreite ein erheblicher Grundrechtseingriff. So verlangt das Bundesverfassungsgericht bereits für das automatisierte Erfassen von Kfz-Kennzeichen zwecks Abgleichs mit dem Fahndungsbestand eine normenklare und verhältnismäßige Rechtsgrundlage, die einen anlasslosen und flächendeckenden Einsatz ausschließt. Da bereits die allgemeine Regelung zur Videoüberwachung nicht zur Erfassung von Kfz-Kennzeichen ermächtigt, muss dies erst recht für die viel stärker in die Grundrechte Betroffener eingreifende Videoüberwachung zwecks Abgleichs biometrischer Gesichtsmerkmale einzelner Personen gelten. Ein Einsatz der Videoüberwachung mit Gesichtserkennung darf daher auf derzeitiger Grundlage auch im Rahmen eines Pilotbetriebs nicht erfolgen.

Der europäische Gesetzgeber hat die enormen Risiken dieser Technik für die Privatsphäre erkannt und die Verarbeitung biometrischer Daten zur Identifizierung sowohl in der ab Mai 2018 wirksamen Datenschutz-Grundverordnung als auch in der bis Mai 2018 umzusetzenden Datenschutz-Richtlinie im Bereich Justiz und Inneres nur unter entsprechend engen Voraussetzungen für zulässig erachtet. Wird über den Einsatz dieser Technik nachgedacht, muss der Wesensgehalt des Rechts auf informationelle Selbstbestimmung gewahrt bleiben und es müssen angemessene und spezifische Regelungen

zum Schutz der Grundrechte und -freiheiten der Betroffenen vorgesehen werden. Hierzu gehören u. a. eine normenklare Regelung für die Verwendung von Templates, z. B. von Personen im Fahndungsbestand, für den Anlass zum Abgleich des Templates mit den aufgenommenen Gesichtern sowie zum Verfahren zur Zulassung von technischen Systemen für den Einsatz.
Etwaige gesetzliche Regelungen müssten die vorgenannten verfassungs- und europarechtlichen Bedingungen beinhalten und den mit dieser Technik verbundenen erheblichen Risiken für die Freiheitsrechte der Bürgerinnen und Bürger angemessen Rechnung tragen!

Anlage 14

Entschließung
der 93. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 29./30. März 2017 in Göttingen

Göttinger Erklärung
Vom Wert des Datenschutzes in der digitalen Gesellschaft

Datenschutz ist zurzeit in aller Munde: Mit der Europäischen Datenschutzreform werden ab Mai 2018 in der ganzen Europäischen Union neue einheitliche Regeln gelten. Gegenwärtig sind die Gesetzgeber in Bund und Ländern mit Hochdruck dabei, das nationale Recht an die Europäischen Vorgaben anzupassen. Zugleich schreitet die Digitalisierung der Gesellschaft mit großen Schritten voran, etwa mit dem Internet der Dinge, der Wirtschaft 4.0 und künstlicher Intelligenz, und fordert die Wahrung des Datenschutzes und die Gewährleistung der Persönlichkeitsrechte heraus. Auch der Staat erweitert fortwährend seine Befugnisse zur Verarbeitung personenbezogener Daten, sei es zur Bekämpfung des Terrorismus und zur Gewährleistung der öffentlichen Sicherheit, sei es bei der Digitalisierung staatlicher Dienstleistungen.
Dabei gerät aber leichtfertig eines aus dem Blick: Datenschutz ist ein Grundrecht, wie die Meinungsfreiheit oder die Eigentumsgarantie. Es bindet alle Staatsgewalten unmittelbar, schützt die Menschenwürde und die freie Entfaltung der Persönlichkeit und kann auch Aspekte der Teilhabe und Chancengleichheit betreffen. Alle gesetzlichen Regelungen, sowie die Geschäftsmodelle und Anwendungen auch im Bereich der Wirtschaft, haben dies zu berücksichtigen. Immer häufiger stellen aber Verantwortliche in Politik und Wirtschaft dieses grundrechtlich geschützte Recht auf informationelle Selbstbestimmung implizit oder sogar explizit in Frage. Datenschutz wird als Hindernis diskreditiert.
Dies betrachtet die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder mit großer Sorge. Es befremdet sehr, wenn Mitglieder der Bundesregierung und andere Stimmen in der Politik in letzter Zeit immer wieder betonen, es dürfe kein Zuviel an Datenschutz geben und das Prinzip der Datensparsamkeit könne nicht die Richtschnur für die Entwicklung neuer Produkte sein.

Stattdessen wird für eine vermeintliche Datensouveränität geworben, deren Zielrichtung aber im Unklaren bleibt.
Die Konferenz betont, dass Informationen über Personen keine Ware sind wie jede andere und nicht allein auf ihren wirtschaftlichen Wert reduziert werden dürfen. Gerade in Zeiten von Big Data, Algorithmen und Profilbildung bieten die digitalen Informationen ein nahezu vollständiges Abbild der Persönlichkeit des Menschen. Mehr denn je muss daher die Menschenwürde auch im digitalen Zeitalter der zentrale Maßstab staatlichen und wirtschaftlichen Handelns sein. Zu einer menschenwürdigen und freien Entfaltung der Persönlichkeit gehört die freie Selbstbestimmung über das eigene Ich.
„Datensouveränität“, verstanden als eigentumsähnliche Verwertungshoheit, kann daher nur zusätzlich zum Recht auf informationelle Selbstbestimmung greifen, dieses jedoch keinesfalls ersetzen.
Die Konferenz fordert daher alle Entscheidungsträger in Politik und Wirtschaft auf, den hohen Wert des Rechts auf informationelle Selbstbestimmung für eine freiheitliche Gesellschaft zu achten und sich nachdrücklich vertrauensbildend für die Persönlichkeitsrechte einzusetzen. Datenschutz stellt kein Hindernis für die Digitalisierung dar, sondern ist wesentliche Voraussetzung für deren Gelingen.
Die Entwicklung datenschutzkonformer IT-Produkte und -Verfahren muss nachhaltig gefördert werden, um den Datenschutz zu einem Qualitätsmerkmal der europäischen Digitalwirtschaft zu machen.

Anlage 15

Entschließung zwischen den Konferenzen 2017

Grundsatzpositionen zum Datenschutz für die neue Legislaturperiode

Datenschutzkonferenz formuliert elf handlungsorientierte Grundforderungen
(Umlaufentschließung vom 16. Oktober 2017)

Zu Beginn der neuen Legislaturperiode hat die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder elf handlungsorientierte Grundforderungen formuliert, deren Ziel es ist, das Datenschutzrecht weiter zu entwickeln und seine Durchsetzung und Akzeptanz zu fördern. Diese Grundsatzpositionen hat die diesjährige Vorsitzende der Datenschutzkonferenz, die niedersächsische Landesdatenschutzbeauftragte Barbara Thiel, nunmehr allen im Bundestag vertretenen Fraktionen vorgelegt.

„Ein wirksamer Datenschutz ist Grundrechtsschutz und darf nicht als Hindernis für die Digitalisierung betrachtet werden. Er muss vielmehr als integraler und förderlicher Bestandteil politischer, wirtschaftlicher und gesellschaftlicher Fortentwicklung verstanden und gelebt werden“, erläutert Barbara Thiel. „Die Digitalisierung eröffnet zweifellos wirtschaftliche und gesellschaftspolitische Chancen, aber sie birgt auch erhebliche Risiken für die Persönlichkeitsrechte der Menschen. Ein an diese Entwicklungen angepasster und damit starker Datenschutz ist deshalb das Gebot der Stunde.“

So zielt eine der Forderungen darauf ab, datenschutzfreundliche und sichere Systemgestaltung stärker öffentlich zu fördern. „Nach der europäischen Datenschutz-Grundverordnung sollen nicht nur die erforderlichen technisch-organisatorischen Maßnahmen für Datensicherheit getroffen werden“, so Thiel. „Vielmehr soll Datenschutz von Anfang an und über den gesamten Lebenszyklus hinweg in Produkte, Dienste und Anwendungen eingebaut sein. Daher sollten Initiativen und Projekte verstärkt gefördert werden, die Datenschutz „by Design“ und „by Default“ gewährleisten und die Qualität derDatensicherheit verbessern.“

Großen Wert legt die Datenschutzkonferenz auch auf die Wahrung des Datenschutzes im Bereich der Inneren Sicherheit. „Nur Sicherheit in Freiheit ist wirkliche Sicherheit für alle“, stellt sie in diesem Zusammenhang fest. Bei der Bekämpfung von Terrorismus und Kriminalität müsse deshalb das Vertrauen unbescholtener Menschen in die Vertraulichkeit ihrer Kommunikation und die Unberührtheit ihrer Privatheit gewahrt werden.

Anlage 16

Entschließung
der 94. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 8./9. November 2017 in Oldenburg

Umsetzung der DS-GVO im Medienrecht

Das Inkrafttreten der Datenschutzgrundverordnung (DS-GVO) und deren Geltungsbeginn im Mai 2018 verlangt eine Anpassung der medienrechtlichen Datenschutzbestimmungen an die neuen Vorgaben. Dabei muss dem hohen Stellenwert der Meinungs- und Informationsfreiheit sowie der Presse-, Rundfunk- und Medienfreiheit gemäß Art. 5 Grundgesetz (GG) und Art. 11 EU-Grundrechtecharta (GRCh) für die freiheitliche demokratische Grundordnung ebenso Rechnung getragen werden wie dem Recht auf Informationelle Selbstbestimmung gemäß Art. 1 i. V. m. Art. 2 GG und dem Recht auf Schutz personenbezogener Daten gemäß Art. 8 GRCh. Kollisionen der Schutzbereiche der Grundrechte sind im Sinne einer praktischen Konkordanz aufzulösen.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder weist daher auf die Anpassungsklausel des Art. 85 DS-GVO hin. Danach können die Mitglied-staaten Ausnahmen und Abweichungen von bestimmten Vorgaben der DS-GVO normieren, wenn „*dies erforderlich ist, um das Recht auf Schutz der personenbezogenen Daten mit der Freiheit der Meinungsäußerung und der Informationsfreiheit in Einklang zu bringen*“. Das sich daraus ergebende Regel-Ausnahme-Verhältnis bedeutet, dass die Vorgaben der DS-GVO grundsätzlich auch auf sämtliche Verarbeitungen personenbezogener Daten zu grundrechtlich besonders geschützten journalistischen, wissenschaftlichen, künstlerischen oder literarischen Zwecken angewendet werden sollen.

Bei der Umsetzung von Art. 85 DS-GVO gilt es insbesondere folgende Anforderungen zu beachten:

- Ausnahmen oder Abweichungen von der Anwendung der DS-GVO auf die Verarbeitung personenbezogener Daten im journalistischen Bereich müssen notwendig sein, um freie Meinungs-

äußerung und Informationsfreiheit gemäß Art. 11 GRCh sicherzustellen.

- Einen regelhaften Vorrang der Presse-, Rundfunk- und Medienfreiheit sieht die DS-GVO nicht vor. Sie verlangt vielmehr, einen angemessenen Ausgleich zwischen den Grundrechten herzustellen, wenn diese in Widerstreit geraten (vgl. 153. Erwägungsgrund der DS-GVO).
- Die Grundsätze des Datenschutzes (Art. 5 DS-GVO) müssen hinreichend Beachtung finden. Jedenfalls steht es nicht im Einklang mit dem Recht auf Schutz personenbezogener Daten, wenn die Grundsätze des Datenschutzes im Journalismus in weitem Umfang ausgeschlossen werden. Eine Regelung kann keinesfalls als notwendig i. S. d. DS-GVO angesehen werden, wenn sie zum Zwecke der Abwägung mit der Meinungs- und Informationsfreiheit die Transparenzrechte und Interventionsmöglichkeiten für betroffene Personen sowie Verfahrensgarantien über eine unabhängige Aufsicht missachtet.
- Über den eingeräumten Gestaltungsspielraum geht es hinaus, wenn die Verarbeitung personenbezogener Daten durch Hilfsunternehmen zu undifferenziert vom Geltungsbereich der DS-GVO ausgenommen wird, ohne dass diese Aktivitäten unmittelbar der journalistischen Tätigkeit dienen. Die Reichweite der journalistischen Tätigkeit bedarf zudem einer Konkretisierung.
- Die künftige Aufsicht über den Datenschutz beim Rundfunk ist unabhängig auszugestalten. Sie bedarf wirksamer Abhilfebefugnisse bei Datenschutzverstößen.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder fordert daher für die Anpassung von Rundfunk-Staatsverträgen, Presse- und Mediengesetzen:

- Die gesetzlichen Anpassungen i. S. d. Art. 85 DS-GVO müssen konkret und spezifisch – bezogen auf die jeweiligen Normen und Vorgaben der DS-GVO – Ausnahmen und Abweichungen regeln und diese begründen.
- Bei der Ausübung der jeweiligen Regelungskompetenz ist das europäische Datenschutzrecht zwingend zu beachten. Eine faktische Beibehaltung der bisherigen nationalen Rechtslage würde dem nicht gerecht.

Anlage 17

Entschließung
der 94. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 8./9. November 2017 in Oldenburg

Keine anlasslose Vorratsdatenspeicherung von Reisedaten

Der Gerichtshof der Europäischen Union (EuGH) hat in seinem Gutachten vom 26. Juli 2017 (Gutachten 1/15) zum Fluggastdaten-Abkommen der EU mit Kanada die langfristige Speicherung von Fluggastdaten (Passenger Name Records – PNR-Daten) sämtlicher Passagiere für nicht mit der Europäischen Grundrechtecharta vereinbar erklärt und seine Position zu anlasslosen Speicherungen personenbezogener Daten bekräftigt. Er erteilt damit einer anlasslosen Vorratsdatenspeicherung von personenbezogenen Daten erneut eine klare Absage. Die Aussagen des EuGH sind nicht nur auf alle geltenden PNR-Instrumente übertragbar und stellen Anforderungen an die Anpassung des Fluggastdatengesetzes, sie betreffen auch die auf europäischer Ebene angestrebte Einrichtung eines Entry-Exit-Systems (EES) sowie eines EU-weiten Reiseinformations- und -genehmigungssystems (ETIAS), die ebenfalls weitreichende anlasslose Speicherungen beabsichtigen.

Zwar hält der EuGH es grundsätzlich für zulässig, Fluggastdaten automatisiert zu übermitteln und auszuwerten, um Personen zu ermitteln, die eine potentielle Gefahr für die öffentliche Sicherheit darstellen und bei ihrer Einreise einer gewissenhaften Kontrolle unterzogen werden sollen. Das gilt jedoch nicht für sensible Daten, die Rückschlüsse etwa auf die rassische und ethnische Herkunft, religiöse Überzeugungen oder das Sexualleben ermöglichen. Der Übermittlungszweck rechtfertigt auch nicht automatisch die weitere Verwendung und Speicherung der Daten. Die übermittelten Daten haben vielmehr ihren Zweck erfüllt, wenn sich während des Aufenthaltes keine konkreten Anhaltspunkte für geplante terroristische oder andere schwere Straftaten ergeben haben. In diesem Fall sieht der EuGH keine Rechtfertigung für eine weitere Speicherung der Daten.

Das Fluggastdatengesetz, mit dem die Richtlinie (EU) 2016/681 des Europäischen Parlaments und des Rates vom 27. April 2016 über die Verwendung von PNR-Daten zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität umgesetzt wurde, geht insbesondere durch die Einbeziehung der innereuropäischen Flüge, die im Widerspruch zu dem Grundsatz des freien Personenverkehrs im Schengen-Raum steht, noch über den verpflichtenden Teil der Richtlinie hinaus.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) sieht in den vom EuGH ausgesprochenen Feststellungen zur Rechtslage einen unverzichtbaren Maßstab für die Verordnungsvorschläge zur Einrichtung eines neuen Entry-Exit-Systems (EES) sowie eines EU-weiten Reiseinformations- und -genehmigungssystems (ETIAS).

Mit dem EES sollen alle Ein- und Ausreisen sowie Einreiseverweigerungen von Drittstaatlern in die EU zentral erfasst und für mehrere Jahre gespeichert werden (einschließlich biometrischer Identifizierungsmerkmale). Im ETIAS sollen zum Zwecke der Erleichterung der Grenzkontrollen vorab Daten von einreisewilligen visabefreiten Drittstaatlern erhoben und ebenfalls für mehrere Jahre zentral gespeichert werden. In beiden Datenbanken sollen also Daten, die im Rahmen der Einreise und Grenzkontrolle erhoben werden, ebenso wie nach dem PNR-Abkommen, ohne konkreten Anlass zentral für einen langen Zeitraum vorgehalten werden. Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder hält dies nicht für vertretbar.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder fordert die jeweils zuständigen Gesetzgeber auf, zeitnah und konsequent sämtliche PNR-Instrumente der EU im Sinne der EuGH-Rechtsprechung nachzubessern, insbesondere das deutsche Fluggastdatengesetz.

Sie fordert die Bundesregierung zudem auf, sich auf europäischer Ebene für eine den Anforderungen der EU-Grundrechtecharta und der Rechtsprechung des EuGH entsprechende Ausgestaltung der angestrebten Systeme EES und ETIAS einzusetzen.

Anlage 18

Pressemitteilung
der 94. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 8./9. November 2017 in Oldenburg

Datenschutzbehörden erteilen der anlasslosen Vorratsdatenspeicherung von Reisedaten eine Absage und fordern die datenschutzrechtliche Anpassung von Rundfunk-Staatsverträgen sowie der Presse- und Mediengesetze

Unter dem Vorsitz der Landesbeauftragten für den Datenschutz Niedersachsen, Barbara Thiel, hat die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) auf ihrer Herbsttagung am 8. und 9. November 2017 in Oldenburg aktuelle Themen des Datenschutzes diskutiert.
Unter der Überschrift „*Keine anlasslose Vorratsspeicherung von Reisedaten*“ fordert die DSK die jeweils zuständigen Gesetzgeber auf, zeitnah und konsequent die Speicherung von Fluggast-daten (Passenger Name Records – PNR-Daten) im Sinne des EuGH-Gutachtens zum Fluggastdatenabkommen zwischen Kanada und der EU vom Juni 2017 nachzubessern. Dies gilt insbesondere für das deutsche Fluggastdatengesetz.

Zugleich fordert die DSK die Bundesregierung auf, sich auf europäischer Ebene für eine den Anforderungen der EU-Grundrechtecharta und der Rechtsprechung des EuGH entsprechende Ausgestaltung des angestrebten Entry-Exit-Systems (EES) sowie des EU-weiten Reiseinformations- und -genehmigungssystems (ETIAS) einzusetzen.

„Zwar hält der EuGH es grundsätzlich für zulässig, Fluggastdaten automatisiert zu übermitteln und auszuwerten, um Personen zu identifizieren, die eine potentielle Gefahr für die öffentliche Sicherheit darstellen und bei ihrer Einreise einer gewissenhaften Kontrolle unterzogen werden sollen“, erläutert die Vorsitzende. Allerdings haben die übermittelten Daten ihren Zweck erfüllt, wenn sich während des Aufenthaltes keine konkreten Anhaltspunkte für geplante terroristische oder andere schwere Straftaten ergeben haben. „In

diesem Fall sieht der EuGH keine Rechtfertigung für eine weitere Speicherung der Daten“, betont Barbara Thiel.

Mit einer weiteren Entschließung fordert die Konferenz die Umsetzung der Datenschutz-Grundverordnung auch im Medienrecht. Anlass dafür sind die bisher durch die Länder vorgelegten Entwürfe für die Novellierung der Rundfunk-Staatsverträge. Diese schließen pauschal die Anwendbarkeit eines Großteils der Vorschriften der Datenschutz-Grundverordnung für den journalistischen Bereich aus und erklären lediglich drei Artikel für anwendbar. Dadurch wird nach Auffassung der DSK das durch Art. 85 DS-GVO vorgegebene Regel-Ausnahme-Verhältnis ins Gegenteil verkehrt.

„Die Vorschriften der Datenschutz-Grundverordnung sind grundsätzlich auch von Rundfunkanstalten und Presseunternehmen zu beachten. Der nationale Gesetzgeber ist lediglich befugt, begründete Ausnahmen zuzulassen, wenn diese erforderlich sind um das Recht auf Schutz personenbezogener Daten mit der Freiheit der Meinungsäußerung und der Informationsfreiheit in Einklang zu bringen“, so Barbara Thiel. Eine faktische Beibehaltung der bisherigen nationalen Rechtslage würde dem nicht gerecht.

Gegenstand der Beratungen waren daneben Fragen der künftigen Einbindung der Datenschutzaufsichtsbehörden der Rundfunkanstalten und der Kirchen, die § 18 Absatz 1 Satz 4 BDSG-neu zwingend vorschreibt, „sofern diese von der Angelegenheit betroffen sind“.
Auch die mögliche Fortsetzung des Dialogs mit Wirtschaftsunternehmen stand auf der Tagesordnung. Ein erstes Treffen im Sommer 2017 war seinerzeit von beiden Seiten positiv bewertet worden. Die DSK kam nun dem Ergebnis, dass ein solcher Austausch mit Wirtschaftsunternehmen und anderen Interessengruppen insbesondere zu Grundsatzfragen des Datenschutzes als sinnvoll anzusehen sei.

Dazu Barbara Thiel: „Um dem in der DS-GVO normierten Auftrag zur Beratung, Sensibilisierung und Aufklärung gerecht werden zu können, halte ich einen Austausch zwischen Aufsichtsbehörden und Wirtschaftsunternehmen auf verschiedenen Ebenen für vorteilhaft und wünschenswert. Dabei muss es aus meiner Sicht vor allem um

grundsätzliche datenschutzpolitische und datenschutzrechtliche Weichenstellungen gehen.

Eine solche gemeinsame Plattform auf strategischer Ebene kann aber auch die Basis für ein besseres und tiefergehendes Verständnis bilden, das allen Beteiligten zu gute kommen kann. Die Aufsichtsbehörden erhalten auf diese Weise aus erster Hand Einblicke und Informationen über datenschutzrelevante Entwicklungen innerhalb der Wirtschaft.“

Anlage 19

Pressemitteilung
vom 1. Februar 2016

Zwei auf einen Streich:
Transparenzgesetz und Digitale Selbstverteidigung

Im Rahmen einer Pressekonferenz wird der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) seinen Vorschlag für ein Thüringer Transparenzgesetz vorstellen, der im politischen Raum als Anregung dienen soll.



Als Beitrag zum 13. Safer Internet Day stellt der TLfDI zudem sein neues Anleitungsheft zur digitalen Selbstverteidigung vor – denn Selbstschutz der Privatsphäre durch Jung und Alt ist dringend angesagt!

Hierzu lädt der TLfDI die Abgeordneten des Thüringer Landtages und die Vertreter der Presse am

Dienstag, 9. Februar 2016, 10 Uhr
in die Behörde des TLfDI
Häßlerstraße 8, 3. Etage
99096 Erfurt
herzlich ein.

Anlage 20

Pressemitteilung
vom 24. Februar 2016



Pressemitteilung
Einladung
Unterrichtsmaterial per Knopfdruck

Dem Thüringer Ministerium für Bildung, Jugend und Sport (TMBJS) und dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) ist die Medienkompetenzentwicklung der Schülerinnen und Schüler ein wichtiges Anliegen. Unterstützungsangebote des TLfDI richten sich besonders an Lehrkräfte und Pädagogen, die die Themen Datenschutz und die Datensicherheit im Unterricht lebensnah aufgreifen wollen, zum Beispiel im Rahmen des Kurses Medienkunde. Die vom TMBJS geförderte **Mediendatenbank** des TLfDI ist ein solches Angebot. In die Datenbank wurden Materialquellen aufgenommen, die das „Leben“ in sozialen Netzwerken ebenso thematisieren wie Virenschutz, Passwortsicherheit, Vorratsdatenspeicherung, Videoüberwachung, Cybermobbing und Urheberrecht. Die Datenbankanwendung enthält zwei Segmente: Der „Medienpool“ ermöglicht die Suche nach Videos, Broschüren, Arbeitsblättern, die sich für den direkten Einsatz im Unterricht eignen. Der „Infopool“ enthält Links zu Quellen, die für die Unterrichtsvorbereitung der Lehrkraft geeignet erscheinen und Hintergrundwissen zur Vertiefung von Themen liefern. Also in Klasse 9 zum Beispiel einfach „Klasse 9“ und „Smartphones“ anklicken – und los geht’s.
Die Mediendatenbank wird Bestandteil des Internetauftritts des TLfDI und per gemeinsamen Knopfdruck mit der Staatssekretärin, Frau Ohler, freigeschaltet.
Hierzu laden der TLfDI und das TMBJS die Presse- und Medienvertreter am

Dienstag, 1. März 2016, 10.30 Uhr in das
THÜRINGER MINISTERIUM FÜR BILDUNG, JUGEND UND SPORT
Werner-Seelenbinder-Straße 7
Raum 415
99096 Erfurt
herzlich ein.

Anlage 21

Pressemitteilung
vom 30. März 2016

Datenschutz und Polizei
optimieren ihre Zusammenarbeit:
Polizistin abgeordnet zum Landesdatenschützer

Die Polizei erhebt, verwendet und speichert bei ihrer täglichen Arbeit personenbezogene Daten. Deshalb liegen dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), Herrn Dr. Hasse und dem Thüringer Minister für Inneres und Kommunales (TMIK), Herrn Dr. Holger Poppenhäger das Datenschutzbewusstsein der Thüringer Polizei sehr am Herzen. Poppenhäger sagte: „Datenschutz ist ein hohes Gut, deshalb ist es auch eine wichtige Aufgabe, unsere Polizeibeamten für die Problematiken in diesem Bereich zu sensibilisieren und über aktuelle Regelungen auf dem Laufenden zu halten.“ Das Ministerium plante, für diesen Zweck Polizeibedienstete an den TLfDI abzuordnen. Das Vorhaben wird nun in die Tat umgesetzt werden. Am 21. März 2016 wurde die erste Polizeibeamtin der Landespolizeidirektion zum TLfDI abgeordnet. Weitere Abordnungen anderer Polizeibeamten und -beamtinnen sollen folgen, so das TMIK. Der Einsatz von Polizeibeamten beim TLfDI wird diesen einerseits einen Überblick über die Arbeit der Datenschutz-Behörde und den Datenschutz verschaffen, andererseits stehen der Polizei im Anschluss an die jeweiligen Abordnungszeiten datenschutzfachkundige Polizeibedienstete als Multiplikatoren zur Verfügung. „Wir freuen uns auf diese neue Art der Zusammenarbeit“, so Hasse.

Anlage 22

Pressemitteilung
vom 8. April 2016

Pressemitteilung

91. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder am 6./7. April 2016 in Schwerin

Unter dem Vorsitz des Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern, Reinhard Dankert, tagte am 6./7. April 2016 die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder in Schwerin.

Neben den aktuell diskutierten Themen wie beispielsweise die neue EU-Datenschutz-Grundverordnung, Zensus 2021, den Datenschutzbestimmungen von Google und Facebook wurden auch Entschließungen der Konferenz zu speziellen Themen gefasst:

So appellierte die Datenschutzkonferenz im Hinblick auf die EU-Datenschutz-Grundverordnung (EU-DS-GVO) an den Bundesgesetzgeber, die Öffnungs- und Konkretisierungsklauseln der EU-DS-GVO konsequent und umfassend zu nutzen, um unverzichtbare Datenschutzstandards im Sinne des Grundrechts auf informationelle Selbstbestimmung auch weiterhin zu gewährleisten. Auch die von der Grundverordnung getroffenen Weiterentwicklungen des Datenschutzes wie beispielsweise die Grundsätze des Datenschutzes durch Technik und durch datenschutzfreundliche Voreinstellungen sowie das Erfordernis von Datenschutz-Folgeabschätzungen müssten wirksam ausgestaltet werden. Aus diesem Grund positionierte sie sich in diesem Zusammenhang auf fünf Themen mit hoher Bedeutung und forderte deshalb Bundes- und Landesgesetzgeber auf, in allen gesetzgeberischen Bereichen die nationalen Spielräume im Sinne des Grundrechts auf informationelle Selbstbestimmung zu nutzen.

Weiterhin forderte die Konferenz in einer Entschließung den Gesetzgeber auf zu prüfen, ob und inwieweit im Zusammenhang mit

Wearables und Gesundheits-Apps die Möglichkeit beschränkt werden sollte, materielle Vorteile von der Einwilligung in die Verwendung von Gesundheitsdaten abhängig zu machen. Zudem wiesen die Datenschutzbeauftragten u. a. darauf hin, dass zum notwendigen Schutz von Gesundheitsdaten die Grundsätze der Datenvermeidung, Datensparsamkeit und der Transparenz zu beachten sind.

Auch die Terroranschläge in Brüssel haben die Konferenz erneut veranlasst, sich zu Fragen des Datenschutzes bei der effektiven Bekämpfung des Terrorismus in Form einer Entschließung zu äußern. Erneut wiesen sie darauf hin, dass alle neu erwogenen Maßnahmen zur Bekämpfung des internationalen Terrorismus daran zu messen sind, ob sie für dessen wirkungsvolle Bekämpfung tatsächlich geeignet, erforderlich und angemessen sind und somit dem Verfassungsgrundsatz der Verhältnismäßigkeit entsprechen. In ihrer Entschließung weist die Konferenz darauf hin, dass der Datenschutz nicht für etwaige Ermittlungs- oder Vollzugsdefizite der Sicherheitsbehörden verantwortlich gemacht werden kann. Das geltende Datenschutzrecht erlaubt es schon jetzt, ermittlungsrelevante und zur Strafverfolgung notwendige Daten zu speichern und Informationen zwischen den Sicherheitsbehörden wechselseitig auszutauschen.

Außerdem standen sogenannte Servicekonten für Bürgerinnen, Bürger und Unternehmen im Blickfeld, die wohl zunehmend, entsprechend den Empfehlungen des IT-Planungsrates, von Behörden flächendeckend angeboten werden sollen. Aus diesem Grund hat die Konferenz in einer weiteren Entschließung Hinweise zur datenschutzkonformen Ausgestaltung dieser Konten formuliert. Die Datenschutzbeauftragten begrüßen durchaus die Bestrebungen, sichere Identifizierungsmöglichkeiten durch die Nutzung der eID-Funktion des Personalausweises zu unterstützen. Sie fordern jedoch, für den Umgang mit personenbezogenen Daten in Servicekonten eine tragende Rechtsgrundlage zu schaffen und beim Betrieb der Konten insbesondere die Datenschutzprinzipien der Datensparsamkeit, der Nichtverkettbarkeit und der Transparenz zu berücksichtigen.

Die Konferenz hat weiterhin eine Orientierungshilfe für Online-Lernplattformen im Schulunterricht verabschiedet. Diese entstand unter Federführung des TLfDI als Vorsitzendem des Arbeitskreises

Datenschutz und Bildung der Datenschutzbeauftragten des Bundes und der Länder.
Immer mehr Bildungsinstitutionen setzen auf die webgestützte Wissensvermittlung und die elektronischen Kommunikationsmöglichkeiten zwischen Lehrenden und Lernenden. Die verabschiedete Orientierungshilfe richtet sich insbesondere an Schulen, die Online-Lernplattformen als Lernmittel einsetzen wollen. Sie sollen sich einen Überblick darüber verschaffen können, welche datenschutzrechtlichen Anforderungen Online-Lernplattformen erfüllen müssen. Diese Orientierungshilfe gibt auch den Anbietern von Online-Lernplattformen die Möglichkeit, ihr jeweiliges Produkt so zu gestalten oder anzupassen, dass eine Nutzung durch Schulen zulässig ist. Nach Rückmeldungen aus der Praxis soll diese OH fortentwickelt werden.
Diese OH fand bereits vor Ort in Schwerin mediales Interesse. Ein entsprechendes Interview mit dem TLfDI am 7. April 2016 vom Deutschlandradio finden Sie hier: Interview mit Deutschlandradio.

Die von der Konferenz verabschiedeten Entschließungen und Orientierungshilfen sind auf der Homepage des TLfDI unter www.tlfdi.de abrufbar.

Anlage 23

Pressemitteilung
vom 14. April 2016

Privacy Shield:
Geplantes Schutzschild-Abkommen zum Datenverkehr
zwischen EU und USA noch immer zu löchrig

Thüringens Datenschutzbeauftragter Dr. Lutz Hasse sieht erheblichen Nachbesserungsbedarf beim „EU-US Privacy Shield“, dem geplanten Nachfolge-Abkommen des vom Europäischen Gerichtshof (EuGH) gekippten Safe-Harbour-Abkommens. „Der ‚Privacy Shield‘ muss mehr sein als nur Kosmetik am gescheiterten Safe Harbour-Abkommen“, sagte Dr. Hasse. „Aus der Stellungnahme der europäischen Datenschutzbeauftragten (Artikel-29-Datenschutzgruppe) vom 13. April 2016 ergibt sich, dass die Privacy Shield-Regelungen in den USA für kein Datenschutzniveau sorgen werden, das mit den EU-Standards vergleichbar ist“, so der Thüringer Datenschutzbeauftragte.

Deshalb fordert Dr. Hasse die EU-Kommission auf, insbesondere die drei Kernforderungen der Artikel-29-Datenschutzgruppe im Laufe der Verhandlungen mit der amerikanischen Gegenseite zu beachten und umzusetzen.

So sei die im Privacy Shield-Abkommen erstmals vorgesehene „Ombudsperson“ weder unabhängig, noch sei sie wegen ihrer beschränkten Kompetenzen in der Lage, wirklich im Sinne des Datenschutzes für die EU-Bürger zu agieren.

Kritisch sieht Hasse auch die ungezügelte, teilweise unerlaubte „Datensammelwut“ des US-amerikanischen Nachrichtendienstes (US Office of Director of National Intelligence), die durch „Privacy Shield“ kaum gebremst werde.

Und schließlich könne mit dem Schutzschild auch nicht sichergestellt werden, dass die zuständigen US-amerikanischen Unternehmen die personenbezogenen Daten löschen, wenn sie für sie nicht mehr erforderlich sind.

Kurzformel: Privacy Shield > Safe Harbor, aber Privacy-Shield ≠ Europäischer Datenschutz.

Es bleibt viel zu tun für die Europäische Kommission, damit der Europäische Gerichtshof nicht auch diesen „Schutzschild“ aus der Hand schlägt.
Die Stellungnahme der Artikel-29-Datenschutzgruppe ist im Internet abrufbar unter http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf.

Press Release

Privacy Shield – New Deal
Effectiveness remains to be seen

Dr. Lutz Hasse, the Thuringian State Commissioner for Data Protection and Freedom of Information, calls upon the European Commission to resolve the following major concerns, that are raised in the Opinion by the Article 29 Data Protection Working Party over the EU-US Privacy Shield draft adequacy decision:

(1) The Privacy Shield Ombudsperson may neither be sufficiently independent nor have adequate power to exercise its duties. The Ombudsperson mechanism may also be overly complicated for EU individuals to use. Inefficiency might be the consequence.
(2) The Privacy Shield may not exclude the US Office of Director of National Intelligence from continuing massive and indiscriminate collection of personal data originating from the EU.
(3) The Privacy Shield may not require US companies to delete data once they are deemed unnecessary.

Hasse claims, that the Privacy Shield should not just be cosmetic change from the now defunct Safe Harbor Privacy Principles. He calls upon the European Commission to identify appropriate solutions in order to improve the draft adequacy decision, and to ensure that the protection offered by the Privacy Shield is equivalent to the standards in the EU.

The Opinion of the Article 29 Working Party is available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf

Anlage 24

Pressemitteilung
vom 15. April 2016

Datenschutz-Grundverordnung verabschiedet – Countdown läuft

28 Mitgliedstaaten – 28 unterschiedliche Datenschutzstandards. Das gehört bald der Vergangenheit an.
Nach vierjähriger Debatte hat das Europäische Parlament am 14. April 2016 die Datenschutz-Grundverordnung (DS-GVO) verabschiedet. Sie löst damit die seit 1995 bestehende Datenschutzrichtlinie ab.

Die DS-GVO vereint zum ersten Mal ein Regelwerk, das sowohl im öffentlichen Bereich als auch im nicht-öffentlichen Bereich unmittelbare Anwendung findet. Wichtige Änderungen sind beispielweise das Recht auf Vergessenwerden und das One-Stop-Shop-Verfahren, bei dem künftig der Betroffene sich an die Datenschutzaufsichtsbehörde seines Landes wenden kann, auch wenn er seine personenbezogenen Daten in einem anderen Land als unrechtmäßig verarbeitet ansieht. Mit der Datenschutz-Grundverordnung werden zudem Verstöße schärfer geahndet. Auf Unternehmen können bei Datenschutzverstößen Strafen von bis zu 4 Prozent des erzielten Jahresumsatzes zukommen.

Zahlreiche sog. Öffnungsklauseln, wie zum Beispiel zum betrieblichen Datenschutzbeauftragten, zur Datenübermittlung in Drittstaaten oder zum Beschäftigtendatenschutz, geben den einzelnen Mitgliedsstaaten die Möglichkeit, weitere eigene Regelungen zu erlassen. Spannend zu beobachten wird sein, inwiefern die Bundesregierung die Öffnungsklauseln mit Leben füllen und ein Gesetz zur DS-GVO als Nachfolgegesetz zum Bundesdatenschutzgesetz auf den Weg bringen wird.

Nach dem In-Kraft-Treten der DS-GVO mit Veröffentlichung im Amtsblatt der EU wird diese – nach der Gewährung einer Umsetzungsfrist von zwei Jahren – im Frühjahr 2018 wirksam sein.

Bis dahin müssen auch in Thüringen die geltenden Datenschutzbestimmungen auf ihre Vereinbarkeit mit der DS-GVO von den jeweils zuständigen Ministerien überprüft und gegebenenfalls vom Gesetzgeber angepasst werden.
Der Countdown läuft …

Anlage 25

Pressemitteilung
vom 17. Mai 2016

Forderung des Bundesrates:
Klagerecht für die Datenschutzaufsichtsbehörden!

Hasse: „Klasse!“
Der Bundesrat hat am vergangenen Freitag, 13. Mai 2016, den Beschluss gefasst, die Bundesregierung zu bitten, ein Klagerecht der Datenschutzbehörden gegen datenschutzrechtliche Rechtsakte der Europäischen Kommission in das Bundesdatenschutzgesetz aufzunehmen.
Hintergrund für diese Forderung ist das Safe-Harbor-Urteil des EuGH vom 6. Oktober 2015 (Rechtssache C-362/14). Der EuGH erklärte in diesem Urteil Datenübermittlungen in die USA auf der Grundlage des sogenannten Safe-Harbor-Abkommens für ungültig (siehe hierzu Pressemitteilung des TLfDI vom 6. Oktober 2015).
Darüber hinaus forderte der EuGH in seinem Urteil jedoch auch, gesetzlich das Recht zur Klage für die Datenschutzbehörden zu regeln, mit dem z. B. auch ein neues Privacy-Shield-Abkommen angegriffen werden kann.
Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI), Dr. Lutz Hasse: „Dieser Schritt geht in die richtige Richtung – es ist ein Fortschritt, dass nicht nur Privatpersonen solche europäischen Rechtsakte zur gerichtlichen Überprüfung stellen dürfen, sondern auch die Datenschutzbehörden, deren Sachverstand die datenschutzrechtlichen Schwächen herauszuschälen bestens in der Lage ist. Wieder ein guter Tag für den Datenschutz.“

Anlage 26

Pressemitteilung
vom 18. Mai 2016

Einladung zur Pressekonferenz:
Es kommt dicker…!
Der TLfDI stellt seine neuen Tätigkeitsberichte
für die Jahre 2014 und 2015 vor!

Dass sich der Arbeitsanfall beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) immens erhöht hat, lässt sich am Umfang der beiden aktuellen Tätigkeitsberichte unschwer ablesen. Allein die registrierten Posteingänge stiegen im Vergleich zu 2011 um fast **70 Prozent**. Die gestiegene Anzahl der Beiträge machte es erforderlich, dass der 2. Tätigkeitsbericht für den nicht-öffentlichen Bereich und der 11. Tätigkeitsbericht für den öffentlichen Bereich nunmehr in zwei gesonderten Bänden gedruckt werden mussten. Einen Schwerpunkt im Berichtszeitraum im nicht-öffentlichen Bereich stellt die datenschutzrechtliche Prüfung von Videoüberwachungsanlagen in Thüringen dar. Dies betraf vor allem die Videoüberwachung von Mitarbeitern, Kunden, Nachbarn oder auch unbeteiligten Dritten. Viele Beschwerden gab es auch im Bereich des Beschäftigtendatenschutzes. Ein wichtiger Teil der Arbeit des TLfDI im öffentlichen Bereich war die Begleitung der Verabschiedung der Datenschutz-Grundverordnung der Europäischen Union (DS-GVO) sowie die Förderung der Medienkompetenz an den Thüringer Schulen. Eine weitere Baustelle riss die Entscheidung des EuGH zu Safe Harbor auf.

Neugierig geworden?

Zur Vorstellung seines 2. Tätigkeitsberichts im nicht-öffentlichen Bereich und seinem
11. Tätigkeitsbericht im öffentlichen Bereich lädt der TLfDI am

Mittwoch, 25. Mai 2016, 10 Uhr
in die Behörde des TLfDI,
Häßlerstraße 8, 3. Etage,
99096 Erfurt

die Vertreter der Presse, der Fraktionen sowie interessierte Bürgerinnen und Bürger ein.

Anlage 27

Pressemitteilung
vom 19. Mai 2016

Gericht bestätigt: Videoüberwachung durch Private in öffentlich zugänglichen Räumen meldepflichtig!

Wie aus einer Pressemitteilung des Unabhängigen Datenschutzzentrums Saarland zu entnehmen ist, stellt ein Urteil des Verwaltungsgerichts Saarland vom 18. Mai 2016 fest, dass der Betrieb von Wildbeobachtungskameras grundsätzlich dem Anwendungsbereich des Bundesdatenschutzgesetzes (BDSG) unterfällt und das Erheben, Verarbeiten oder Nutzen der mit einer Wildkamera erstellten Aufnahmen eine automatisierte Verarbeitung darstellen, sofern hiervon personenbezogene Daten möglicherweise betroffen sind. Damit sind die Kameras gemäß § 4d Abs. 1 BDSG meldepflichtig (siehe auch: https://www.tlfdi.de/tlfdi/themen/video/).
Auch nicht-öffentliche Stellen in Thüringen, die eine solche Kamera einsetzen wollen, müssen dies zuvor dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) als zuständige Aufsichtsbehörde melden, wenn sie keinen betrieblichen Datenschutzbeauftragten haben. Der Inhalt der erforderlichen Meldepflicht ergibt sich aus § 4e BDSG. Damit bestätigt das Verwaltungsgericht die vom TLfDI vertretene Position.
Nach Auffassung des TLfDI hat das Urteil auch eine weitreichende Bedeutung für den Einsatz von **allen übrigen Videoüberwachungsanlagen** durch private Stellen, die (teilweise) öffentlich zugängliche Räume beobachten. Auch diese Stellen sind gegenüber dem TLfDI meldepflichtig.

Anlage 28

Pressemitteilung
vom 15. Juli 2016

Upgrade auf Windows 10 – TLfDI gibt hilfreiche Tipps

Das Microsoft Angebot, Besitzern von Starter-, Home-, Professional- oder Ultimate-Lizenzen von Windows 7 oder Windows 8.x ein kostenloses Upgrade auf Windows 10 zu ermöglichen, läuft in 14 Tagen, am 29. Juli 23:59 Uhr ab. Daher werden noch viele Nutzer die Umstellung diesen Monat durchführen.
In seiner Pressemitteilung „Windows 10 – Gefahren für die Privatsphäre“ vom 5. August 2015 wies der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) auf die drohenden Gefahren beim Wechsel auf das neue Betriebssystem hin.
Zur Schadensbegrenzung stellt der TLfDI daher eine Handreichung zur Verfügung, wie beim Umstieg auf Windows 10 der Datenschutz berücksichtigt werden kann.
In der Handreichung sind Tipps zu datenschutzfreundlichen Einstellungen während der Installation ebenso gegeben wie Hinweise zu weiterführender Literatur. Damit können auch die Bürger, die ihr System bereits umgestellt haben, ihre Einstellung nachträglich noch einmal überprüfen. Sie finden die Handreichung unter https://www.tlfdi.de/imperia/md/content/datenschutz/themen/datenschutzunddatensicherheitiminternet/windows_10.pdf. Anbei auch der QR-Code, falls Sie die Tipps per Handy aufrufen wollen:

Wachsam bleiben!

Anlage 29

Pressemitteilung
vom 15. Juli 2016

US-Gericht verbietet Zugriff der amerikanischen Dienste auf europäische Server

Unternehmen mit Sitz in den USA, die personenbezogene Daten auf Servern in Europa speichern, können aufatmen. Vorerst. Im April 2014 entschied zunächst ein Bundesgericht der USA, dass solche Unternehmen mittels eines Durchsuchungsbefehls gezwungen werden können, Daten, die auf europäischen Servern gespeichert sind, an die US-Ermittlungsbehörden herauszugeben. Und zwar ohne Information des betroffenen Kunden. Am 14. Juli 2016 hat der United States Court of Appeals (Bundesberufungsgericht der Vereinigten Staaten) diese Entscheidung endlich aufgehoben und ist den Argumenten von Microsoft gefolgt. Der Stored Communication Act (SCA) ermächtigt nur dazu, Durchsuchungsbefehle zu erlassen, die auf das Hoheitsgebiet der USA begrenzt sind. Nicht jedoch darüber hinaus. Damit können Unternehmen auf diese Weise nicht verpflichtet werden, Daten, die in Europa gespeichert sind, an die US-Ermittlungsbehörden herauszugeben. Im Wesentlichen begründet das Gericht seine Aufhebung damit, dass der Congress üblicherweise Gesetze nur für das eigene Staatsgebiet erlässt; eine darüber hinausgehende Wirkung komme allenfalls dann in Betracht, wenn dies ausdrücklich im Gesetz bestimmt sei. Dies sei aber beim SCA gerade nicht der Fall.
Ein Wort der Vorsicht ist trotzdem angebracht. Einerseits ist die Entscheidung noch nicht rechtskräftig; den Vereinigten Staaten von Amerika als Berufungsgegner steht noch der Weg zum Supreme Court offen. Andererseits können Gesetze geändert werden, wie man auch in Deutschland beim „BND-Gesetz“ leidvoll erfahren musste.
Glücklicherweise gibt es die Reparaturinstanz der Gerichte!
Wieder ein guter Tag für den Datenschutz. ☺

Anlage 30

Pressemitteilung
vom 12. August 2016

Datenschutz konkret: Unternehmen im Fokus

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) interessiert sich für die Umsetzung datenschutzrechtlicher Regelungen in den Unternehmen, insbesondere für den betrieblichen Datenschutzbeauftragten und den internationalen Datenverkehr. Beides sind Themen, die in der Praxis des TLfDI als mögliche „Problemzonen" bekannt sind. Gerade beim internationalen Datenverkehr in die USA haben die Aufhebung des Safe Harbor-Abkommens und die Querelen um das Nachfolgeabkommen Privacy Shield bei vielen Unternehmen für Unsicherheit gesorgt, so zumindest der Eindruck des TLfDI.

Deswegen nimmt der TLfDI im Rahmen einer Umfrage zu diesen Themen 75 Unternehmen in den Blick.

Ziel der Umfrage ist es, bei den befragten Unternehmen Defizite zu erkennen und diese bei notwendigen datenschutzrechtlichen Nachbesserungen zu beraten und zu unterstützen. Der TLfDI setzt wie gewohnt auf Kooperation mit den Unternehmen, um die datenschutzrechtlichen Bestimmungen effektiv umzusetzen.

Anlage 31

Pressemitteilung
vom 17. August 2016

Reaktion des Datenschutzbeauftragten auf Spekulationen in der „Abhöraffäre“

Die Ermittlungen des Datenschutzbeauftragten Dr. Lutz Hasse in der sog. Polizei-Abhöraffäre beziehen sich inzwischen auch auf das Thüringer Innenministerium.

Pikanterweise verlautet dazu – wie heute der Presse zu entnehmen ist – nun aus „dem Umfeld“ des Thüringer Innenministeriums, dass der Datenschutzbeauftragte in seiner früheren Funktion als Referatsleiter im Innenministerium möglicherweise in die Aufhebung der in der Dienstanweisung zur Aufzeichnung von Telefonaten in der Thüringer Polizei geregelten Berichtspflicht der Polizeibehördenleiter involviert gewesen sein soll.

Aufgrund dieser Spekulationen hat Dr. Lutz Hasse vorsorglich die datenschutzrechtliche Prüfung der Angelegenheit vorerst und bis zur Klärung des Sachverhalts an seine Stellvertreterin im Amt abgegeben.

Anlage 32

Pressemitteilung
vom 18. August 2016

„DeviceWatch“

Während der gestrigen Landtagssitzung wies der Abgeordnete Rainer Kräuter (DIE LINKE) darauf hin, dass im LKA Thüringen die Software „DeviceWatch“ installiert worden sei. Dabei handele es sich um ein Projekt, „dass die flächendeckende Überwachung eines jeden Nutzers im Polizeisystem, eines jeden Personalratsmitglieds, eines jeden Gewerkschafters, eines Beauftragten, eines jeden Beschäftigten ermöglicht.“

„Eine derartige Überwachung würde in hohem Maße in das Grundrecht auf informationelle Selbstbestimmung der Betroffenen eingreifen“, sagte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI), Dr. Lutz Hasse. Er hat sich bereits der Angelegenheit angenommen und beabsichtigt, das Verfahren zu prüfen. Vom Thüringer Landeskriminalamt hat der TLfDI heute Aufklärung in der Sache verlangt und einen Kontrolltermin vereinbart.

Anlage 33

Pressemitteilung
vom 26. August 2016

Apple im Visier – Sicherheitslücke „Pegasus“
gefährdet iPhone-Nutzer

Heute Morgen ist bekannt geworden, dass eine Schadsoftware für das iPhone existiert, die bisher unbekannte Sicherheitslücken des Smartphones ausnutzen kann. Die Spionage-Software mit dem Namen „Pegasus“ kann viele Funktionen manipulieren, Gespräche abhören und Nachrichten mitlesen. Sicherheitsforscher haben die Spyware untersucht und Apple gemeldet. Apple hat reagiert und ein Sicherheitsupdate entwickelt. Die Version iOS 9.3.5 ist bereits fertiggestellt und kann auf iPhones installiert werden. Das Update wird von Apple automatisch angeboten oder ist über die Software iTunes installierbar.

Sicherheitslücken sind immer eine Gefahr für Smartphones und andere Computersysteme. Ein regelmäßiges Aktualisieren durch Updates ist auch für Smartphones unverzichtbar, um die Sicherheit des Gerätes zu gewährleisten. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) Dr. Lutz Hasse rät daher: „iPhone-Nutzer sollten das Update schnell installieren und die Programme von Apple nutzen, um die Sicherheit des Smartphones wiederherzustellen.“

Anlage 34

Pressemitteilung
vom 31. August 2016

Telefonaufzeichnungen in der Thüringer Polizei: Thüringer Landesbeauftragter für den Datenschutz und die Informationsfreiheit (TLfDI) rügt Falschauskunft durch ehemaliges TIM

Bereits 2013 hatte der TLfDI in der „Babyphone“-Affäre das Thüringer Innenministerium aufgefordert, auch die Telefonapparate mit Aufzeichnungsfunktion zu benennen.

Wie sich im Zuge der Ermittlungen des TLfDI zur Aufzeichnungsaffäre nunmehr herausstellte, war die Antwort der ehemaligen Hausspitze auf diese Frage falsch und irreführend.

Mit dieser Falschauskunft sollte der TLfDI hinter die Fichten geführt werden – erfolglos!

Diesen Verstoß der früheren Hausspitze gegen das Thüringer Datenschutzgesetz beanstandete der TLfDI heute förmlich.

Hiervon unberührt bleibt natürlich die bisherige datenschutzfreundliche Kooperation mit der neuen Hausspitze.

Anlage 35

Pressemitteilung
vom 2. September 2016

Medienkompetenz: Unterrichtsmaterial aktualisiert!

„Den Schutz der Privatsphäre in den Köpfen der Schüler und Lehrer höher hängen!“ – ist berechtigtes Anliegen des obersten Datenschützers in Thüringen. Seit mehreren Jahren setzt sich der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit, Dr. Lutz Hasse, nachdrücklich dafür ein, dass Datenschutzaspekte in den Unterricht an allgemeinbildenden Schulen einfließen, um Kinder und Jugendliche zu kompetentem Mediengebrauch zu befähigen. Im März 2016 ging eine Mediendatenbank seiner Behörde online, die Lehrerinnen und Lehrer auf geeignete Materialien hinweist. Seit dem 1. September 2016 ist nun eine neue Fassung verfügbar (https://medien.tlfdi.de). Der Datenbestand wurde aktualisiert und ergänzt. Unter anderem wurden einige empfehlenswerte Links aufgenommen, die auch für Eltern interessant sind: „SCHAU HIN! – Was dein Kind mit Medien macht“ ist eine Initiative des Bundesfamilienministeriums und weiterer Akteure. Ein Blick auf die Internetseite http://www.schau-hin.info/ lohnt sich, wenn man Infos zu sinnvollem Umgang der Kids mit Internet, sozialen Medien und Mobilgeräten sucht. Auch den Artikel bei www.heise.de „Pokémon Go – Datenschützer kritisiert Nutzungsbedingungen“ sollte man gelesen haben, bevor man seine Kinder auf die Suche nach Rattfratz, Habitak, Schiggy und Co. gehen lässt. Lehrer, die Material zum Thema Big Data für ihren Unterricht suchen, werden bei den Links zur Reihe „Dennis Digital“ fündig.
☺ Lehr- und Lernspaß wünscht:

Dr. Lutz Hasse

Anlage 36

Pressemitteilung
vom 27. Oktober 2016

Save the Date: Profiling
Big Data – Small Privacy
Zum Niedergang der Privatsphäre



Das Abfischen von Daten zur Bildung von Persönlichkeitsprofilen z. B. beim Einkaufen, in sozialen Netzwerken, in persönlichen Blogs oder von Kontakt-, Bewegungs- oder Geodaten ist heutzutage gang und gäbe.

Oft geschieht es heimlich. Aber warum? Wer hat Interesse an den Daten?
Zu welchem Zweck werden die Daten genutzt? An wen werden sie weitergegeben?

Die Veranstaltung wird in unbekannte Welten vordringen und ist wahrscheinlich nichts für schwache Nerven.

Ministerpräsident Bodo Ramelow und Minister Wolfgang Tiefensee, zuständig für Wirtschaft, Wissenschaft und Digitale Gesellschaft, konnten bereits für Grußworte gewonnen werden.

In die Untiefen des Daten-Meeres führen uns:

- Yvonne Hofstetter
(Autorin Spiegel-Bestseller „Sie wissen alles“ und „Das Ende der Demokratie“),
- Mike Kuketz (analysierte u. a. die Android-App „Pokémon-Go“),
- Kai Biermann (u. a. Journalist, Autor, Blogger),
- Prof. Dr. Dorina Gumm (u. a. Spezialistin für IT-Sicherheit),
- Prof. Dr. Kai-Uwe Sattler (u. a. Spezialist für Big Data).

Bitte merken Sie sich diese spannende Veranstaltung schon einmal vor!

Wann: Am 14. Februar 2017 von 10.00 bis 15.30 Uhr

Wo: Augustinerkloster Erfurt

Wichtig: Die Teilnehmeranzahl ist begrenzt.
Anmeldungen können bereits jetzt per E-Mail an poststelle@datenschutz.thueringen.de erfolgen.

Anlage 37

Pressemitteilung
vom 8. November 2016

Dashcams: Selbsternannten Rittern des Rechts wird datenschutzrechtliche Abfuhr erteilt!

Die Dashcam als ständiger Begleiter in Fahrzeugen wird auch auf Thüringens Straßen immer beliebter. Nicht selten werden diese kleinen und fast nicht wahrnehmbaren Geräte dazu benutzt, die Fahrtstrecke mit allen Fahrzeugen und Verkehrsteilnehmern ohne besonderen Anlass zu beobachten und gleichzeitig aufzuzeichnen. Diese Praxis steht jedoch nicht im Einklang mit dem Bundesdatenschutzgesetz (BDSG), sie stellt vielmehr einen eklatanten Eingriff in das Recht auf informationelle Selbstbestimmung der übrigen Verkehrsteilnehmer dar. Unlängst wurde nun dieses lückenlose Abfilmen von Autofahrten mit einer Dashcam vor dem Verwaltungsgericht Göttingen verhandelt. Ein Autofahrer hatte sein Fahrzeug an Front- und Heckscheibe mit Dashcams ausgerüstet, um im Nachhinein vermeintliche und tatsächliche Verkehrsverstöße Dritter zur Anzeige zu bringen. Ihm wurde seitens der zuständigen Behörde die Verwendung dieser Kameras zur Dokumentation des Verkehrsgeschehens untersagt und die Löschung der datenschutzwidrig angefertigten Videoaufnahmen angeordnet.
Das Verwaltungsgericht Göttingen hat diese Auffassung bestätigt und ebenfalls einen Verstoß gegen datenschutzrechtliche Vorschriften, insbesondere gegen § 4 Abs. 1 BDSG, gesehen. Es stellte weiterhin fest, dass der betroffene Autofahrer hier die Kameras nutzt, um sich zum Sachwalter öffentlicher Interessen aufzuschwingen, indem er andere Verkehrsteilnehmer beobachtet und Beweisdokumentationen anfertigt. Das Verwaltungsgericht stellt hier klar, dass die öffentliche Aufgabe der Gewährleistung des gesetzeskonformen Straßenverkehrs ausschließlich der Polizei und den Straßenverkehrsbehörden obliegt, nicht aber privaten Dritten. Inwieweit dann solche unzulässig erstellten Aufnahmen als Beweismittel vor Gericht verwertet werden können, ist ein Teil der unabhängigen tatrichterlichen Prüfung und ist dem Kontrollrecht des TLfDI entzogen. Im letzten Tätigkeitsbericht des TLfDI (2. TB LfDI Thüringen, S. 129f.) wurde bereits auf die datenschutzrechtliche Unzulässigkeit von Dashboard-

Kameras und auf das Urteil des VG Ansbach vom 12. August 2014 hingewiesen.

Anlage 38

Pressemitteilung
vom 25. November 2016

Kontrollfreie Zonen für besonders sensible Daten

Im Internet findet sich der Entwurf des Bundesinnenministeriums für ein Gesetz zur Anpassung des nationalen Datenschutzrechts an die Europäische Datenschutz-Grundverordnung. Er sieht vor, dass die Aufsichtsbehörde bei Berufsgeheimnisträgern künftig nur noch den Datenschutz mit Blick auf die Technikgestaltung und auf datenschutzfreundliche Voreinstellungen prüfen darf.
Prüfungen, wie in einer Praxis mit den Patientendaten tatsächlich umgegangen wird, sind damit ab 25. Mai 2018 tabu. Wenn etwa im Karneval (wieder) Patientendaten mit der Konfettikanone in der Öffentlichkeit verbreitet würden, wären dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) die Hände gebunden. Oft wenden sich Patienten an den TLfDI und teilen mit, dass Patientenakten offen herumlägen oder Daten leichtfertig an Dritte weitergegeben würden. Zwar haben die Betroffenen zivilrechtliche Ansprüche gegen die Berufsgeheimnisträger und die unbefugte Offenbarung von Berufsgeheimnissen ist unter Strafe gestellt. Der Gang zum Rechtsanwalt stellt für viele aber eine hohe Hürde dar und die Staatsanwaltschaft wird i. d. R. nur auf einen fristgebundenen Antrag des Betroffenen tätig. Der Betroffene muss zum einen von dem Verstoß wissen und sich zum anderen trauen, rechtliche Schritte einzuleiten. In der Vergangenheit vertrauten sich die Patienten in solchen Fällen stattdessen oftmals lieber dem Datenschutzbeauftragten an.
„Eine derartige Beschneidung der bewährten Prüfbefugnisse der Aufsichtsbehörde ist sachlich nicht gerechtfertigt und schwächt die Position der Betroffenen nachhaltig“, so Dr. Lutz Hasse. Er wird sich dafür einsetzen, dass die Aufsichtsbehörde die Einhaltung datenschutzrechtlicher Vorschriften bei Berufsgeheimnisträgern auch in Zukunft wirksam durchsetzen kann.

Anlage 39

Pressemitteilung
vom 5. Dezember 2016

Wearables mit „Gesundheitsfunktion“

Mehrere Landesdatenschutzbeauftragte beteiligten sich an einer deutschlandweiten Prüf-Aktion von Fitness-Armbändern als auch Smart Watches mit Gesundheitsfunktionen, sogenannte Wearables mit Gesundheitsfunktionen.
Das Prüf-Ergebnis war eindeutig: **Keines der 16 getesteten Geräte erfüllt die datenschutzrechtlichen Anforderungen vollständig.**
Diese scheinen zu einer gesunden Lebensweise zu motivieren und die Bewegung im Alltag zu fördern. So können die Wearables z B. Schritte zählen, zurückgelegte Kilometer messen und verbrauchte Kalorien erfassen. Man könnte meinen, sie können auch den Arzt ersetzen: Die geprüften Geräte können die Herzfrequenz überwachen, über Sensoren die Körpertemperatur auf der Haut bestimmen und informieren über den Schlafrhythmus. Diese Angaben dienen immer mehr aber auch Krankenkassen, Unternehmen der Versicherungs-und der Gesundheitsbranche.
Daher lohnte es aus datenschutzrechtlicher Sicht, die Geräte genauer unter die Lupe zu nehmen:
Datenschutzmängel finden sich zurzeit in allen nur denkbaren Varianten: keine Transparenz, fehlende Nachvollziehbarkeit, unzureichende informierte Einwilligung!
Datenschutzerklärungen sind häufig zu pauschal und nicht nachvollziehbar. Wer Wearables mit Gesundheitsfunktionen nutzt, sieht sich oftmals zahlreichen Firmen gegenüber, die die Nutzer-Daten erhalten können. Offen bleibt zumeist, wer für was zuständig ist und was mit den Daten zu welchen Zwecken bei wem passiert und wie lange die Daten gespeichert werden.
Widerspruchsmöglichkeiten sind in der Regel nicht vorgesehen. Viele Geräte und Apps bieten dem Nutzer keine Möglichkeit, Daten selbst und vollständig zu löschen. Infolge der Zusammenführung der teilweise besonders schützenswerten Angaben kann ein präzises Profil des Tagesablaufs und ggf. des Gesundheitszustands eines Nutzers generiert werden.

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit, Dr. Lutz Hasse: „Die Kunden müssen wissen, dass eine datenschutzgerechte Nutzung der meisten Wearables mit Gesundheitsfunktionen derzeit kaum möglich ist. Wegen der fehlenden Löschfunktion vielen Geräten birgt insbesondere auch ein Verlust oder Weiterverkauf von Wearables ein hohes Risiko."

Anlage 40

Pressemitteilung
vom 9. Dezember 2016

Kooperation zwischen Kultusministerkonferenz und Datenschutzbeauftragtem macht große Fortschritte

Es ist soweit! Nach intensiver Arbeit hat die Kultusministerkonferenz am 8. Dezember ihre Strategie „Bildung in der digitalen Welt“ ins Land geschickt. Nach großem Kraftakt mit breiter Fachdiskussion haben die Kultusminister festgelegt, was sich ändern muss in Sachen Medienbildung an Schulen und Hochschulen. Und weil Medienbildung im Digitalzeitalter immer was mit Privatsphärenschutz zu tun hat, war auch die Meinung der Datenschützer von Bund und Ländern gefragt. Der Arbeitskreis „Datenschutz und Bildung“ unter Federführung des TLfDI lieferte eine umfangreiche Zuarbeit zum Entwurf. Das Ergebnis dieser Kooperation kann sich sehen lassen. Dieses Strategiepapier schlägt jenes von 2012 um Längen. Klar wird definiert, was Schülerinnen und Schüler können müssen, um im Digitalzeitalter zu bestehen. Dabei ist auch ein Kompetenzbereich „Schützen und sicher agieren“, der zum sensiblen Umgang mit Risiken für die Privatsphäre befähigen soll. Kompetenz meint: Kennen, bewerten und handeln können (!). Veränderungen in der Schule brauchen veränderte Lehrer. Folgerichtig sind klare Anforderungen an deren Aus- und Fortbildung formuliert. Hochschulen mit Lehramtsstudiengängen haben hier eine Schlüsselposition. Neben eigener Medienkompetenz heißt das für angehende Lehrer auch, digitale Medien im Fachunterricht sinnvoll nutzen und über Medieninhalte mit den Schülern reflektieren zu können. Und da gibt’s Nachholbedarf! Es geht alle Lehrer an, denn Medienbildung ist und bleibt Sache aller Unterrichtsfächer. Deshalb sollen Bildungs- und Lehrpläne ausnahmslos auf den Prüfstand und jene Lehrer, die bereits in den Schulen unterrichten, durch zeitgemäße Fortbildungsangebote fit gemacht werden.
Die KMK-Strategie ist eine Seite, die andere die Umsetzung. Sie muss sportlich angegangen werden, denn bereits ab Schuljahr 2018/19 soll es losgehen in den Klassenstufen 1 und 5. Der betreffende Arbeitskreis der Datenschutzbeauftragten unter Vorsitz des TLfDI hat bereits gegenüber dem KMK-Sekretariat seine Unter-

stützung bei der Implementation erklärt. Das Angebot des TLfDI gilt selbstverständlich auch für Thüringen – entsprechende Kooperation mit Thüringer Ministerien, der Landesmedienanstalt und dem Lehrerfortbildungsinstitut ist bereits in Vorbereitung.

Anlage 41

Pressemitteilung
vom 20. Dezember 2016

Polizei: Aufzeichnung von Telefongesprächen/„DeviceWatch“

Die datenschutzrechtlichen Vorwürfe gegen die Thüringer Polizei über das Aufzeichnen von Telefongesprächen und die behauptete Mitarbeiterüberwachung durch das Programm „DeviceWatch“ hielten den Thüringer Landesbeauftragten für den Datenschutz (TLfDI) in den letzten Wochen in Atem. Heute zog er angesichts aktuellen Medieninteresses eine Zwischenbilanz:

So hat das Thüringer Innenministerium u. a. nicht überprüft, ob die Voraussetzungen an eine zulässige Telefonüberwachung in der Praxis eingehalten wurden. Nach einer Dienstanweisung (DA) hierzu ist eine Aufzeichnung nur bei Notrufen, in Fällen des Notstandes oder der Nothilfe sowie bei Vorliegen einer Einwilligung möglich. Nach vorliegenden Erkenntnissen des Innenministeriums wurden jedoch nicht nur Notrufe, sondern auch Nicht-Notrufe auf dem Telefon des Diensthabenden zum Zweck der Dokumentation von dienstlichen Anweisungen automatisch aufgezeichnet. Dabei wurden auch andere aus- und eingehende Anrufe aufgezeichnet. Mit der Einrichtung der Landeseinsatzzentrale kam es zu einer grundlegenden Umstrukturierung des Notrufsystems der Thüringer Polizei. Die DA bildete indes diese neue Situation nicht ab, obwohl der nachgeordnete Bereich das Innenministerium mehrmals auf diese Notwendigkeit hingewiesen hatte. Auch bei der Praxis der Löschung der Aufzeichnungen gab es Änderungsbedarf.

Der TLfDI forderte das Thüringer Ministerium für Inneres und Kommunales auf, die notwendigen Maßnahmen zu ergreifen, damit bei der Aufzeichnung von Telefonaten in der Polizei die datenschutzrechtlichen Grundsätze beachtet werden. Hierzu gehört insbesondere, die DA zeitnah zu überarbeiten, wofür der TLfDI seine Unterstützung angeboten hat.

Datenschutzrechtlich beanstandet wurde auch das Thüringer Landeskriminalamt wegen des Einsatzes der Software „DeviceWatch“:

Zwar konnte der TLfDI derzeit keinen missbräuchlichen Einsatz der Software gegenüber Polizeibeamten feststellen. Dr. Lutz Hasse monierte aber in seiner ausgesprochenen Beanstandung unter anderem, dass für „DeviceWatch“ kein Verfahrensverzeichnis und kein Sicherheitskonzept vorliegen. Ferner fehlte es an einer Rechtsgrundlage zur Anfertigung von sog. Schattenkopien sowie transparenten Kontrollmechanismen. Aufgrund einer noch ausstehenden Information des Innenministeriums ist zudem noch nicht gänzlich geklärt, ob angesichts dieser Mitarbeiterkontrollmöglichkeit eine ordnungsgemäße Personalratsbeteiligung erfolgte.

Der TLfDI bleibt dran.

Anlage 42

Pressemitteilung
vom 31. Januar 2017

Polizei: Telefonatmitschnitte und „DeviceWatch“ –
TLfDI ermittelt weiter

Wir erinnern uns: Als sich der TLfDI mit seinen Ermittlungen im „Telefonmitschnitt-Skandal“ dem Thüringer Innenministerium näherte, wurde „aus dem Umfeld des Innenministeriums“ das Gerücht kolportiert, der TLfDI habe als ehemaliger Referatsleiter im TIM die Durchsetzung einer Dienstanweisung zur Anfertigung der Telefonatsaufzeichnungen durch Erlass behindert. Daraufhin hat der TLfDI – wie es sich gehört – die weiteren Ermittlungen in dieser Sache seiner Stellvertreterin übertragen. Nunmehr jedoch haben sich die Anwürfe gegen den TLfDI als haltlos erwiesen: Infolge der Nachforschungen des Innenministeriums selbst sowie des Sonderbeauftragten hat sich dieser Vorwurf erledigt. Der TLfDI wird hier also wieder die Zügel in die Hand nehmen. Dr. Lutz Hasse: „Ich danke meiner Stellvertreterin für die zwischenzeitlich fortgeführten Ermittlungen, die ich wieder an mich gezogen habe. Sowohl die Ermittlungen in Sachen Telefonmitschnitte als auch die Nachforschungen zum Software-Baukasten „DeviceWatch“ sind längst nicht abgeschlossen

Anlage 43

Pressemitteilung der unabhängigen Datenschutzbehörden der Länder
vom 1. Februar 2017

Entwurf zum Bundesdatenschutzgesetz verspielt Chance auf besseren Datenschutz!

Am heutigen Mittwoch hat das Bundeskabinett den Entwurf zu einem neuen Bundesdatenschutzgesetz (BDSG) beschlossen, der jetzt in den Bundestag eingebracht werden soll. Anlass der Gesetzesnovelle ist das neue EU-Datenschutzrecht, bestehend aus der Datenschutz-Grundverordnung (DS-GVO) und der Datenschutz-Richtlinie im Bereich Justiz und Inneres. Die Mitgliedstaaten haben bis Mai 2018 ihr nationales Datenschutzrecht an die Verordnung anzupassen und die Richtlinie in nationales Recht umzusetzen.

Nach Auffassung der unabhängigen Datenschutzbehörden der Länder wird der im Bundeskabinett beschlossene Gesetzentwurf den europarechtlichen Vorgaben nicht gerecht und stellt bereits bestehende datenschutzrechtliche Standards infrage. So schränkt der Entwurf die Informations-, Auskunfts- und Löschrechte der betroffenen Personen erheblich ein. Diese Einschnitte in die Betroffenenrechte stellen lediglich eine Arbeitserleichterung für die Daten verarbeitenden Stellen dar und stehen dem Schutzcharakter der Vorschriften zur Auskunft, Information und Löschung von Daten diametral entgegen. Die DS-GVO gestattet dem nationalen Gesetzgeber nur in sehr engem Rahmen, weitere Einschränkungen der Betroffenenrechte vorzusehen. Entsprechend der Intention der DS-GVO haben die Verantwortlichen vielmehr primär durch geeignete technische und organisatorische Maßnahmen dafür Sorge zu tragen, ihren Informations-, Auskunfts- und Löschpflichten zu genügen. Der nationale Gesetzgeber sollte auf eine weitergehende Beschneidung der Betroffenenrechte verzichten.

Darüber hinaus sieht der Gesetzentwurf zur Verarbeitung von Gesundheitsdaten sehr weitgehende Regelungen ohne Interessenabwägung vor. Er schafft damit zu allgemeine gesetzliche Verarbeitungsbefugnisse sowohl für nicht-öffentliche als auch öffentliche Stellen.

Es werden zudem keine verbindlichen technisch-organisatorischen Schutzmaßnahmen geregelt. Dies kann zu Lücken im gebotenen Grundrechtsschutz führen.

Daten dürfen nur zu einem oder mehreren vorab festgelegten Zwecken verarbeitet werden. Die auch hier bestehende Möglichkeit für den nationalen Gesetzgeber, in engem Rahmen konkrete Normen zur Zweckänderung zu schaffen, ist als Ausnahmetatbestand restriktiv auszulegen. Die detaillierten nationalen Regelungen des Gesetzentwurfs überdehnen ihn aber über alle Maßen, höhlen damit die Zweckbindung weiter aus und konterkarieren überdies das Ziel der Vereinheitlichung des europäischen Rechts. Diese Aushöhlung des Grundsatzes der Zweckbindung darf nicht Gesetzeskraft erlangen.

Wiederholt haben die Datenschutzbeauftragten des Bundes und der Länder ein umfassendes Gesetz zum Beschäftigtendatenschutz gefordert. Der Gesetzentwurf sieht demgegenüber lediglich einige klarstellende Regelungen für den Beschäftigtendatenschutz vor. Stattdessen bedarf es aber detaillierter bereichsspezifischer Regelungen auf Grundlage der DS-GVO.

Auch im Entwurf zum neuen BDSG findet sich die ausgeweitete Regelung zur Videoüberwachung durch Private, wie sie bereits mit dem „Videoüberwachungsverbesserungsgesetz“ eingefügt werden soll. Diesbezüglich wird auf die Entschließung der DSK vom 9. November 2016 verwiesen.

Schließlich kritisieren die Datenschutzbehörden der Länder, dass die Bundesbeauftragte für den Datenschutz als alleinige Vertreterin für alle deutschen Datenschutzbehörden im Europäischen Datenschutzausschuss (EDSA) vorgesehen ist. Stattdessen fordern die Landesdatenschutzbehörden eine Vertretungsregelung, die nicht nur der Unabhängigkeit aller Aufsichtsbehörden, sondern auch den tatsächlichen Vollzugszuständigkeiten Rechnung trägt, die vorwiegend bei den Ländern liegen. Dem EDSA kommt zukünftig eine zentrale Bedeutung zu, kann dieser doch Beschlüsse treffen, die für alle Aufsichtsbehörden verbindlich sind.

Der vom Kabinett verabschiedete Entwurf ist nach alledem trotz einiger Verbesserungen im Vergleich zu Vorentwürfen an einigen

Stellen europarechtlich zweifelhaft und enthält eine Reihe von datenschutzrechtlichen Rückschritten.

Anlage 44

Pressemitteilung
vom 20. Februar 2017

Small sister is watching you!

In tausenden Kinderzimmern steht sie und erfüllt Mädchenträume: die sprechende Spielzeugpuppe „Cayla“. Aber „Cayla“ ist in Wirklichkeit ein illegales Abhörgerät – ein verkleideter Bluetooth-Sender – und sendet ihre Gesprächsinhalte an die Server des amerikanischen Konzerns „Nuance Communications“. Dort werden die Stimmprofile, die „Cayla“ gesendet hat, ausgewertet und analysiert, einschließlich Wohnadresse der Puppenmama. Small sister ist watching you! Die Bundesnetzagentur hat Eltern dazu aufgerufen, die Puppe zu vernichten, da der Besitz von getarnten Abhöranlagen strafbar sei. Ein Vernichtungsprotokoll befindet sich auf der Webseite der Bundesnetzagentur. Konstruiert wurde die Puppe vom amerikanischen Unternehmen „Genesis“.
„Dass Privatunternehmen derart perfide Abhörtechniken benutzen und Kinderspielzeug in dieser Form manipulieren, um auch sensible Daten von Kindern und Familien verarbeiten zu können, ist schlicht eine Sauerei“, so Dr. Hasse. „Abhören und Überwachen von Privatpersonen wird offensichtlich zunehmend eher zur Regel als zur Ausnahme und die gesetzlichen Regelungen zum Datenschutz werden zunehmend zur Makulatur. Denn wohl kaum haben die Kinder, die mit der Puppe spielen, oder deren Eltern freiwillig eingewilligt, dass die Dialoge mit der Puppe aufgezeichnet, weitergesendet und ausgewertet werden.“ Der Thüringer Datenschützer rät den Eltern dringend, jedes „smarte“ Spielzeug zuvor ausgiebig unter die Lupe zu nehmen, bevor sie es ihrem Nachwuchs tatsächlich zum Spielen überlassen. „Wir brauchen dringend einen Spielzeug-TÜV, der sich auch auf derartige technische Kommunikationsfunktionen konzentriert“, so Hasse abschließend.

Wenn etwas unklar ist: TLfDI fragen!

Anlage 45

Pressemitteilung
vom 21. Februar 2017

Vernetzung fördern – Medienkompetenz stärken
Landesdatenschützer unterzeichnet Kooperationsvereinbarung

Am 20. Februar 2017 unterzeichnete der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit, Dr.Lutz Hasse, in Erfurt die Kooperationsvereinbarung zur nachhaltigen Weiterentwicklung von Medienkompetenz in Thüringen. Mitunterzeichner sind die Thüringer Staatskanzlei, das Thüringer Finanzministerium, Sozialministerium, Kultusministerium und Wirtschaftsministerium, die Landesmedienanstalt (TLM) sowie das Institut für Lehrerfortbildung, Lehrplanentwicklung und Medien (ThILLM). Ziel der Kooperationsvereinbarung ist es, die Medienkompetenz von Nutzern – Kindern und Jugendlichen ebenso wie Senioren – zu stärken. Die Vernetzung von unterschiedlichen Akteuren und Institutionen soll deren mediale Angebote für politische, soziale und kulturelle Teilhabe besser nutzbar machen.
„Diese Vereinbarung hat mir sehr am Herzen gelegen und ich bin froh, dass wir sie auf den Weg gebracht haben“, so Hasse. „Mit der Kooperationsvereinbarung wollen wir unsere Kräfte bündeln und damit die Nutzerfreundlichkeit der digitalen Medien für die Bürger erhöhen“, so Hasse weiter. „In der Datenschutzkonferenz der Länder führt der TLfDI den Vorsitz des Arbeitskreises ‚Datenschutz und Bildung‘ und kooperiert hierbei eng mit der Kultusministerkonferenz. Daher begrüße ich es sehr, dass diese Kooperationsvereinbarung auch die pädagogischen Kräfte in der Kindertagesbetreuung und das Lehrpersonal an Schulen und Hochschulen in den Blick nimmt. Denn neben dem Umgang mit modernen Medien ist ein wesentliches Ziel in der Lehrerbildung und in der Ausbildung von Lehramtsanwärtern auch, die Lehrkräfte zu befähigen, Schülern die Kenntnisse und Fähigkeiten zu vermitteln, mit denen sie ihre Privatsphäre effektiv und sicher schützen können. Privatsphärenschutz muss kein Lehrfach werden, aber er darf auch kein ‚Leerraum‘ in der Medienkompetenz sein“, sagte Hasse abschließend.

Anlage 46

Pressemitteilung
vom 7. März 2017

Medieninformation – Einladung

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit, Dr. Lutz Hasse, wird am 8. März 2017 im Staatlichen Berufsschulzentrum Wirtschaft und Verwaltung in Jena (Karl-Volkmar-Stoy-Schule) um 9.15 Uhr den 3. Datenschutztag eröffnen.

Herr Dr. Hasse wird einen Vortrag halten zum Thema „Datenschutz? – Mir doch egal!“. Im Nachgang findet eine Diskussionsrunde statt. Hier besteht auch die Möglichkeit, mit Herrn Dr. Hasse zu verschiedenen Themen des Datenschutzes ins Gespräch zu kommen.

Die Vertreter der Medien sind herzlich zur Teilnahme eingeladen.

Anlage 47

Pressemitteilung
vom 9. Mai 2017

2. Tätigkeitsbericht zur Informationsfreiheit

„Warum bekomme ich keine Auskunft über die Höhe von tatsächlich aufgewendeten Finanzmitteln für bestimmte, durch das Land geförderte Projekte?“, „Weshalb verweigert mir die Gemeinde die Kopie eines Protokolls einer öffentlichen Bauausschusssitzung?“, „Wer schützt sogenannte Whistleblower, d. h. Personen, die über Rechtsverstöße im öffentlichen und nicht-öffentlichen Bereich berichten?“, „Kann ich Einsicht in die Gutachten der Wissenschaftlichen Dienste des Bundestages und des Landtages nehmen?“. All diese Fragen und viele weitere werden im 2. Tätigkeitsbericht des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) beantwortet. Das inhaltliche Spektrum der Fragen ist dabei sehr vielfältig. Wer von wem wann welche Auskünfte verlangen darf, ist im Thüringer Informationsfreiheitsgesetz (ThürIFG) geregelt. Zweck des ThürIFG ist es, den freien Zugang zu amtlichen Informationen zu gewährleisten und die Voraussetzungen festzulegen, unter denen derartige Informationen zugänglich zu machen sind. Das Gesetz soll unter Wahrung schutzwürdiger Belange die Transparenz der Verwaltung vergrößern, die Möglichkeiten der Kontrolle staatlichen Handelns durch die Bürgerinnen und Bürger verbessern und damit die demokratische Meinungs- und Willensbildung in der Gesellschaft fördern.
„Information ist die Währung der Demokratie“, meinte bereits im 19. Jahrhundert der amerikanische Präsident Thomas Jefferson. Dies gilt in Zeiten erkennbarer Politikverdrossenheit mehr denn je. Diese Einstellung kann nur ausgeräumt werden, wenn den Bürgerinnen und Bürgern umfänglich das Recht auf Information eingeräumt wird.
Dass sich das Informationsfreiheitsgesetz noch nicht im wünschenswerten Umfange durchgesetzt hat, wird auf seine Defizite zurückzuführen sein: hohe Hürden für den informationssuchenden Bürger – zu vernachlässigende Kontrollrechte des TLfDI.
Mithin ruhen die Hoffnungen auf dem neuen Thüringer Transparenzgesetz.

Anlage 48

Pressemitteilung
vom 23. Juni 2017

Gericht kippt Vorratsdatenspeicherung in Deutschland –
ein guter Tag für den Datenschutz

Der Thüringer Datenschutzbeauftragte, Dr. Lutz Hasse, weist auf einen Beschluss des Oberverwaltungsgerichts für das Land Nordrhein-Westfalen (OVG NRW) vom 22. Juni 2017 hin (Az.: 13 B 238/17). Darin kommen die Richter zu dem Ergebnis, dass die deutschen Regelungen zur Vorratsdatenspeicherung gegen europäisches Recht verstoßen!

Dr. Hasse: „Der Beschluss ist ein erster Etappensieg auf dem Weg, das Recht auf informationelle Selbstbestimmung in das richtige Verhältnis zu den Sicherheitsregelungen zu setzen."

Das OVG NRW führt in seiner Begründung aus, dass die Regelungen im Telekommunikationsgesetz (TKG) pauschal die Speicherung von Verkehrs- und Standortdaten nahezu aller Nutzer von Telefon- und Internetdiensten ab dem 1. Juli 2017 vorschreiben. Diese pauschale Speicherpflicht, so das Gericht, verstoße gegen die Datenschutzrichtlinie für elektronische Kommunikation 2002/58/EG und gegen das Urteil des Europäischen Gerichtshofs vom 21. Dezember 2016 (Az.: C-203/15 und C-698/15). Danach seien nur solche Regelungen zulässig, die den Kreis der von der Speicherung betroffenen Personen personell, zeitlich oder geografisch soweit beschränken, dass zumindest mittelbar ein Bezug zu schweren Straftaten oder schwerwiegenden Gefahren für die öffentliche Sicherheit hergestellt werde. Diese Vorgaben verletze das TKG jedoch.

Geklagt hatte im Ausgangsfall ein IT-Unternehmen aus München, das u. a. Internetzugangsleistungen für Geschäftskunden in Deutschland und in anderen EU-Mitgliedstaaten erbringt und daher der Verpflichtung zur Vorratsdatenspeicherung hätte nachkommen müssen.

„Glücklicherweise erweist sich im zunehmenden Maße die Justiz als das notwendige Korrektiv zu einer die Privatsphäre durchlöchernden

Gesetzgebung. Man darf also gespannt sein, welche weiteren Schnellschuss-Gesetze am EU- und Verfassungsrecht abprallen werden“, so das Fazit von Dr. Hasse.

Anlage 49

Pressemitteilung
vom 29. Juni 2017

Bundesnetzagentur dreht Vorratsdatenspeicherung die Luft ab

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI), Dr. Lutz Hasse, hat in seiner Pressemitteilung vom 23. Juni 2017 über Folgendes berichtet:

Gericht kippt Vorratsdatenspeicherung in Deutschland – ein guter Tag für den Datenschutz. Am 22. Juni 2017 hat das Oberverwaltungsgericht Nordrhein-Westfalen (OVG NRW) entschieden, dass die deutschen Regelungen zur Vorratsdatenspeicherung gegen europäisches Recht verstoßen (vgl. OVG NRW, Az.: 13 B 238/17). Zur Begründung hatte das OVG ausgeführt, dass die Regelungen im Telekommunikationsgesetz (TKG) in ihrer gegenwärtigen Ausgestaltung nicht mit der Datenschutzrichtlinie für elektronische Kommunikation 2002/58/EG und dem Urteil des Europäischen Gerichtshofs vom 21. Dezember 2016 (Az.: C-203/15 und C-698/15) vereinbar seien. Die pauschale Speicherung von Verkehrs- und Standortdaten fast aller Nutzer von Telefon- und Internetdiensten ab dem 1. Juli 2017 ohne einen konkreten Verdacht auf strafbare Handlungen ist nach Auffassung des Gerichts rechtswidrig.

Gestern, am 28. Juni 2017, reagierte die Bundesnetzagentur auf das Urteil des OVG NRW und setzte die Pflicht zur Vorratsdatenspeicherung aus. Damit wird die Speicherpflicht bis auf weiteres nicht durchgesetzt.

„Die Entscheidung des OVG NRW und seine Umsetzung durch die Bundesnetzagentur sind ein wichtiger Etappensieg für den Datenschutz“, so Dr. Lutz Hasse. „Im Interesse des Schutzes der Privatsphäre unbescholtener Bürgerinnen und Bürger werden diese nicht mehr unter Generalverdacht gestellt. Ich vertraue auf unsere Justiz, dass der hier eingeschlagene Weg weiter beschritten wird“, so Dr. Hasse zuversichtlich.

Anlage 50

Pressemittelung
vom 30. Juni 2017

Drohnenverordnung: Keine Peepshow mehr mit Drohnen!

Mittlerweile ist es auch in Thüringen für viele Privatpersonen ein beliebtes Hobby: das Steuern einer Drohne mit Kamerafunktion. Aber Vorsicht: Sobald mit der Kamera z. B. Menschen gefilmt und damit personenbezogene Daten erhoben werden, müssen das Recht am eigenen Bild und das Grundrecht auf informationelle Selbstbestimmung beachtet werden. „Mit der Kamera einer Drohne darf grundsätzlich niemand gegen seinen Willen gefilmt werden“, so der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) Dr. Lutz Hasse. Daher begrüßt Dr. Hasse ausdrücklich diesbezügliche Regelungen in der Verordnung zur Regelung des Betriebs von unbemannten Fluggeräten vom 30. März 2017. Bereits im April 2017 sind weite Teile der Verordnung in Kraft getreten.

„Im Hinblick auf den Schutz der Privatsphäre begrüße ich es sehr, dass die Drohnenverordnung ein Betriebsverbot von Kameradrohnen über Wohngrundstücken ohne Zustimmung der Bewohner ausdrücklich festschreibt“, so Dr. Hasse.

Darüber hinaus müssen alle Drohnen ab einem Gewicht von 250 g ab 1. Oktober 2017 mit Namen und Anschrift des Eigentümers versehen werden (Kennzeichnungspflicht). Für den Betrieb von Drohnen ab 2 kg Gewicht ist dann zudem ein behördlich ausgestellter und anerkannter Kenntnisnachweis erforderlich.

„In einigen öffentlichen Bereichen wie in der Land- und Forstwirtschaft oder zur Gefahrenabwehr im Sicherheitsbereich durch Feuerwehr und Polizei ist die Drohnennutzung mit ihren optischen und akustischen Möglichkeiten zweifellos sinnvoll. Im privaten Bereich ist die Drohnennutzung eher ein technisches Hobby, das der Gesetzgeber nicht gänzlich verbieten kann; er steht hier jedoch in der Pflicht, den datenschutzgerechten Einsatz gesetzlich zu regeln und so zu verhindern, dass der Garten des Nachbarn oder der FKK-Bereich

am See plötzlich als Peep-Show bei Youtube zu finden sind. Insofern sind die neuen Regelungen der Drohnenverordnung des Bundesministeriums für Verkehr und digitale Infrastruktur ein Schritt in die richtige Richtung“, so Hasse abschließend.

Anlage 51

Pressemitteilung
vom 27. Juli 2017

Keine Weitergabe von Fluggastdaten:
EuGH stärkt Datenschutzrechte

Am gestrigen Mittwoch, 26 Juli 2017, veröffentlichte der Europäische Gerichtshof (EuGH) sein Gutachten zur geplanten Übermittlung von Passagierdaten zwischen der EU und Kanada. Wie zu erwarten war, stoppte der EuGH das geplante Abkommen und steht damit zu 100 Prozent rechtlich auf der Linie der Datenschutzbeauftragten des Bundes und der Länder.
Bereits im März 2011 hatte die Konferenz der Datenschutzbeauftragten die EU-Richtlinie zur Nutzung von EU-Flugpassagierdaten zur Gefahrenabwehr und Strafverfolgung aus Datenschutzgründen abgelehnt mit der Begründung, dass die Richtlinie weitreichende Eingriffe in Bürgerrechte ermögliche, insbesondere im Hinblick auf die vorgeschlagene Speicherung von Fluggastdaten. In Bezug auf das nunmehr geplante Abkommen zwischen der EU und Kanada zum Austausch und der Speicherung von Fluggastdaten argumentierte der EuGH erneut in diesem Sinne.
Insbesondere kritisierte er, dass die Übermittlung sensibler Daten (z. B. rassische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit, Sexualleben) angesichts des Datenmissbrauchsrisikos einer präzisen und besonders fundierten, auf andere Gründe als den Schutz der öffentlichen Sicherheit vor Terrorismus gestützten rechtlichen Rechtfertigung bedürfe. Hieran fehle es indes. Weiterhin bewertete der EuGH die geplante Datenspeicherung für fünf Jahre als rechtlich unzulässig, wenn nachweislich keine objektiven Anhaltspunkte für kriminelle bzw. terroristische Bestrebungen des betreffenden Passagiers bestehen.
„Ohne Zweifel stehen die EU-Staaten in der Pflicht, die Sicherheit der Menschen in der Europäischen Union bestmöglich und umfassend zu gewährleisten, insbesondere im Hinblick auf die Opfer der Terroranschläge von Paris, Berlin und London 2016 und 2017“, so der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit Dr. Lutz Hasse. „In diesem Sinne müssen grenzüber-

schreitende Kriminalität und terroristische Straftaten bereits im Vorfeld aufgedeckt und verhindert werden. Dennoch müssen gerade für die grenzüberschreitende Übermittlung von sensiblen personenbezogenen Daten klare rechtsstaatliche Voraussetzungen gelten und diese Übermittlung darf nicht um jeden Preis auf Kosten des Datenschutzes und des Schutzes der Privatsphäre erfolgen. Daher begrüße ich es, dass der EuGH diesen Rechten erneut einen hohen Stellenwert eingeräumt hat“, so Dr. Hasse abschließend.

Anlage 52

Pressemitteilung
vom 28. Juli 2017

Keine Kündigung infolge illegaler Überwachung des PC!

Eine Arbeitgeberin hatte ihre Mitarbeiter darüber informiert, dass ihre Internetaktivitäten auf dem Dienst-PC mithilfe einer Software (Keylogger), die alle Tastaturangaben aufzeichnet, kontrolliert und regelmäßige Bildschirmfotos (Screenshots) erstellt werden. Nach Auswertung der entsprechenden Dateien kündigte die Arbeitgeberin einem Arbeitnehmer wegen der privaten Nutzung des Dienst-PCs fristlos. Der Arbeitnehmer klagte dagegen und erhielt gestern, 27. Juli 2017, vom Bundesarbeitsgericht (BAG) in Erfurt Recht.
Danach ist die verdeckte Überwachung von Arbeitnehmern durch den Arbeitgeber rechtswidrig, wenn kein durch konkrete Tatsachen begründeter Verdacht auf eine Straftat oder eine schwerwiegende Pflichtverletzung besteht. Arbeitgeber dürfen solche rechtswidrig erlangten Informationen, die sie aus der Überwachung ihrer Arbeitnehmer am PC gewonnen haben, nicht als Kündigungsgrund heranziehen und die durch eine Überwachungssoftware gewonnenen Daten über private Tätigkeiten von Arbeitnehmern am PC dürfen im gerichtlichen Verfahren nicht verwendet werden, so der Tenor des aktuellen Urteils des BAG (BAG, 2 AZR 684/16).
„Das BAG hat mit seinem Urteil das Recht der Arbeitnehmer auf informationelle Selbstbestimmung erheblich gestärkt und damit auch dem Schutz der Privatsphäre deutlichen Vorrang gegenüber Arbeitgeberinteressen eingeräumt“, so der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) Dr. Lutz Hasse. „Ohnehin kann es nicht sein, dass Arbeitgeber von vornherein jeden Arbeitnehmer unter den Generalverdacht von Pflichtverletzung stellen und damit auch noch eine technische Überwachung rechtfertigen. Daher ist die Entscheidung der Erfurter Richter ein weiterer entscheidender Schritt auf dem Weg zur Stärkung des Beschäftigtendatenschutzes. Sowohl im Unternehmens-, aber auch im Behördenbereich wird in zunehmendem Maße Software eingesetzt, deren Mächtigkeit dem Arbeitgeber vielleicht gar nicht bewusst ist. Umso dringender ist es geboten, dass vor Nutzung solcher Software die

Personalvertretungen und Datenschutzkundigen, gern auch der TLfDI, in diese Prozesse eingebunden werden“, so Dr. Hasse.

Anlage 53

Pressemitteilung
vom 17. August 2017

EU-US Privacy Shield:
Informationen und Beschwerdeformulare für Betroffene veröffentlicht

Seit 1. August 2016 sind die zwischen der EU und den USA vereinbarten Neuregelungen für die Übermittlungen personenbezogener Daten in Kraft. Diese werden als EU-US Privacy Shield (EU-US-Datenschutzschild) bezeichnet. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) hat auf seiner Internetseite umfangreiche Informationen zum Privacy Shield einschließlich eines einheitlichen Beschwerdeformulars bereitgestellt.

Mit der Entscheidung der Europäischen Kommission vom 12. Juli 2016 zum sogenannten EU-US-Datenschutzschild steht seit 1. August 2016 eine neue Grundlage für Übermittlungen personenbezogener Daten in die USA zur Verfügung. Auf dieser Grundlage können personenbezogene Daten an US-Unternehmen übermittelt werden, die eine Privacy-Shield-Zertifizierung besitzen. Personen aus Europa haben in diesem Fall gegenüber den zertifizierten US-Unternehmen eine Reihe von Rechten: auf Information, auf Auskunft, auf Berichtigung und – unter bestimmten Umständen – auf Löschung sowie auf Garantien für den Fall einer Weiterübermittlung. Diese Rechte können von Betroffenen direkt gegenüber den zertifizierten US-Unternehmen geltend gemacht werden. Daneben ist es auch möglich, sich jederzeit an die zuständige nationale Datenschutzbehörde zu wenden.

Um es Betroffenen zu erleichtern sich zu informieren und gegebenenfalls eine Beschwerde einzureichen, hat der TLfDI allgemeine Informationen zum Privacy Shield sowie ein einheitliches **Beschwerdeformular** auf seiner Internetseite veröffentlicht.

Der Privacy Shield räumt europäischen Bürgern erstmals auch eine Überprüfungsmöglichkeit ein, wenn sie Zugriffe von US-amerikanischen Sicherheitsbehörden oder Nachrichtendiensten unter Verstoß gegen geltende Bestimmungen auf ihre aus Europa übermittelten Daten befürchten. Für die Untersuchung solcher Anträge wurde eine Ombudsperson im US-Außenministerium neu eingerichtet.

Diese ist verpflichtet, Anträgen zur Überprüfung, die ihr von den europäischen Datenschutzbehörden zugeleitet wurden, nachzugehen und diese zu beantworten.
Der TLfDI hat unter https://www.tlfdi.de/tlfdi/datenschutz/save-harbor-privacy-shield/ auf seiner Internetseite für Bürger und Unternehmen die wichtigsten Informationen und relevanten Dokumente zum Privacy Shield bereitgestellt.

Anlage 54

Pressemitteilung
vom 22. August 2017

Richtigstellung des Datenschutzbeauftragten

In einer Pressemitteilung der CDU-Fraktion im Thüringer Landtag vom 20. August 2017 unter dem Titel „CDU-Fraktion droht mit rechtlichen Schritten gegen Hasse“ beklagt sich der Obmann der CDU-Fraktion im Untersuchungsausschuss 6/2, der Abgeordnete Manfred Scherer: „Seit Monaten missachtet der Thüringer Datenschutzbeauftragte einen Beschluss des Ausschusses auf Aktenvorlage. Nicht einmal eine Stellungnahme oder Erklärung zu dem Verlangen des Ausschusses hat Herr Hasse bislang für nötig erachtet.“ Zu diesem Vorwurf darf ich Ihnen – da sich diese Information in der Presseschau des Thüringer Landtags und der Thüringer Landesregierung vom heutigen Tag nicht findet – die Presseinformation des Thüringer Landtags Nr. 183/2017 (Anlage) zur Kenntnis geben.

Danach erweist sich der Vorwurf des Abgeordneten Scherer als haltlos: „Es wurde festgestellt, dass der TLfDI am 21. Juli 2017 auf das ergänzende Aktenvorlageersuchen der Fraktion der CDU ein Schreiben versandt hat, welches irrtümlich der Vorsitzenden zugeleitet worden ist.“ Zwischenzeitlich wurde dem TLfDI auch bestätigt, dass die Anlagen zu diesem Schreiben natürlich ebenfalls rechtzeitig vorgelegen haben. Mithin ist der TLfDI – wie bisher – seinen Verpflichtungen nachgekommen.

Anlage zur Pressemitteilung vom 22. August 2017

Nr. 183/2017 Erfurt, 21. August 2017

Untersuchungsausschuss 6/2

Heute (Montag) kam der Untersuchungsausschuss 6/2 zur Aufklärung eines möglichen Fehlverhaltens des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und anderer Behörden im Zusammenhang mit dem Auffinden eines Aktenlagers in Immelborn zu seiner 27. Sitzung zusammen.

In der Sitzung wurde ein Antrag auf Verlesung eines Schriftstückes beschlossen, dessen Inhalt für die rechtliche Einordnung der im Zusammenhang mit dem Aktenlager in Immelborn durch den TLfDI getroffenen Maßnahmen relevant sein soll.

Zudem wurden sechs Zeugen vernommen, darunter der Direktor des zuständigen Registergerichts, welcher Fragen im Zusammenhang mit dem Nachtragsliquidationsverfahren über das Vermögen der Aktenmanagement & Beratungs GmbH beantwortete, außerdem ein vormaliger Mitgesellschafter dieser GmbH sowie zwei Mitarbeiter des TLfDI, die in dem Aktenlager in Immelborn die Aussonderung von Akten beaufsichtigt haben.

Außerdem wurden Fotoaufnahmen in Augenschein genommen, die ein Zeuge Anfang des Jahres 2015 in dem Aktenlager in Immelborn gefertigt hatte.

Es wurde festgestellt, dass der TLfDI am 21. Juli 2017 auf das ergänzende Aktenvorlageersuchen der Fraktion der CDU ein Schreiben versandt hat, welches irrtümlich der Vorsitzenden zugeleitet worden ist. Es muss noch geprüft werden, ob die darin benannten Anlagen vorliegen.

Die nächste (29.) Sitzung findet am 18. September 2017 statt.

Anlage 55

Pressemitteilung
vom 19. September 2017

Meldepflicht für (Wild-)Kameras bestätigt!

Bereits mit Urteil vom 18. Mai 2016 stellte das Verwaltungsgericht Saarland fest, dass die Videoüberwachung mittels Wildbeobachtungskameras durch nicht-öffentliche Stellen **(u. a. natürliche und juristische Personen des Privatrechts)** grundsätzlich der Meldepflicht des § 4d Abs. 1 Bundestatenschutzgesetz (BDSG) unterfällt. Die gegen das Urteil eingelegte Berufung von drei Jägern wurde mit Urteil vom 14. September 2017 durch das **Oberverwaltungsgericht Saarland** abgewiesen und die **Meldepflicht für Wildtierkameras bestätigt**. Die Revision gegen das Urteil wurde nicht zugelassen.

Auch der TLfDI vertritt, wie schon seit seiner Pressemitteilung vom 19. Mai 2016, die Auffassung, dass Wildtierkameras der Meldepflicht unterfallen.

Was allerdings für Wildkameras gilt, muss für alle anderen Kameras erst recht gelten:
Nicht-öffentliche Stellen in Thüringen müssen Kameras vor dem Einsatz dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) als zuständige Aufsichtsbehörde melden, sofern sie keinen betrieblichen Datenschutzbeauftragten bestellt haben. Der Inhalt der Meldung ergibt sich aus § 4e BDSG. Der TLfDI stellt auf seiner Website entsprechende Meldeformulare zur Verfügung:
(https://www.tlfdi.de/mam/tlfdi/datenschutz/video/tlfdi_meldeformular_v__.pdf).

„Bürgerinnen und Bürger sowie Unternehmen sollten dieser bußgeldbewehrten Meldepflicht rechtsbewusst nachkommen – für Fragen/Informationen stehe ich natürlich jederzeit zur Verfügung!“ – so Dr. Lutz Hasse.

Anlage 56

Pressemitteilung
vom 17. Oktober 2017

Trust – Wem kann ich trauen im Netz und warum?

Seit einigen Jahren setzt **FIfF**, das Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e. V. dafür ein, dass die Informationstechnik im Dienst einer lebenswerten Welt steht. Jährlich veranstaltet das FIfF eine Konferenz an wechselnden Orten zu aktuellen Themen des Komplexes Informatik und Gesellschaft. Bei der 17. Konferenz am 20. bis 22. Oktober in Jena ist auch der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit dabei. Herr Dr. Lutz Hasse hält einen Vortrag unter dem Titel „Vertrauen – Fortschritt – Kontrolle“, in dem er deutlich macht, welche Vertrauensdefizite in der heutigen IT-Landschaft bestehen und Möglichkeiten aufzeigt, diesem Defizit wirksam zu begegnen. „Ich halte das Anliegen des FIfF, die Öffentlichkeit vor schädlichen Entwicklungen zu warnen, eigene Lösungswege aufzuzeigen und sich gegen den Einsatz der Informationstechnik zur unverhältnismäßigen Kontrolle und Überwachung der Bürgerinnen und Bürger zur Wehr zu setzen, aus datenschutzrechtlicher Sicht für sehr wichtig und freue mich auf rege Diskussionen“, so der Landesbeauftragte. Nähere Informationen zu der Veranstaltung finden Sie unter http://www.fiff.de/veranstaltungen/fiffkon/fiffkon2017/.

Anlage 57

Pressemitteilung
vom 9. November 2017

Für Kleine kein Persönlichkeitsrecht –
In sozialen Netzwerken lassen Eltern die Hüllen der Kinder fallen!

Eltern haften in der Regel für ihre Kinder. Was ist aber, wenn Eltern selbst das Kindeswohl nicht immer im Blick haben? Dieser Eindruck entsteht mitunter, wenn man sich Fotos von mehr oder weniger unbekleideten Kindern ansieht, die (Groß-) Eltern ins Internet gestellt oder per WhatsApp verschickt haben.
Was im Augenblick für Eltern lustig oder liebenswert erscheint, kann für Eltern und insbesondere für ihre Kinder irgendwann einmal peinlich oder gar gefährlich werden, sodass man sich wünscht, die Bilder nie veröffentlicht zu haben. Etwa wenn diese Fotos auf Pädophilen-Foren landen.
Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit, Dr. Lutz Hasse, warnt davor, leichtsinnig Fotos von Kindern in sozialen Netzwerken zu veröffentlichen. So haben Facebooknutzer entsprechend der Nutzungsbedingungen von Facebook unter Pkt. 2 „Teilen Deiner Inhalte und Informationen“ zugestimmt, dass Facebook gebührenfrei und weltweit diese Fotos nutzen darf. Auch wenn man Fotos oder seinen Account löscht, sind entsprechend der Nutzungsbedingungen die Fotos weiterhin vorhanden, wenn sie mit anderen geteilt wurden und diese den Inhalt nicht gelöscht haben. Auch bei der Nutzung von WhatsApp kann ein Zugriff auf Fotos nicht ausgeschlossen werden, da die Speicherung in der Regel in dem normalen Bildordner des Smartphones erfolgt, auf den auch andere Apps Zugriff haben. Hier empfiehlt der TLfDI die von WhatsApp eingerichtete Option zu nutzen, eine Speicherung zu unterbinden. Dies gelingt indes nur beim Empfänger. Hilfe dafür finden Sie bei WhatsApp unter FAQ.
Fotos per *klassischer Mail* verschlüsselt zu versenden, minimiert das Risiko zwar, aber letztendlich wird – leider – nur ein Foto *per Post* dem Datenschutz gerecht werden können.
Da es also keine 100 prozentige digitale Sicherheit gibt: **Seien Sie, liebe Eltern, wachsam, welche Fotos Ihrer Kinder Sie in die – undichte – digitale Wolke laden.**

Eltern, die Rat benötigen, können sich jederzeit an den TLfDI wenden.

Anlage 58

Pressemitteilung
vom 20. November 2017

TLfDI warnt: Diese Kinder-Uhren ticken anders!
- Appell an Eltern: Vernichten Sie smart getarnte Abhöranlagen -

Bereits im Februar 2017 warnte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit vor der Spielzeugpuppe „Cayla“, die einen Bluetooth-Sender in sich trug und Gesprächsinhalte an die Server des amerikanischen Konzerns „Nuance Communications“ sendete. Die Bundesnetzagentur hatte damals Eltern dazu aufgerufen, die Puppe zu vernichten, da der Besitz von getarnten Abhöranlagen strafbar sei.
Nun hat die Bundesnetzagentur ein weiteres Gerät verboten. Man mag es kaum glauben: Es ist eine Smart-Uhr, konzipiert für Kinder im Alter von 5 bis 12 Jahren. „Smart“: Mittels einer App können Eltern solche Kinderuhren nutzen, um unbemerkt das Kind und seine Umgebung abzuhören. Aus Sicht der Eltern vielleicht toll, kann sie doch unbemerkt als „Babyphone“ genutzt werden. Auch z. B. in Schulen, sodass der Unterricht abgehört wird.
Der TLfDI, Dr. Lutz Hasse, weist auf § 90 Telekommunikationsgesetz hin; danach ist es u. a. **verboten**, Sendeanlagen oder sonstige Telekommunikationsanlagen zu **besitzen**, die ihrer Form nach einen **anderen Gegenstand vortäuschen** und dazu bestimmt sind, **das nicht öffentlich gesprochene Wort eines anderen von diesem unbemerkt abzuhören**.
Dr. Lutz Hasse: „Mittels App funktionieren diese mit SIM-Karte ausgestatteten Kinderuhren ähnlich wie Telefone, allerdings mit dem folgenden Unterschied: Die Eltern können bestimmen, dass die Uhr – vom Kind unbemerkt – ihre Telefonnummer anruft; dadurch können sie dann die Umgebung des Kindes abhören. § 90 Telekommunikationsgesetz bezweckt den Schutz der Privatsphäre, auch von Kindern. Eltern sollten in sich gehen und überlegen, ob Fürsorge eine solche Rundumüberwachung ihres Kindes rechtfertigt, zumal Dritte hiervon betroffen sind.“

Anlage 59

Pressemitteilung
vom 24. November 2017

Microsoft trifft TLfDI
-Wirtschaft und Datenschutzaufsicht – geht das zusammen?-

Der TLfDI, Dr. Lutz Hasse, ist Bundesvorsitzender des Arbeitskreises Datenschutz und Bildung aller Landesdatenschutzbeauftragten. In diesem Kreis werden derzeit bundesweite Lösungen etwa für Fragen erarbeitet, die sich im Zusammenhang mit Medienkompetenz von Lehrern und Schülern, aber auch mit Lernplattformen und digitalen „Schul-Büchern“ aufdrängen. Einer der großen Akteure in diesem Segment ist Microsoft, z. B. als bedeutender Cloud-Anbieter. In einem von der Wirtschaft und Politik aufmerksam beobachteten Prozess gehen der Global Player und die Datenschutzaufsichtsbehörden in Erfurt aufeinander zu, um gemeinsam datenschutzkonforme Lösungen zu finden.

Dr. Lutz Hasse: „Wir praktizieren ein neues Modell des Umgangs. Wir agieren nicht als Gegenspieler, sondern richten gemeinsam Wirtschaftsinteressen am Datenschutzrecht aus. Ohne gegenseitiges Vertrauen ist das nicht möglich – Microsoft ist hier zukunftsweisende Schritte gegangen, die Nachahmung finden sollten. Win-win für alle Beteiligten!“

Anlage 60

Pressemitteilung
vom 27. November 2017

Immelborn – AdActa

Seit kurzem liegt er vor: der **Zwischenbericht** des Untersuchungsausschusses 6/2 „Aktenlager Immelborn“ (Drucksache 6/4641). Beim Versuch, den Wertungsteil des Zwischenberichts zu verhindern, scheiterte die CDU-Fraktion vor dem Thüringer Verfassungsgerichtshof. Die Hauptfrage der Untersuchung lautete, ob der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) das damalige Thüringer Innenministerium (TIM) auf Amtshilfe zur Beräumung des Aktendepots verklagt habe, um dem damaligen Innenminister Geibert zu schaden. Das **Fazit** des **Zwischenberichtes** lautet: „Der dem Auftrag des Untersuchungsausschusses zugrunde liegende **Verdacht**, der TLfDI habe die Klage erhoben, um im damals anstehenden Wahlkampf dem politischen Konkurrenten in Gestalt des von ihm geführten TIM schaden zu wollen, konnte durch die die bisherige Beweisaufnahme **nicht erhärtet** werden.“
Ferner förderte der Zwischenbericht auch **andere wichtige Tatsachen und Feststellungen** ans Licht:
1. Die Zustellung der Bescheide des TLfDI durch **öffentliche Bekanntmachung** war **rechtmäßig** und erfolgte an den **richtigen Adressaten**.
2. Die getroffenen Maßnahmen des TLfDI waren **verhältnismäßig**.
3. Die **Ersatzvornahme** durch den TLfDI wird von der **Fachliteratur gestützt**.
4. Die **Polizei wollte** dem TLfDI **helfen**, wurde durch **Einwirkung der Hausleitung des TIM indes daran gehindert**.
5. Die Hausleitung des TIM **ließ gezielt Ablehnungsgründe gegen das Amtshilfegesuch generieren**, etwa: statt der vom TLfDI geforderten 10 Mann für 10 Tage, ließ die Hausleitung des TIM bei der Polizei anfragen, ob denn **100 Mann für 30 Tage** leistbar wären, **um dort eine ablehnende Haltung hervorzurufen**.
6. Das **TIM verweigerte dem TLfDI einen konstruktiven Dialog** völlig.
7. Das **Amtshilfeersuchen des TLfDI war zulässig und begründet**.

8. Der TLfDI durfte **nicht auf Private verwiesen** werden und die **Erfüllung polizeilicher Aufgaben** wäre durch die Amtshilfe **nicht gefährdet** gewesen.
9. Die **Bestellung des Nachtragsliquidators erfolgte zügig und rechtskonform**.
10. Für die **Beräumung des Aktenlagers entstanden dem Freistaat keine Kosten**.

Anlage 61

Kurzpapier Nr. 1
Verzeichnis von Verarbeitungstätigkeiten –Art. 30 DS-GVO

Dieses Kurzpapier der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz –DSK) dient als erste Orientierung insbesondere für den nicht-öffentlichen Bereich, wie nach Auffassung der DSK die Datenschutz-Grundverordnung (DS-GVO) im praktischen Vollzug angewendet werden sollte. Diese Auffassung steht unter dem Vorbehalt einer zukünftigen – möglicherweise abweichenden – Auslegung des Europäischen Datenschutzausschusses.

Altes Recht = neues Recht?
Das aus dem BDSG bekannte Verfahrensverzeichnis (§ 4g Abs. 2 und 2a BDSG; dort „Übersicht" genannt) wird mit der DS-GVO abgelöst durch ein (schriftliches oder elektronisches) Verzeichnis aller Verarbeitungstätigkeiten mit personenbezogenen Daten. Dieses Verzeichnis betrifft sämtliche – auch teilweise – automatisierte Verarbeitungen sowie nichtautomatisierte Verarbeitungen personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Grundsätzlich ist jeder Verantwortliche (z. B. Unternehmen, Freiberufler, Verein) und – neu – auch jeder Auftragsverarbeiter zur Erstellung und Führung eines solchen Verzeichnisses verpflichtet. Es wird in der Praxis wegen der Unterschiede bei den eingesetzten Verfahren notwendigerweise oft aus einer Reihe von Einzelbeiträgen bestehen müssen. Das Verfahrensverzeichnis wird somit die Summe der einzelnen Verfahrensbeschreibungen sein.

Stellen mit weniger als 250 Mitarbeitern
Unternehmen und Einrichtungen mit weniger als 250 Mitarbeitern müssen kein Verzeichnis von Verarbeitungstätigkeiten führen, es sei denn, der Verantwortliche bzw. Auftragsverarbeiter führt Verarbeitungen personenbezogener Daten durch,

- die ein Risiko für die Rechte und Freiheiten der betroffenen Personen bergen (dazu gehören regelmäßig Fälle von Scoring und Überwachungsmaßnahmen) oder
- die nicht nur gelegentlich erfolgen (z. B. die regelmäßige Verarbeitung von Kunden- oder Beschäftigtendaten) oder

- die besondere Datenkategorien gemäß Art. 9 Abs. 1 DS-GVO (Religionsdaten, Gesundheitsdaten, usw.) oder strafrechtliche Verurteilungen und Straftaten im Sinne des Art. 10 DS-GVO betreffen.

Die Pflicht zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten besteht also bereits dann, wenn mindestens eine der genannten Fallgruppen erfüllt ist. Da es anders als in Art. 35 DS-GVO (Datenschutz-Folgenabschätzung) nicht darauf ankommt, dass es sich voraussichtlich um ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen handelt, sondern jedes Risiko für die Rechte und Freiheiten bezüglich der Verarbeitung zu betrachten ist, wird vielfach das Erstellen eines Verzeichnisses von Verarbeitungstätigkeiten geboten sein.

Kein öffentliches Verzeichnis und keine Meldepflicht mehr

Anders als im bisherigen BDSG ist eine Möglichkeit für jedermann, in das Verzeichnis von Verarbeitungstätigkeiten Einsicht zu nehmen, nach der DS-GVO nicht vorgesehen. Ebenso entfallen mit der DS-GVO die bisher in § 4d und § 4e BDSG geregelten Meldepflichten von manchen Unternehmen an die Aufsichtsbehörde. Erstellt und vorgehalten werden müssen die Verzeichnisse dennoch, da sie den Aufsichtsbehörden jederzeit auf Anfrage zur Verfügung zu stellen sind (siehe Art. 30 Abs. 4 DS-GVO und ErwGr. 82).

Inhalt des Verzeichnisses für Verantwortliche (Art. 30 Abs. 1 DS-GVO)

Das Verzeichnis der Verantwortlichen muss nach Art. 30 Abs. 1 DS-GVO wesentliche Angaben zur Verarbeitung beinhalten wie z. B. die Zwecke der Verarbeitung und eine Beschreibung der Kategorien der personenbezogenen Daten, der betroffenen Personen und der Empfänger. Verantwortliche Stellen, die bereits jetzt über ein strukturiertes Verfahrensverzeichnis oder eine strukturierte Datenschutzdokumentation zu den Verfahren verfügen, sollten mit den geforderten Pflichtangaben des neuen Artikels aus der DS-GVO keine Probleme haben.

Inhalt des Verzeichnisses für Auftragsverarbeiter (Art. 30 Abs. 2 DS-GVO)

Ein Verzeichnis beim Auftragsverarbeiter zu allen Kategorien der von ihm im Auftrag eines Verantwortlichen durchgeführten Tätig-

keiten der Verarbeitung war vom BDSG bislang nicht vorgeschrieben. Nach Art. 30 Abs. 2 DS-GVO ist ein solches Verzeichnis jedoch künftig zu erstellen. Auch hier sind die Pflichtangaben überschaubar, so dass der Aufwand, dieses Verzeichnis zu erstellen, als eher gering einzustufen sein wird.

Beschreibung technischer und organisatorischer Maßnahmen
Art. 30 Abs. 1 Buchstabe g und Art. 30 Abs. 2 Buchstabe d DS-GVO geben vor, dass das Verzeichnis, wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1 DS-GVO enthalten soll. Wie detailliert diese Beschreibung sein muss, lässt sich der DS-GVO nicht unmittelbar entnehmen. Jedenfalls sollte die Beschreibung der Maßnahmen nach Art. 32 DS-GVO so konkret erfolgen, dass die Aufsichtsbehörden eine erste Rechtmäßigkeitsüberprüfung vornehmen können.

Rechtsfolgen bei Verstoß
Verstöße durch eine fehlende oder nicht vollständige Führung eines Verzeichnisses oder das Nichtvorlegen des Verzeichnisses nach Aufforderung durch die Aufsichtsbehörde können nach Art. 83 Abs. 4 Buchstabe a DS-GVO mit einer Geldbuße sanktioniert werden.

Das Verzeichnis als Teil der Rechenschaftspflicht
Mit der Erstellung des Verzeichnisses der Verarbeitungstätigkeiten sind keinesfalls alle von der DS-GVO geforderten Dokumentationspflichten erfüllt. Das Verzeichnis ist nur ein Baustein, um der in Art. 5 Abs. 2 normierten Rechenschaftspflicht zu genügen. So müssen beispielsweise auch das Vorhandensein von Einwilligungen (Art. 7 Abs. 1), die Ordnungsmäßigkeit der gesamten Verarbeitung (Art. 24 Abs. 1) und das Ergebnis von Datenschutz-Folgenabschätzungen (Art. 35 Abs. 7) durch entsprechende Dokumentationen nachgewiesen werden.

Ausblick: Wesentliche Rolle des Verzeichnisses und Muster-Vorlage der Datenschutzaufsichtsbehörden
Das Verzeichnis von Verarbeitungstätigkeiten nach der DS-GVO wird wie die bisherigen internen Verfahrensverzeichnisse eine wesentliche Rolle spielen, um datenschutzrechtliche Vorgaben über-

haupt einhalten zu können. Nur wer die eigenen Verarbeitungsprozesse kennt, kann gezielt Maßnahmen ergreifen, um eine rechtmäßige Verarbeitung personenbezogener Daten sicherstellen zu können. Die deutschen Aufsichtsbehörden werden im Jahr 2017 eine Muster-Vorlage sowie weitere Hinweise für ein Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 DS-GVO bereitstellen.

Unsere Empfehlung
Es ist ratsam, rechtzeitig im eigenen Interesse ein vollständiges Verzeichnis von Verarbeitungstätigkeiten zu erstellen. Das Verzeichnis von Verarbeitungstätigkeiten dient als wesentliche Grundlage für eine strukturierte Datenschutzdokumentation und hilft dem Verantwortlichen dabei, gemäß Art. 5 Abs. 2 DS-GVO nachzuweisen, dass die Vorgaben aus der DS-GVO eingehalten werden (Rechenschaftspflicht). Die Übergangszeit bis zur Geltung der DS-GVO am 25. Mai 2018 sollte dazu genutzt werden, die bereits bestehende Verfahrensdokumentation an die neu-en Anforderungen anzupassen.

Anlage 62

Kurzpapier Nr. 2
Aufsichtsbefugnisse/Sanktionen

Dieses Kurzpapier der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz –DSK) dient als erste Orientierung insbesondere für den nicht-öffentlichen Bereich, wie nach Auffassung der DSK die Datenschutz-Grundverordnung (DS-GVO) im praktischen Vollzug angewendet werden sollte. Diese Auffassung steht unter dem Vorbehalt einer zukünftigen – möglicherweise abweichenden – Auslegung des Europäischen Datenschutzausschusses.

Die DS-GVO stellt den Aufsichtsbehörden einen umfassenden Katalog von Untersuchungs-und Abhilfebefugnissen zur Verfügung, um die Einhaltung datenschutzrechtlicher Bestimmungen durchzusetzen. Neben diesen verwaltungsrechtlichen Maßnahmen können Verstöße auch mit hohen Geldbußen sanktioniert werden.

Untersuchungs- und Abhilfebefugnisse im Verwaltungsverfahren (Art. 58 -GVO)

Gegenüber Verantwortlichen und Auftragsverarbeitern können vorsorgliche Warnungen ausgesprochen werden, wenn diese Datenverarbeitungen beabsichtigen, die voraussichtlich einen Verstoß gegen die Grundverordnung darstellen, bzw. Verwarnungen, wenn mit Datenverarbeitungen bereits gegen die Grundverordnung verstoßen wurde. Darüber hinaus können Verantwortliche und Auftragsverarbeiter künftig im Rahmen eines förmlichen Verwaltungsaktes von den Aufsichtsbehörden angewiesen werden, Betroffenenrechten zu entsprechen, Datenverarbeitungen mit der Grundverordnung in Einklang zu bringen sowie von einem Datenschutzverstoß betroffene Personen entsprechend zu benachrichtigen. Des Weiteren ist künftig auch die Anordnung der Aussetzung der Übermittlung von Daten an einen Empfänger in einem Drittland oder an eine internationale Organisation möglich. Die Befugnis der Aufsichtsbehörden, Beschränkungen und Verbote von Datenverarbeitungen und die Berichtigung oder Löschung bestimmter Daten sowie eine Einschränkung der Verarbeitung solcher Daten anzuordnen, bleibt unbe-

rührt. Nicht zuletzt können mit Inkrafttreten der Grundverordnung Zertifizierungen seitens der Aufsichtsbehörden selbst widerrufen oder Zertifizierungsstellen angewiesen werden, erteilte Zertifizierungen zu widerrufen oder neue Zertifizierungen nicht zu erteilen. Zusätzlich zu oder anstelle all dieser Maßnahmen können Verstöße gegen die Grundverordnung mit Geldbußen geahndet werden. Zu beachten ist, dass sich die genannten behördlichen Maßnahmen zukünftig nicht nur gegen den Verantwortlichen selbst, sondern auch gegen Auftragsverarbeiter richten können. Die Aufsichtsbehörden haben umfassende Untersuchungsbefugnisse, wobei den Verantwortlichen und auch Auftragsverarbeiter Mitwirkungspflichten treffen. Insbesondere können die Aufsichtsbehörden den Verantwortlichen und Auftragsverarbeiter sowie deren Vertreter anweisen, alle Informationen bereitzustellen, die für die Erfüllung der Aufgaben der Aufsichtsbehörde erforderlich sind. Alle Anordnungen können mit Zwangsmitteln, wie Zwangsgeldern, durchgesetzt werden. Rechtsschutz bei Zweifeln an der Rechtmäßigkeit der Anordnungen der Aufsichtsbehörde ist wie bisher auch im verwaltungsgerichtlichen Verfahren gewahrt.

Verhängung von Geldbußen (Art. 83 DS-GVO)

Zusätzlich zu oder anstelle all dieser Maßnahmen können Verstöße gegen die Grundverordnung mit Geldbußen geahndet werden. Der Rahmen für die Geldbußen wird mit der DS-GVO deutlich erhöht. Dies trägt der gestiegenen Bedeutung des Datenschutzes Rechnung. So können Geldbußen von bis zu 10.000.000 € bzw. bei Unternehmen bis zu 2% des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres verhängt werden (z. B. ist eine weitere erwähnenswerte Neuerung gegenüber der aktuellen Rechtslage, dass unter dem Regime der DS-GVO auch ein Verstoß gegen die Pflicht zur Ergreifung geeigneter und angemessener technischer und organisatorischer Maßnahmen zum Schutz personenbezogener Daten mit einer Geldbuße geahndet werden kann). Bei bestimmten, besonders schwerwiegenden Verstößen, darunter Verstöße gegen die Datenverarbeitungsgrundsätze und gegen die Betroffenenrechte oder im Falle einer Verarbeitung ohne Rechtsgrundlage, sind Geldbußen von bis zu 20.000.000 € möglich. Gegen Unternehmen kann diese Grenze sogar noch überschritten werden, nämlich bis zu 4% des weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres.

Für den Fall der Nichtbefolgung einer Anweisung der Aufsichtsbehörde nach Art. 58 Abs. 2 DS-GVO ist ebenfalls die Verhängung einer Geldbuße von bis zu 20.000.000 € oder im Fall eines Unternehmens von bis zu 4% seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres vorgesehen. In allen drei Fallgestaltungen richtet sich die maximale Obergrenze für die Geldbuße danach, welcher der Beträge höher ist.
Hierbei geht die DS-GVO von einem gegenüber Art. 4 Nr. 18 DS-GVO erweiterten Unternehmensbegriff aus. Wie der Begriff „Unternehmen“ im Zusammenhang mit dem Bußgeldverfahren zu verstehen ist, ist Erwägungsgrund (ErwGr.) 150 der DS-GVO zu entnehmen. Danach gilt der aus dem Kartellrecht entlehnte weite, funktionale Unternehmensbegriff nach Art. 101 und 102 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV). Dies hat zur Folge, dass Mutter- und Tochtergesellschaften als wirtschaftliche Einheit betrachtet werden, so dass bei der Bemessung des Bußgeldes der Gesamtumsatz der Unternehmensgruppe zu Grunde gelegt wird. Nach dem Wortlaut der DS-GVO reicht es für die Zurechnung eines Verstoßes zu einem Unternehmen aus, dass ein Beschäftigter des Unternehmens oder auch ein für das Unternehmen agierender externer Beauftragter gehandelt hat. Die Zurechnung ist damit nicht mehr wie bisher (vgl. § 30 OWiG) auf Handlungen gesetzlicher Vertreter oder anderer Leitungspersonen des Unternehmens begrenzt. Für die Zumessung der Geldbußen gilt zuvörderst der Grundsatz, dass die Geldbußen wirksam, verhältnismäßig und abschreckend sein müssen. Art. 83 Abs. 2 S. 2 DS-GVO enthält eine Auflistung von Kriterien, die bei der Entscheidung über die Verhängung und die Höhe einer Geldbuße (ggf. auch einem Absehen davon, vgl. ErwGr. 148) gebührend im Einzelfall berücksichtigt werden sollen. Neben Art, Schwere und Dauer des Verstoßes ist unter anderem auch zu berücksichtigen, welche Art von Daten verarbeitet wurde sowie ob früher angeordnete Maßnahmen vom Verantwortlichen eingehalten wurden. Zu berücksichtigen ist künftig auch die Art und Weise, wie der Verstoß der Aufsichtsbehörde bekannt wurde, insbesondere, ob und wie die Verantwortlichen mit den Aufsichtsbehörden zusammen gearbeitet haben, um Verstößen abzuhelfen und ihre möglichen nachteiligen Auswirkungen zu mindern, und ob sie die Verstöße eigenständig mitgeteilt haben. Ferner ist auch der Grad der Verantwortung des Verantwortlichen bzw. Auftragsverarbeiters unter Berücksichtigung der von ihm getroffenen technischen und organisatorischen Maß-

nahmen ein zu berücksichtigendes Kriterium. Mithin wird im Einzelfall zu überprüfen sein, inwieweit ein Unternehmen im Rahmen seiner internen Organisation, etwa durch Ausgestaltung seiner Strukturen, Arbeitsprozesse und Kontrollmechanismen, Vorkehrungen getroffen hat, die dazu dienen, die Einhaltung der datenschutzrechtlichen Anforderungen sicherzustellen, bzw. inwieweit die interne Organisation diesbezüglich Mängel aufweist. Zudem können jegliche anderen erschwerenden oder mildernden Umstände im jeweiligen Fall, wie unmittelbar oder mittelbar durch den Verstoß erlangte finanzielle Vorteile oder vermiedene Verluste, Berücksichtigung finden. Abzuwarten bleibt, in welcher Form der Europäische Datenschutzausschuss seinen Auftrag aus Art. 70 Abs. 1 Buchstabe k DS-GVO umsetzen wird. Danach obliegt ihm die Aufgabe, Leitlinien für die Aufsichtsbehörden in Bezug auf die Anwendung von Maßnahmen nach Art. 58 Abs. 1, 2 und 3 DS-GVO und die Festsetzung von Geldbußen gemäß Art. 83 DS-GVO zu erlassen.

Anlage 63

Kurzpapier Nr. 3
Verarbeitung personenbezogener Daten für Werbung

Dieses Kurzpapier der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) dient als erste Orientierung insbesondere für den nicht-öffentlichen Bereich, wie nach Auffassung der DSK die Datenschutz-Grundverordnung (DS-GVO) im praktischen Vollzug angewendet werden sollte. Diese Auffassung steht unter dem Vorbehalt einer zukünftigen – möglicherweise abweichenden – Auslegung des Europäischen Datenschutzausschusses.

Keine Detailregelung für Werbung
Mit der DS-GVO fallen alle detaillierten Regelungen des Bundesdatenschutzgesetzes (BDSG) zur Verarbeitung personenbezogener Daten für werbliche Zwecke weg.

Werbung nach Interessenabwägung
Grundlage für die Beurteilung der Zulässigkeit von Werbung ist in Zukunft, abgesehen von einer Einwilligung, eine Interessenabwägung nach Art. 6 Abs. 1 Buchstabe f DS-GVO. Ausgangspunkt für die zu treffende Abwägungsentscheidung ist Erwägungsgrund (ErwGr.) 47 DS-GVO, der u. a. ausführt: „Die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung kann als eine einem berechtigten Interesse dienende Verarbeitung betrachtet werden.“ Ferner gibt ErwGr. 47 DS-GVO im Rahmen der durchzuführenden Interessenabwägung vor, die „vernünftigen Erwartungen der betroffenen Person“, die auf ihrer Beziehung zu dem Verantwortlichen beruhen, in den Abwägungsprozess einzubeziehen. Wann diese Voraussetzungen vorliegen, ist derzeit noch nicht abschließend geklärt. Dem Working Paper der Art. 29 Datenschutzgruppe (WP 217, S. 51), das sich allerdings auf die Datenschutzrichtlinie 95/46/EG bezieht, können insoweit erste Interpretationshinweise entnommen werden. Die vernünftigen Erwartungen der betroffenen Person werden bei Maßnahmen zur werblichen Ansprache maßgebend durch die Informationen nach Art. 13, 14 DS-GVO zu den Zwecken der Datenverarbeitung bestimmt werden. Informiert der Verantwortliche transparent und umfassend über eine vorgesehene werbliche Nut-

zung der Daten, geht die Erwartung der betroffenen Person in aller Regel auch dahin, dass ihre Kundendaten entsprechend genutzt werden. Insoweit ist im Rahmen der Interessenabwägung zu berücksichtigen, dass die von Werbung betroffenen Personen ein jederzeitiges und umfassendes Widerspruchsrecht haben (Art. 21 Abs. 2 DS-GV0), auf das sie ausdrücklich hinzuweisen sind (Art. 21 Abs. 4 DS-GVO). Der Werbewiderspruch hat nach Art. 21 Abs. 3 DS-GVO zur Folge, dass personenbezogene Daten für Werbezwecke nicht mehr verarbeitet, insbes. verwendet werden dürfen. Im Übrigen ist zu berücksichtigen, ob die betroffene Person bereits Kunde des Verantwortlichen ist oder dessen Dienste nutzt (ErwGr. 47 DS-GVO). Ferner sind bei der Inte-ressenabwägung auch die allgemeinen Grundsätze aus Art. 5 Abs. 1 DS-GVO zu berücksichtigen, also insbesondere:

- faire Verfahrensweise
- dem Verarbeitungszweck angemessen
- in einer für die betroffene Person nachvollziehbaren Weise (insbesondere Nennung der Quelle der Daten)

Diese Grundsätze sprechen jedenfalls dagegen, Profile zur werblichen Ansprache (Werbescores) zu erstellen, die z. B. Informationen aus sozialen Netzwerken berücksichtigen. Eingriffsintensivere Maßnahmen wie Profilbildung sprechen eher dafür, dass ein Interesse der betroffenen Person am Ausschluss der Datenverarbeitung überwiegt. Unabhängig von der Interessenabwägung müssen die Informationspflichten nach den Art. 13, 14 DS-GVO eingehalten werden.

Ohne Einwilligung keine werbliche Nutzung besonderer Datenkategorien

Art. 9 DS-GVO enthält keine Erlaubnisnorm für die Verarbeitung besonderer Kategorien personenbezogener Daten für Zwecke der Werbung. Dies ist nur bei Vorliegen einer ausdrücklichen Einwilligung der betroffenen Person zulässig. Von Relevanz ist dies z. B. für Unternehmen und Berufe des Gesundheitswesens (Apotheken, Sanitätshäuser, Optiker, Orthopäden usw.).

Besondere Grenzen aus § 7 UWG

Auch nach neuem Recht wird die Interessenabwägung bei der Nutzung der Kontaktdaten von Verbrauchern für Telefon- und Faxwerbung dazu führen, dass diese weiterhin nur mit einer vorherigen ausdrücklichen Einwilligung erlaubt ist. Alles andere wäre im Hin-

blick auf die klaren Regelungen in § 7 des Gesetzes gegen den unlauteren Wettbewerb (UWG) mit den vernünftigen Erwartungen der Betroffenen (ErwGr. 47 DS-GVO) nicht zu vereinbaren. Ebenso ist eine Kontaktdatennutzung für E-Mail-und SMS-Werbung außerhalb einer Einwilligung nur im Fall der Eigenwerbung bei Bestandskunden unter den Maßgaben von § 7 Abs. 3 UWG zulässig. Im Übrigen bleibt abzuwarten, inwieweit die geplante neue ePrivacy-Verordnung im Bereich der elektronischen Werbung konkrete Regelungen (z. B. ausschließliche Opt-in-Lösung) für werbliche Ansprachen enthalten wird.

Fortgeltung von Einwilligungen

Bisher erteilte Einwilligungen wirken nach Erwägungsgrund 171 der DS-GVO fort, sofern sie der Art nach den Bedingungen der Datenschutz-Grundverordnung entsprechen. Die im Wirtschafts-leben EU-weit vorhandenen Einwilligungen sind auf ihre Wirksamkeit hin zu überprüfen. Dabei ist u. a. von Bedeutung, ob auf Grundlage der neuen Anforderungen nach Art. 7 Abs. 4 der DS-GVO eine freiwillige Erklärung abgegeben und dass die Altersgrenze für die Einwilligungsfähigkeit bei Inanspruchnahme von Diensten der Informationsgesellschaft nach Art. 8 Abs. 1 der DS-GVO berücksichtigt wurde.

„Koppelungsverbot“ bei Einwilligungen für Werbung

Das bisher schon bestehende Koppelungsverbot für Werbung findet sich auch in der DS-GVO wieder, ist aber nicht mehr davon abhängig, ob ein anderer Zugang zu gleichwertigen vertraglichen Leistungen möglich ist. Bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, ist dem Umstand in größtmöglichem Umfang Rechnung zu tragen, ob unter anderem die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrages nicht erforderlich ist (Art. 7 Abs. 4 DS-GVO). Bei „kostenlosen“ Dienstleistungsangeboten, die die Nutzer mit der Zustimmung für eine werbliche Nutzung ihrer Daten „bezahlen“ (z. B. kostenloser E-Mail-Account gegen Zustimmung für Newsletter-Zusendung als „Gegenfinanzierung“), muss diese vertraglich ausbedungene Gegenleistung des Nutzers bei Vertragsabschluss klar und verständlich dargestellt werden. Nur dann besteht keine Notwendigkeit mehr für eine Einwilligung.

Ausblick für den künftigen Umgang mit personenbezogenen Daten für Werbung

Soweit Werbung nicht auf einer wirksamen Einwilligung der betroffenen Person beruht, wird für die Zulässigkeit von Werbung in Zukunft fast ausschließlich die nach Art. 6 Abs. 1 Buchstabe f DS-GVO vorgeschriebene Interessenabwägung maßgeblich sein. Inwieweit es in Europa gelingen wird, die in Deutschland entwickelten Maßstäbe auch unter Geltung der DS-GVO aufrechtzuerhalten, wird sich zeigen. Anzustreben sind für diesen Bereich möglichst EU-weite Verhaltensregeln. Sollte das nicht für die wesentlichen Bereiche der Werbung gelingen, wird mit Leitlinien des Europäischen Datenschutzausschusses auch zu diesem Thema zu rechnen sein.

Anlage 64

Kurzpapier Nr. 4
Datenübermittlung in Drittländer

Dieses Kurzpapier der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) dient als erste Orientierung insbesondere für den nicht-öffentlichen Bereich, wie nach Auffassung der DSK die Datenschutz-Grundverordnung (DS-GVO) im praktischen Vollzug angewendet werden sollte. Diese Auffassung steht unter dem Vorbehalt einer zukünftigen – möglicherweise abweichenden – Auslegung des Europäischen Datenschutzausschusses.

Die DS-GVO sieht für die Übermittlung personenbezogener Daten in ein Land außerhalb der EU/des EWR besondere Regelungen vor: Art. 44 – 49. Länder außerhalb der EU/des EWR werden in der DS-GVO als „Drittländer" bezeichnet, in der Praxis wird auch der Begriff „Drittstaat" verwendet. Bei der Datenübermittlung in ein Drittland muss zunächst überprüft werden, ob unabhängig von den in den Art. 45 ff. geregelten spezifischen Anforderungen an Datenübermittlungen in Drittländer auch alle übrigen Anforderungen der DS-GVO (z. B. Art. 9 Abs. 3) an die in Rede stehende Datenverarbeitung eingehalten werden (1. Stufe). Steht nach diesem Prüfungsschritt einer Verarbeitung nichts entgegen, müssen gemäß Art. 44 zusätzlich die spezifischen Anforderungen der Art. 45 ff. an die Übermittlung in Drittländer beachtet werden (2. Stufe; „2-Stufen-Prüfung"). Dies gilt auch bei einer Weiterübermittlung der personenbezogenen Daten durch die empfangende Stelle im Drittland (Art. 44 S. 1 2. HS (siehe auch Erwägungsgrund (ErwGr.) 101)). Die DS-GVO sieht für Datentransfers in Drittländer folgende Möglichkeiten vor (für öffentliche Stellen gelten im Einzelfall ergänzende Regelungen):

- **Feststellung der Angemessenheit des Datenschutzniveaus im Drittland durch die EU-Kommission (Art. 45 DS-GVO)**
- **Vorliegen geeigneter Garantien (Art. 46 DS-GVO) oder**
- **Ausnahmen für bestimmte Fälle (Art. 49 DS-GVO).**

1. Feststellung der Angemessenheit des Datenschutzniveaus im Drittstaat durch die Kommission (Art. 45 DS-GVO)

Die Kommission hat die Möglichkeit, nach entsprechender Prüfung das Bestehen eines angemessenen Schutzniveaus in einem bestimmten Drittland festzustellen. Die Feststellung kann auch auf ein bestimmtes Gebiet oder einen bestimmten Sektor in dem Drittland oder auch auf bestimmte Datenkategorien beschränkt sein. Ein angemessenes Schutzniveau besteht dann, wenn in dem Drittland auf Grundlage seiner innerstaatlichen Rechtsvorschriften und deren Anwendung, der Existenz und der wirksamen Funktionsweise einer oder mehrerer unabhängiger Aufsichtsbehörden sowie seiner eingegangenen internationalen Verpflichtungen ein Schutzniveau existiert, welches dem in der DS-GVO gewährten Schutzniveau gleichwertig ist. Eine Datenübermittlung auf Grundlage eines solchen Angemessenheitsbeschlusses bedarf keiner weiteren Genehmigung durch die für den Verantwortlichen oder Auftragsverarbeiter zuständige nationale Aufsichtsbehörde. Die DS-GVO sieht eine Fortgeltung der bereits erlassenen Angemessenheitsbeschlüsse vor (Art. 46 Abs. 5 S. 2). Für den EU-US Privacy Shield hat die Kommission die Angemessenheit des Datenschutzniveaus festgestellt (C(2016) 4176 final)).

2. Vorliegen geeigneter Garantien (Art. 46 DS-GVO)

Eine Datenübermittlung in ein Drittland ist weiter zulässig, wenn der Verantwortliche oder Auftragsverarbeiter geeignete Garantien zur Gewähr-leistung eines angemessenen Schutzniveaus vorgesehen hat. Folgende Garantien kommen in Betracht:

a) Verbindliche interne Datenschutzvorschriften (Binding Corporate Rules) (Art. 46 Abs. 2 Buchstabe b, Art. 47)

Verbindliche interne Datenschutzvorschriften (BCR) wurden schon bisher in der Praxis verwendet und sind nun in der DS-GVO (anders als in der noch geltenden EU-Datenschutzrichtlinie 95/46/EG) ausdrücklich als Möglichkeit zur Erbringung „geeigneter Garantien“ für Datenübermittlungen in Drittländer geregelt. Sie können vor allem bei international tätigen Konzernen mit internem Datenfluss (auch) in Drittländer empfehlenswert sein. Dabei legt das Unternehmen Regelungen für den Umgang mit personenbezogenen Daten auch in Drittländern fest. Die BCR müssen einen Schutz bieten, der im Wesentlichen der DS-GVO entspricht. Der Mindest-Inhalt ist in Art. 47 Abs. 2 festgelegt. Zudem müssen die BCR für alle betreffenden Mitglieder der Unternehmensgruppe rechtlich bindend sein und den betroffenen Personen durchsetzbare Rechte gewähren (Art. 47 Abs. 1

Buchstabe a und b). Die Genehmigung der BCR erfolgt gemäß dem Kohärenzverfahren durch die zuständige Aufsichtsbehörde (Art. 47 Abs. 1). Die konkreten Datenübermittlungen auf Grundlage der BCR werden dann nicht mehr einzeln genehmigt.

b) Standarddatenschutzklauseln der Kommission oder einer Aufsichtsbehörde (Art. 46 Abs. 2 Buchstabe c und d)

Schließen der Datenexporteur und der Datenimporteur einen Vertrag unter Verwendung der Standarddatenschutzklauseln der Kommission, ist der darauf basierende Datentransfer ohne weitere Genehmigung durch die Aufsichtsbehörde zulässig (vorbehaltlich der weiteren Anforderungen nach der DS-GVO). Auch den Aufsichtsbehörden ist es möglich, eigene Standarddatenschutzklauseln zu entwerfen. Diese bedürfen der Abstimmung im Kohärenzverfahren und sind anschließend von der Kommission förmlich zu genehmigen.

Die bereits bestehenden EU-Standardvertrags-klauseln gelten gemäß Art. 46 Abs. 5 S. 2 ausdrücklich fort. Sofern die Standarddatenschutzklauseln in unveränderter Form verwendet werden, sind die Datenübermittlungen genehmigungsfrei. Dies gilt auch noch dann, wenn ihnen weitere Klauseln oder zusätzliche Garantien hinzugefügt werden, solange diese weder mittelbar noch unmittelbar im Widerspruch zu den Standarddatenschutzklauseln stehen und die Grundrechte und Grundfreiheiten der betroffenen Personen nicht beschneiden (ErwGr. 109). Bei solchen Hinzufügungen sollten Unternehmen jedoch eine gewisse Vorsicht walten lassen, da im Falle eines inhaltlichen Widerspruchs zu den Standarddatenschutzklauseln die Übermittlung nicht mehr genehmigungsfrei ist.

c) Genehmigte Verhaltensregeln und genehmigter Zertifizierungsmechanismus (Art. 46 Abs. 2 Buchstabe e und f)

Neu hinzugekommen ist die Möglichkeit, Datenübermittlungen auf Grundlage von branchenspezifischen Verhaltensregeln gemäß Art. 40 zu legitimieren, sofern diese mit rechtsverbindlichen und durchsetzbaren Verpflichtungen des Verantwortlichen oder des Auftragsverarbeiters versehen sind und von der zuständigen Aufsichtsbehörde genehmigt worden sind.

Auch Zertifizierungen nach Art. 42 können nun zusammen mit rechtsverbindlichen und durchsetzbaren Verpflichtungen des Verantwortlichen oder des Auftragsverarbeiters als rechtliche Grundlage für einen Datentransfers in ein Drittland herangezogen werden, wenn die Zertifizierungsmechanismen zuvor genehmigt worden sind.

Die europäischen Aufsichtsbehörden werden in der Folgezeit die für eine praktische Anwendung dieser Instrumente notwendigen weiteren Einzelheiten im Hinblick auf rechtliche Rahmenbedingungen und Verfahrensfragen erarbeiten.

d) Einzeln ausgehandelte Vertragsklauseln (Art. 46 Abs. 3)

Ebenso können einzeln ausgehandelte individuelle Vertragsklauseln eine Datenübermittlung in ein Drittland legitimieren, allerdings nur nach Genehmigung der Aufsichtsbehörde und Durchführung des Kohärenzverfahrens nach Art. 63.

e) Rechte der betroffenen Personen

Gemäß Art. 46 Abs. 1 a. E. ist es bei allen in Betracht kommenden geeigneten Garantien im Sinne von Art. 46 zusätzlich erforderlich, den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe einzuräumen.

3. Ausnahmen für bestimmte Fälle (Art. 49 DS-GVO)

Eine Datenübermittlung kann in einer Reihe besonderer, vom Gesetz explizit genannter und abschließender Fälle, auch zulässig sein, wenn weder ein Angemessenheitsbeschluss der Kommission noch geeignete Garantien vorliegen. Die hierfür von der DS-GVO definierten Ausnahmetatbestände sind gemäß ihrem Ausnahmecharakter eng auszulegen.

a) Einwilligung (Art. 49 Abs. 1 UAbs. 1 Buchstabe a)

Eine wirksame Einwilligung der betroffenen Person in die Datenübermittlung in ein Drittland setzt zunächst eine ausdrückliche Einwilligung in die Weitergabe ihrer Daten für den konkreten Fall voraus. Weiter ist die betroffene Person vorher explizit über bestehende mögliche Risiken derartiger Datenübermittlungen aufzuklären, d.h. insbesondere darüber, dass kein angemessenes Datenschutzniveau gegeben ist und Betroffenenrechte ggf. nicht durchgesetzt werden können. Auch ist die betroffene Person darauf hinzuweisen, dass sie die Einwilligung jederzeit widerrufen kann (Art. 7 Abs. 3).

b) Erforderlichkeit zur Vertragserfüllung (Art. 49 Abs. 1 UAbs. 1 Buchstabe b und c)

Eine Datenübermittlung in ein Drittland ist (vorbehaltlich der weiteren Anforderungen der DS-GVO) zulässig, wenn und soweit die Übermittlung zur Erfüllung eines Vertrages mit der betroffenen Person oder zum Abschluss oder zur Erfüllung eines Vertrages im Interesse der betroffenen Person erforderlich ist. Wesentlich ist hier

jeweils die strikte Erforderlichkeit gerade dieser Datenübermittlung zur Erfüllung des Vertragszwecks.

c) Wichtige Gründe des öffentlichen Interesses (Art. 49 Abs. 1 UAbs. 1 Buchstabe d)

Die Übermittlung kann auch zulässig sein, wenn sie aus wichtigen Gründen des öffentlichen Interesses notwendig ist. In Betracht kommen nur wichtige öffentliche Interessen, die im Recht der Europäischen Union oder des Mitgliedstaates, dem der Verantwortliche unterliegt, anerkannt sind (Art. 49 Abs. 4). Wie aus Erwägungsgrund 112 hervorgeht, hatte der Gesetzgeber insoweit insbesondere Datentransfers im Rahmen der internationalen behördlichen Zusammenarbeit im Auge, etwa zwischen Wettbewerbs-, Steuer- oder Zollbehörden.

d) Verfolgung von Rechtsansprüchen (Art. 49 Abs. 1 UAbs. 1 Buchstabe e)

Auch die Verfolgung von Rechtsansprüchen kann eine Datenübermittlung legitimieren, wenn die Datenübermittlung hierzu erforderlich ist. In Erweiterung der bisherigen Regelung im BDSG kommt auch die Geltendmachung von Rechtsansprüchen in außergerichtlichen Verfahren in Betracht (ErwGr. 111).

e) Schutz lebenswichtiger Interessen (Art. 49 Abs. 1 UAbs. 1 Buchstabe f)

Ist die betroffene Person aus physischen oder rechtlichen Gründen nicht in der Lage, ihre Einwilligung zu erteilen, darf die Datenübermittlung dennoch durchgeführt werden, soweit dies zum Schutz ihrer lebenswichtigen Interessen oder derjenigen anderer Personen erforderlich ist.

f) Wahrung zwingender berechtigter Interessen (Art. 49 Abs. 1 UAbs. 2 S. 1)

Im Einzelfall kann eine Datenübermittlung in ein Drittland legitimiert sein, wenn ein zwingendes berechtigtes Interesse des Verantwortlichen an der Übermittlung besteht, die Übermittlung nicht wiederholt erfolgt, nur eine begrenzte Anzahl von Personen betrifft und keine überwiegenden schutzwürdigen Interessen oder Rechte und Freiheiten der betroffenen Person entgegenstehen und der Verantwortliche durch geeignete Garantien den Schutz personenbezogener Daten gewährleistet. Voraussetzung für diese Übermittlungserlaubnis ist ein zwingendes berechtigtes Interesse des Verantwortlichen an der Übermittlung, dem eine heraus-gehobene und besondere Bedeutung zukommt. Zudem muss die Übermittlung unbedingt erforderlich

sein zur Verfolgung dieses berechtigten Interesses. Die Übermittlung darf sich nicht bereits auf einen der oben genannten Erlaubnistatbestände stützen lassen. Wird eine Übermittlung in ein Drittland auf Grundlage eines zwingenden berechtigten Interesses in einem absoluten Einzelfall durchgeführt, ist sowohl die Aufsichtsbehörde als auch die betroffene Person hierüber zu informieren (Art. 49 Abs. 1 UAbs. 2 S. 2 und 3).

Anlage 65

Kurzpapier Nr. 5
Datenschutz-Folgenabschätzung, Art. 35 DS-GVO

Dieses Kurzpapier der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) dient als erste Orientierung, wie nach Auffassung der DSK die Datenschutz-Grundverordnung (DS-GVO) im praktischen Vollzug angewendet werden sollte. Diese Auffassung steht unter dem Vorbehalt einer zukünftigen – möglicherweise abweichenden – Auslegung des Europäischen Datenschutzausschusses.

Auch bei einer rechtmäßigen Verarbeitung personenbezogener Daten entstehen Risiken für die betroffenen Personen. Deswegen sieht die DS-GVO unabhängig von sonstigen Voraussetzungen für die Verarbeitung vor, dass durch geeignete Abhilfemaßnahmen (insbesondere durch technische und organisatorische Maßnahmen (TOMs)) diese Risiken eingedämmt werden. Das Instrument einer Datenschutz-Folgenabschätzung (DSFA) kann hierfür systematisch eingesetzt werden.

Was ist eine Datenschutz-Folgenabschätzung nach DS-GVO?
Eine DSFA ist ein spezielles Instrument zur Beschreibung, Bewertung und Eindämmung von Risiken für die Rechte und Freiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten. Die DSFA ist durchzuführen, wenn die Form der Verarbeitung, insbesondere bei der Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko zur Folge hat. Sie befasst sich insbesondere mit Abhilfemaßnahmen durch die der Schutz personenbezogener Daten sichergestellt und die Einhaltung der Verordnung nachgewiesen werden kann (Art. 35 Abs. 1, 7 DS-GVO sowie ErwGr. 84, 90). Zum Begriff des Risikos, der ein zentrales Konzept der DS-GVO ist, wird es ein eigenes Kurzpapier geben.

Verarbeitungsvorgang als Ankerpunkt
Eine DSFA bezieht sich auf einzelne, konkrete Verarbeitungsvorgänge. Unter Verarbeitungsvorgängen ist die Summe von Daten, Systemen (Hard- und Software) und Prozessen zu verstehen.

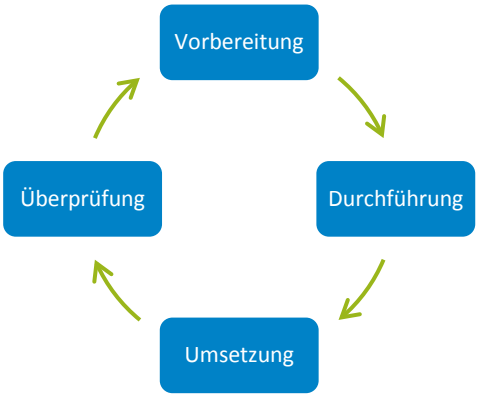
Sofern mehrere ähnliche Verarbeitungsvorgänge voraussichtlich ein ähnliches Risiko aufweisen, können diese zusammen bewertet werden (Art. 35 Abs. 1 DS-GVO). Ähnliche Risiken können beispielsweise dann gegeben sein, wenn ähnliche Technologien zur Verarbeitung vergleichbarer Daten(-kategorien) zu gleichen Zwecken eingesetzt werden (vgl. auch ErwGr. 92 DS-GVO). Bei einer gemeinsamen Bewertung von ähnlichen Verarbeitungsvorgängen sind die im Folgenden dargestellten Vorgehensweisen ggf. anzupassen.

Erforderlichkeit einer DSFA
Ob eine DSFA durchzuführen ist, ergibt sich aus einer Abschätzung der Risiken der Verarbeitungsvorgänge („Schwellwertanalyse“). Ergibt diese ein voraussichtlich hohes Risiko, dann ist eine DSFA durchzuführen. Wird festgestellt, dass der Verarbeitungsvorgang kein hohes Risiko aufweist, dann ist eine DSFA nicht zwingend erforderlich. In jedem Fall ist die Entscheidung über die Durchführung oder Nichtdurchführung der DSFA mit Angabe der maßgeblichen Gründe für den konkreten Verarbeitungsvorgang schriftlich zu dokumentieren.
Art. 35 Abs. 3 DS-GVO benennt einige Faktoren, die wahrscheinlich zu einem hohen Risiko i. S. d. Art. 35 Abs. 1 DS-GVO führen. Aufbauend auf den Leitlinien der Artikel-29-Datenschutzgruppe werden die Datenschutzaufsichtsbehörden eine nicht-abschließende Liste mit Verarbeitungstätigkeiten, bei denen eine DSFA durchzuführen ist, veröffentlichen. Auch zur Durchführung der Schwellwertanalyse werden künftig Hinweise zur Verfügung gestellt.

Zeitpunkt der Durchführung einer DSFA
Eine DSFA ist vor der Aufnahme der zu betrachtenden Verarbeitungsvorgänge durchzuführen. Auch bereits bestehende Verarbeitungsvorgänge können unter die Pflicht einer DSFA fallen. Da eine DSFA meist nicht ad hoc in wenigen Tagen erstellt werden kann, muss sie rechtzeitig, beispielsweise unterstützt durch ein allgemeines Datenschutz-Managementsystem, auf den Weg gebracht werden.

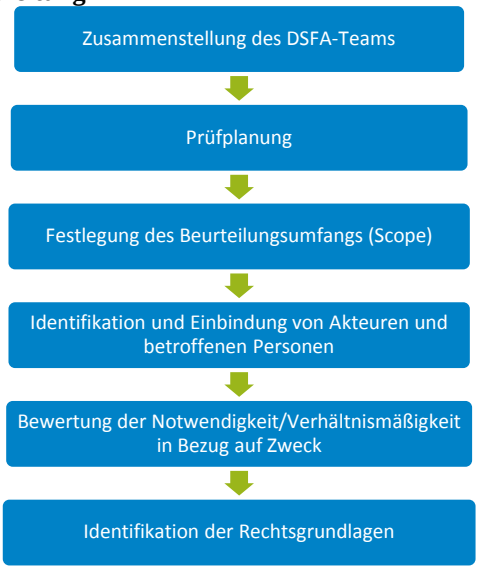
Wie kann eine DSFA durchgeführt werden?
Die formellen Anforderungen an die Durchführung einer DSFA ergeben sich aus der DS-GVO, speziell aus Art. 35 sowie den Erwägungsgründen 84, 90, 91, 92 und 93. Bei der verwendeten Methode wird dem Verantwortlichen mehr Spielraum gelassen. Werden be-

stehende Methoden oder Standards eingesetzt, ist zu beachten, dass die Anforderungen der DS-GVO immer vorrangig zu behandeln sind.
Eine DSFA ist kein einmaliger Vorgang. Sollten sich z .B. neue Risiken ergeben, die Bewertung bereits erkannter Risiken ändern oder wesentliche Änderungen im Verfahren ergeben, die in der DSFA bisher nicht berücksichtigt wurden, so ist die DSFA zu überprüfen und ebenso anzupassen. Um dies zu garantieren, wird ein stetiger, iterativer Prozess der Überprüfung und Anpassung empfohlen:



Die Bestandteile der Hauptprozessschritte werden im Einzelnen nachfolgend dargestellt.

Vorbereitung



1. Zusammenstellung des DSFA-Teams
Eine DSFA kann im Allgemeinen nur von einem interdisziplinären Team erstellt werden, das Kompetenzen im Bereich Datenschutz, Risikoermittlung und Fachprozesse mitbringt. Der Datenschutzbeauftragte steht diesem während des gesamten Prozesses beratend zur Seite. Es kann sinnvoll oder notwendig sein, z. B. Auftragsverarbeiter oder Hersteller von IT-Systemen ebenfalls mit einzubeziehen.

2. Prüfplanung
Da eine DSFA meist ein komplexer Prozess ist, der viele Mitwirkende einbindet, ist eine Prüfplanung (z. B. mit Methoden des Projektmanagements) empfehlenswert.

3. Festlegung des Beurteilungsumfangs (Scope)
Die betrachteten Verarbeitungsvorgänge sind von anderen (Geschäfts-)Prozessen abzugrenzen und ausführlich und abschließend mit allen Datenflüssen zu beschreiben. Wesentlich ist es, die beabsichtigten Zwecke der Verarbeitungsvorgänge festzuhalten.

4. *Identifikation und Einbindung von Akteuren und betroffenen Personen*

Die Akteure und betroffenen Personen sind zu identifizieren. Bei der Durchführung der DSFA zieht der Verantwortliche den Datenschutzbeauftragten zurate (Art. 35 Abs. 2 DS-GVO). Ggf. holt der Verantwortliche den Standpunkt der betroffenen Personen oder ihrer Vertreter zu der beabsichtigten Verarbeitung ein (Art. 35 Abs. 9 DS-GVO). Dies umfasst beispielsweise die Einbindung von Gremien der Mitbestimmung, z. B. von Betriebsräten.

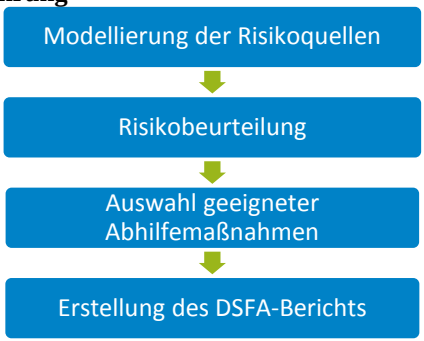
5. *Bewertung der Notwendigkeit/Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf ihren Zweck*

Die im vorigen Schritt beschriebenen Verarbeitungsvorgänge werden ausgehend von den mit ihnen verfolgten Zwecken daraufhin bewertet, ob der durch sie bewirkte Eingriff in die Rechte und Freiheiten der Betroffenen im Verhältnis zu dem angestrebten Zweck steht, ob sie zum Erreichen der Zwecke tatsächlich notwendig sind oder ob alternative Vorgehensweisen zur Verfügung stehen, die in die Rechte und Freiheiten der Betroffenen weniger stark eingreifen. Ggf. nimmt der Verantwortliche eine Anpassung der Verarbeitungsvorgänge vor, z. B. durch Beschränkung der zu verarbeitenden Daten oder durch Änderung der beteiligten Akteure oder eingesetzten Technologien.

6. *Identifikation der Rechtsgrundlagen*

Aufbauend auf dem vorigen Schritt können sodann die Rechtsgrundlagen für die zu bewertenden Verarbeitungsvorgänge bestimmt und dokumentiert werden.

Durchführung



7. Modellierung der Risikoquellen
Die Quellen des Risikos für die Rechte und Freiheiten natürlicher Personen müssen identifiziert werden. Insbesondere ist zu bestimmen, welche Personen motiviert sein könnten, die Verarbeitungsvorgänge und die hierin verarbeiteten Daten in unrechtmäßiger Weise zu nutzen, und welches ihre Beweggründe und möglichen Ziele sein können. Anhand dessen können die damit zusammenhängenden Eintrittswahrscheinlichkeiten ermittelt werden.

8. Risikobeurteilung
Aufbauend auf den vorherigen Schritten wird bestimmt, ob in Bezug auf die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen besteht. Potenzielle Schäden können physischer, materieller oder immaterieller Art sein. Ihre Schwere sowie die jeweilige Eintrittswahrscheinlichkeit sind dabei zu berücksichtigen (ErwGr. 75 f.).

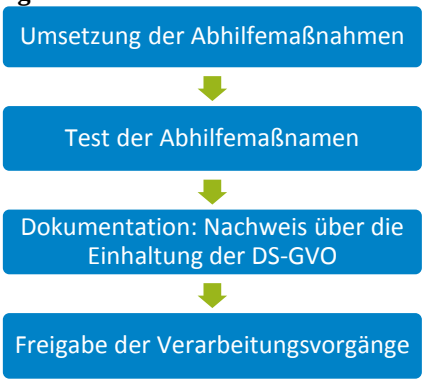
9. Auswahl geeigneter Abhilfemaßnahmen
Die ermittelten Risiken müssen durch geeignete Abhilfemaßnahmen (insbesondere durch TOMs) eingedämmt werden. Eine Auswahl sowie Planung der Umsetzung der Maßnahmen findet statt. Dabei wird den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen. Verbleibende Restrisiken werden ermittelt und dokumentiert.

10. Erstellung des DSFA-Berichts
Der DSFA-Bericht enthält gem. Art. 35 Abs. 7 DS-GVO jedenfalls die systematische Beschreibung der geplanten Verarbeitungsvorgänge und ihrer Zwecke, die Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitung, die Beschreibung und Beurteilung der Risiken sowie der Abhilfemaßnahmen zur Risikoeindämmung. Der Bericht ist um eine Darstellung der Restrisiken samt Entscheidung über den Umgang mit diesen zu ergänzen. Er kann sich dabei an den hier dargestellten Phasen orientieren. Der DSFA-Bericht dient ferner als Baustein einer umfassenden Dokumentation zur Umsetzung der in Art. 5 Abs. 2 DS-GVO normierten Rechenschaftspflicht. Es ist zu prüfen, inwieweit Teile des DSFA-Berichts

im Sinne einer erhöhten Transparenz für die betroffenen Personen veröffentlicht werden sollen.

Weitere Schritte nach Durchführung der DSFA
Die folgenden Schritte dienen der Implementierung der Abhilfemaßnahmen und sollten nicht lediglich linear durchlaufen werden, sondern eine Rückkoppelung der jeweiligen Ergebnisse im Sinne eines iterativen Vorgehens ermöglichen. Beispielsweise können durch eine Maßnahme weitere Verarbeitungsvorgänge nötig werden, für die wiederum etwaige Risiken zu betrachten sind.

Umsetzung



11. Umsetzung der Abhilfemaßnahmen
Bevor die geplante Datenverarbeitung eingesetzt wird, müssen die für die Eindämmung des Risikos geeigneten Abhilfemaßnahmen (insbesondere TOMs) umgesetzt sein. Vorher darf die Verarbeitung personenbezogener Daten nicht stattfinden. Sofern sich bei der Umsetzung herausstellt, dass geplante Maßnahmen nicht (wirksam) realisiert werden können, müssen andere geeignete Maßnahmen ausgewählt, die Restrisikobewertung angepasst oder die Verarbeitungsvorgänge insgesamt angepasst werden, so dass sie den Anforderungen der DS-GVO genügen.

12. Test der Abhilfemaßnahmen
Nachdem Abhilfemaßnahmen umgesetzt wurden, müssen sie auf ihre Wirksamkeit getestet werden. Möglicherweise zeigt sich bei der

Umsetzung der Maßnahmen, dass weitere Risiken bestehen, die ebenfalls zu behandeln sind.

13. Dokumentation: Nachweis über die Einhaltung der DS-GVO
Gem. Art. 5 Abs. 2 DS-GVO hat der Verantwortliche eine umfassende Dokumentations- und Rechenschaftspflicht, durch die die Einhaltung der DS-GVO insgesamt nachgewiesen werden soll. Der DSFA-Bericht und eine Bestätigung der Wirksamkeit der umgesetzten Maßnahmen dienen als Bausteine zur Erfüllung dieser Pflicht.

14. Freigabe der Verarbeitungsvorgänge
Im Anschluss und mit Vorliegen der vollständigen Dokumentation können die Verarbeitungsvorgänge formal durch den Verantwortlichen freigegeben werden.

Überprüfung



15. Ggf. Überprüfung und Audit der DSFA
Um eine ordnungsgemäße Durchführung sicherzustellen, kann es sinnvoll sein, den DSFA-Bericht von einem unabhängigen Dritten überprüfen zu lassen. Auch könnte der Datenschutzbeauftragte, der gemäß Art. 35 Abs. 2 DS-GVO sowieso einzubeziehen ist, die DSFA abschließend prüfen und das Ergebnis der Leitungsebene des Verantwortlichen mitteilen.

16. Fortschreibung
Die DSFA ist kein strikt linearer oder abgeschlossener Prozess. Vielmehr muss die Einhaltung der DS-GVO während der gesamten Dauer der Verarbeitungsvorgänge fortlaufend überwacht werden. Hierfür bietet sich ein Datenschutz-Managementsystem an. Spätestens wenn sich das mit der Verarbeitung verbundene Risiko ändert, muss erneut eine DSFA durchgeführt werden.

Umgang mit hohen Restrisiken
Ergibt eine DSFA, dass trotz technischer und organisatorischer Maßnahmen zur Risikoeindämmung weiterhin ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen besteht (Restrisiko), muss nach Art. 36 DS-GVO der Verantwortliche die zuständige Aufsichtsbehörde konsultieren. Er trifft unter Berücksichtigung der Empfehlungen der Aufsichtsbehörde eine Entscheidung, ob die Verarbeitungsvorgänge angesichts der verbleibenden Restrisiken durchgeführt werden können und ggf. welche zusätzlichen Abhilfemaßnahmen in diesem Fall zum Einsatz kommen sollen. Die Aufsichtsbehörde kann ihrerseits die in Art. 58 DS-GVO genannten Befugnisse ausüben und z. B. eine Warnung, Anweisung oder Untersagung aussprechen.

Fazit
Die Datenschutz-Folgenabschätzung ist ein sinnvolles Instrument zur systematischen Risikoeindämmung und stellt eine der wichtigsten Neuerungen der DS-GVO gegenüber dem BDSG dar. Rechtzeitig auf den Weg gebracht hilft sie nicht nur, die eigenen Prozesse bei der Verarbeitung personenbezogener Daten besser zu verstehen, sondern auch die Pflichten nach der Grundverordnung umzusetzen.

Anlage 66

Kurzpapier Nr. 6
Auskunftsrecht der betroffenen Person, Art. 15 DS-GVO

Dieses Kurzpapier der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) dient als erste Orientierung insbesondere für den nicht-öffentlichen Bereich, wie nach Auffassung der DSK die Datenschutz-Grundverordnung (DS-GVO) im praktischen Vollzug angewendet werden sollte. Diese Auffassung steht unter dem Vorbehalt einer zukünftigen – möglicherweise abweichenden – Auslegung des Europäischen Datenschutzausschusses.

Auskunftsrecht als zentrales Recht zur Schaffung von Transparenz

Wie schon nach der bisherigen Rechtslage haben betroffene Personen das Recht mit formlosem Antrag und ohne Begründung von einem Verantwortlichen Auskunft über dort gespeicherte personenbezogene Daten zu verlangen. Die Auskünfte können es beispielsweise erleichtern, gezielt weitere Rechte, wie auf Berichtigung, Löschung oder Einschränkung der Verarbeitung („Sperrung“), geltend zu machen.

Umfang des Auskunftsrechts

Nach Art. 15 Abs. 1 DS-GVO steht der betroffenen Person ein abgestuftes Auskunftsrecht zu.

Zum einen kann die betroffene Person von dem Verantwortlichen eine Bestätigung darüber verlangen, ob dort sie betreffende personenbezogene Daten verarbeitet werden. Auch eine Negativauskunft ist erforderlich, wenn der Verantwortliche entweder keine Daten zu dieser Person verarbeitet oder personenbezogene Daten unumkehrbar anonymisiert hat.

Zum anderen kann die betroffene Person ganz konkret Auskunft darüber verlangen, welche personenbezogenen Daten vom Verantwortlichen verarbeitet werden (z. B. Name, Vorname, Anschrift, Geburtsdatum, Beruf, medizinische Befunde).

Weiterhin sind bei der Datenauskunft vom Verantwortlichen nach Art. 15 Abs. 1 DS-GVO vor allem noch folgende Informationen mitzuteilen:

- Verarbeitungszwecke,
- Kategorien personenbezogener Daten, die verarbeitet werden (mit Gruppenbezeichnungen wie Gesundheitsdaten, Bonitätsdaten usw.),
- Empfänger bzw. Kategorien von Empfängern, die diese Daten bereits erhalten haben oder künftig noch erhalten werden,
- geplante Speicherdauer falls möglich, andern-falls die Kriterien für die Festlegung der Speicherdauer,
- Rechte auf Berichtigung, Löschung oder Einschränkung der Verarbeitung,
- Widerspruchsrecht gegen diese Verarbeitung nach Art. 21 DS-GVO,
- Beschwerderecht für die betroffene Person bei der Aufsichtsbehörde,
- Herkunft der Daten, soweit diese nicht bei der betroffenen Person selbst erhoben wurden, und
- das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling mit aussagekräftigen Informationen über die dabei involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen solcher Verfahren.

Im Falle der Datenübermittlung in Drittländer ist über die insoweit gegebenen Garantien gemäß Art. 46 DS-GVO zu informieren (z. B. vereinbarte Standard-Datenschutzklauseln, verbindliche interne Datenschutzvorschriften, d. h. BCR). Keine Drittländer sind die EU-Mitgliedsstaaten

Form der Auskunftserteilung

Die Auskunftserteilung an die betroffene Person kann nach Art. 12 Abs. 1 Sätze 2 und 3 DS-GVO je nach Sachverhalt schriftlich, elektronisch oder – auf Wunsch der betroffenen Person – mündlich erfolgen. Der Verantwortliche stellt eine Kopie der Daten zur Verfügung (Art. 15 Abs. 3 Satz 1 DS-GVO). Stellt die betroffene Person ihren Auskunftsantrag elektronisch, ist die Auskunft nach Art. 15 Abs. 3 Satz 2 DS-GVO in einem gängigen elektronischen Format zur Verfügung zu stellen (z. B. im PDF-Format). Als datenschutzfreundlichste Gestaltung wird in Erwägungsgrund (ErwGr.) 63 Satz 4 ein vom Verantwortlichen eingerichteter Fernzugriff der betroffenen

Person auf ihre eigenen Daten bezeichnet. Alle Kommunikationswege müssen angemessene Sicherheitsanforderungen erfüllen.

Frist für die Auskunftserteilung
Auskunftserteilungen müssen gemäß Art. 12 Abs. 3 DS-GVO unverzüglich erfolgen, spätestens aber innerhalb eines Monats; nur in begründeten Ausnahmefällen kann die Monatsfrist überschritten werden, worüber die betroffene Person zu informieren ist (Art. 12 Abs. 3 Satz 3 DS-GVO). Der Verantwortliche muss (vorbereitend) geeignete organisatorische Maßnahmen treffen, damit die betroffene Person eine beantragte Auskunft zeitnah und in verständlicher Form erhalten kann (Art. 12 Abs. 1 Satz 1 und Art. 5 Abs. 2 DS-GVO).

Kosten der Auskunftserteilung
Die Auskunftserteilung an die betroffene Person (z. B. als Kopie) muss durch den Verantwortlichen regelmäßig unentgeltlich erfolgen, Art. 12 Abs. 5 Satz 1 DS-GVO. Für weitere Kopien kann er ein angemessenes Entgelt fordern. Außerdem kann bei offenkundig unbegründeten oder exzessiven Anträgen ein angemessenes Entgelt für die Auskunft verlangt werden (Art. 12 Abs. 5 Satz 2, ErwGr. 63).

Identitätsprüfung
Es muss sichergestellt werden, dass die zu beauskunftenden Daten nicht unbefugten Dritten zur Verfügung gestellt werden. Hierauf ist auch insbesondere bei mündlicher oder elektronischer Auskunftserteilung zu achten. Hat der Verantwortliche begründete Zweifel an der Identität eines Antragstellers auf Datenauskunft, so kann er nach Art. 12 Abs. 6 DS-GVO zusätzliche Informationen zur Bestätigung der Identität nachfordern (z. B. eine Postadresse bei elektronischem Auskunftsantrag).

Grenzen des Auskunftsrechts
Bei einer großen Menge von gespeicherten Informationen über die betroffene Person kann der Verantwortliche verlangen, dass präzisiert wird, auf welche Informationen oder Verarbeitungsvorgänge sich das Auskunftsersuchen konkret bezieht (ErwGr. 63 Satz 7). Das kann z. B. bei Banken oder Versicherungen mit umfangreichen Vertragsbeziehungen zu der betroffenen Person der Fall sein.

Offenkundig unbegründete oder exzessive Anträge einer betroffenen Person können zur Ablehnung oder zu einer Kostenerstattungspflicht führen (Art. 12 Abs. 5 S. 2 DS-GVO). Die betroffene Person muss jedoch (und zwar kostenfrei) ihr Recht in angemessenen Abständen wahrnehmen können, um sich der Verarbeitung bewusst zu sein und deren Rechtmäßigkeit überprüfen zu können (ErwGr. 63). Eine Ablehnung oder Kostenerstattung kommt daher nur in Ausnahmefällen in Betracht. Der Verantwortliche trägt die Beweislast für das Vorliegen eines unbegründeten oder exzessiven Antrags (Art. 12 Abs. 5 Satz 3 DS-GVO). Er muss der betroffenen Person in der Regel die Gründe für die Verweigerung der Auskunft mitteilen und sie über Rechtsschutzmöglichkeiten informieren (Art. 12 Abs. 4 DS-GVO).
Das BDSG-neu enthält in § 34 noch weitere Eingrenzungen des Auskunftsrechts, insbesondere für Archivdaten und Protokollierungsdaten.
Ob und wenn ja wie weit die Regelungen des BDSG-neu zur Einschränkung der Betroffenenrechte wegen des bestehenden Anwendungsvorrangs der DS-GVO angewendet werden können, bleibt eine Entscheidung im jeweiligen konkreten Einzelfall vorbehalten.

Beachtung Rechte Dritter
Die Auskunftserteilung an die betroffene Person darf nach Art. 15 Abs. 4 DS-GVO sowie ErwGr. 63 Satz 5 die Rechte des Verantwortlichen oder anderer Personen nicht beeinträchtigen, was bei Geschäftsgeheimnissen oder bei Daten mit Bezug auch auf andere Personen der Fall sein kann. Dies darf im Ergebnis aber nicht dazu führen, dass jegliche Auskunft verweigert wird.

Rechtfolgen bei Verstoß
Unterlassene oder nicht vollständige Auskunftserteilungen an betroffene Personen sind nach Art. 83 Abs. 5 Buchstabe b DS-GVO mit einer hohen Geldbuße bedroht.

Empfehlung
Es ist für Verantwortliche ratsam, rechtzeitig im eigenen Interesse organisatorische Vorkehrungen für zügige und korrekte Auskunftserteilungen zu treffen.

Anlage 67

Kurzpapier Nr. 7
Marktortprinzip: Regelungen für außereuropäische Unternehmen

Dieses Kurzpapier der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) dient als erste Orientierung insbesondere für den nicht-öffentlichen Bereich, wie nach Auffassung der DSK die Datenschutz-Grundverordnung (DS-GVO) im praktischen Vollzug angewendet werden sollte. Diese Auffassung steht unter dem Vorbehalt einer zukünftigen – möglicherweise abweichenden – Auslegung des Europäischen Datenschutzausschusses.

Regelung des Marktortprinzips in Art. 3 Abs. 2 DS-GVO
Das Marktortprinzip schließt unter bestimmten Bedingungen auch Unternehmen, die nicht in der EU niedergelassen sind, in den Anwendungsbereich der DS-GVO ein.

Seit In-Kraft-Treten der EU-Datenschutzrichtlinie im Jahr 1995 haben sich neue Fragestellungen zum Anwendungsbereich des europäischen Datenschutzrechts entwickelt, beispielsweise mit Blick auf die fortschreitende Verlagerung von Geschäftsaktivitäten ins Internet (eCommerce). Sie erfordern keine physischen Betriebs- und Organisationsstrukturen in Europa, die als direkter Anknüpfungspunkt für die Anwendbarkeit europäischen Datenschutzrechts dienen könnten.

Der europäische Gesetzgeber erstreckt den Anwendungsbereich des europäischen Datenschutzrechts mit Einführung des Marktortprinzips auf datenschutzrechtlich relevante Geschäftsaktivitäten von Unternehmen, die keine Niederlassungen in der EU besitzen und damit an sich außerhalb des territorialen Anwendungsbereichs nach Art. 3 Abs. 1 DS-GVO liegen würden. Unter den von Art. 3 Abs. 2 Buchstabe a und Buchstabe b DS-GVO festgelegten Bedingungen erstreckt sich der Anwendungsbereich der DS-GVO auf Verarbeitungen personenbezogener Daten von Betroffenen, die sich in der EU befinden, ohne Rücksicht auf physische Organisations- oder Betriebsstrukturen von Unternehmen in der EU.

1. Anknüpfungspunkt: Angebot von Waren und Dienstleistungen (Art. 3 Abs. 2 Buchstabe a DS-GVO)
Die DS-GVO findet Anwendung, wenn eine Daten-verarbeitung im Zusammenhang damit steht, betroffenen Personen in der EU Waren oder Dienst-leistungen anzubieten. Das Unternehmen muss dies offensichtlich beabsichtigen (vgl. ErwGr. 23). Die Zahlung eines Entgeltes für das Waren- oder Dienstleistungsangebot ist hierbei für die Anwendbarkeit der DS-GVO irrelevant, sondern es sollen explizit auch unentgeltliche Angebote, z. B. Dienstleistungen durch soziale Netzwerke, darunter fallen.

Ein maßgeblicher Anknüpfungspunkt ist die Ausrichtung bestimmter Werbe- bzw. Verkaufsmaßnahmen auf Personen, die sich in der EU befinden. Wann dies der Fall ist, muss anhand von Hilfsfaktoren und Indizien bestimmt werden. Keine ausreichenden Anhaltspunkte hierfür sind etwa allein

- die bloße Abrufbarkeit einer kommerziellen Internetpräsenz, einer E-Mail-Adresse oder sonstiger Kontaktdaten oder
- die Verwendung einer (EU-)Sprache, die in dem Drittstaat, in dem das jeweilige Unter-nehmen niedergelassen ist, allgemein gebräuchlich ist.

Haftungsausschlüsse (so genannte Disclaimer), die beispielsweise die Anwendbarkeit der DS-GVO beschränken oder ausschließen, lassen wiederum nicht zwingend auf die Nichtanwendbarkeit der DS-GVO schließen.
Andere Faktoren wie

- die Verwendung der Sprache oder Währung eines Mitgliedstaates in Verbindung mit der Möglichkeit, Waren und Dienstleistungen in dieser anderen Sprache zu bestellen oder
- die Erwähnung von Kunden oder Nutzern, die sich in der EU befinden,

können darauf hindeuten, dass ein Unternehmen beabsichtigt, den betroffenen Personen in der EU Waren oder Dienstleistungen anzubieten (vgl. ErwGr. 23). Ein Angebot kann auch dann (potentielle) Kunden und Nutzer in der EU adressieren, wenn das jeweilige Waren- oder Dienstleistungsangebot einen hinreichend konkreten perso-

nalen Bezug zum Marktgeschehen aufweist. Zur Bestimmung dessen können beispielsweise „Flaggen-Icons“, landesspezifische „Top Level Domains“ oder geographische Referenzen zu den mitgliedstaatlichen Märkten herangezogen werden.

2. Anknüpfungspunkt: Überwachung des Verhaltens von Personen (Art. 3 Abs. 2 Buchstabe b DS-GVO)
Die DS-GVO ist auch dann anwendbar, wenn die Datenverarbeitung im Zusammenhang damit steht, das Verhalten von betroffenen Personen zu beobachten, soweit dieses Verhalten in der EU erfolgt. Dies ist zum Beispiel dann der Fall, wenn die Internetaktivitäten der betroffenen Person nachvollzogen werden. Eine solche Nachvollziehbarkeit kann auch im Fall der nachfolgenden Erstellung von (Persönlichkeits-)Profilen angenommen werden, wenn

- diese die Grundlage für eine die jeweilige Person betreffende Entscheidung bilden oder
- anhand derer die Vorlieben, Verhaltensweisen oder Gepflogenheiten einer natürlichen Person analysiert oder vorausgesagt wer-den sollen (vgl. ErwGr. 24).

Dies kann zum Beispiel durch den Einsatz von „Tracking-Cookies“ oder „Browser Fingerprints“ statt-finden. Diese Techniken können auch als Grundlage für die weitere Erstellung persönlicher Profile, etwa zum Zwecke individualisierter bzw. zielgruppenspezifischer Werbung (sog. Behavioural Targeting) dienen.

Weitere Folgen
Außereuropäische Unternehmen, auf deren Verarbeitungstätigkeiten die DS-GVO anwendbar ist, müssen grundsätzlich einen in einem betroffenen Mitgliedstaat niedergelassenen Vertreter benennen. Der Vertreter ist ausdrücklich zu bestellen und schriftlich zu beauftragen, in Bezug auf die sich aus der DS-GVO ergebenden Pflichten an Stelle des Verantwortlichen oder des Auftragsverarbeiters zu handeln. Als Anlaufstelle soll dieser Vertreter einerseits den betroffenen Personen ermöglichen, ihre Betroffenenrechte wirksam geltend zu machen und andererseits die Aufsichtsbehörden in die Lage versetzen, ihre Aufsichtsmaßnahmen effektiv durchzusetzen (Art. 27 DS-GVO, siehe auch ErwGr. 80). Die Pflicht entfällt, wenn die Verarbeitung

- lediglich gelegentlich erfolgt,
- nicht die umfangreiche Verarbeitung sensibler personenbezogener Daten im Sinn von Art. 9 DS-GVO einschließt,
- nicht die umfangreiche Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten (Art. 10 DS-GVO) einschließt und
- nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.

Der Verstoß gegen die Pflicht zur Bestellung ist bußgeldbewehrt (vgl. Art. 83 Abs. 4 Buchstabe a DS-GVO).

Fazit
Auch Unternehmen, die keine Niederlassung in der EU haben, aber auf dem europäischen Markt tätig sind, müssen die DS-GVO voll anwenden. Darüber hinaus sind diese Unternehmen grundsätzlich verpflichtet, einen Vertreter in der EU zu benennen. Der europäische Gesetzgeber stellt die Aufsichtsbehörden mit Einführung des Marktortprinzips vor die nicht zu unterschätzende Herausforderung, den Geltungsanspruch der DS-GVO gegenüber Unternehmen in Drittstaaten durchzusetzen.

Anlage 68

Kurzpapier Nr. 8
Maßnahmenplan „DS-GVO“ für Unternehmen

Dieses Kurzpapier der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) dient als erste Orientierung insbesondere für den nicht-öffentlichen Bereich, wie nach Auffassung der DSK die Datenschutz-Grundverordnung (DS-GVO) im praktischen Vollzug angewendet werden sollte. Diese Auffassung steht unter dem Vorbehalt einer zukünftigen – möglicherweise abweichenden – Auslegung des Europäischen Datenschutzausschusses.

Bedeutung
Die DS-GVO, die im Mai 2016 in Kraft getreten ist, wird weitreichende Auswirkungen auf nahezu alle Unternehmen in Europa haben. Anders als die bisherige EU-Richtlinie wird diese EU-Verordnung ab dem 25. Mai 2018 unmittelbar in den Mitgliedsstaaten der EU anwendbar sein und wird das bis dahin geltende Bundesdatenschutzgesetz (BDSG) ablösen. Gleichzeitig sieht das deutsche Datenschutz-Anpassungs- und Umsetzungsgesetz-EU (DSAnpUG-EU) eine ergänzende Neufassung des nationalen Rechts vor (z. B. BDSG-neu), soweit in der DS-GVO Spielraum für nationale Regelungen besteht. Viele Unternehmen sind aber noch nicht auf die DS-GVO und deren Auswirkungen auf die Unternehmensprozesse vorbereitet. Daher haben die unabhängigen Datenschutzbehörden einige Tipps zur Erstellung eines Maßnahmenplans für Unternehmen zusammengestellt.

Information der Geschäftsleitung
Alle Entscheidungsträger in einem Unternehmen sollten sich der Auswirkungen der DS-GVO bewusst sein und wissen, was dies für den alltäglichen Betrieb in ihrem Unternehmen bedeutet. In einem ersten Schritt ist daher von den betrieblichen Datenschutzbeauftragten und/oder den IT-Verantwortlichen die Geschäftsleitung zu informieren.

Start eines Projekts zur Umsetzung der DS-GVO

Alle Verfahren, mit denen personenbezogene Daten verarbeitet werden, sind dahingehend zu überprüfen, ob es einen Anpassungsbedarf im Hinblick auf die DS-GVO gibt. Dies betrifft insbesondere die rechtlichen, technischen und organisatorischen Bereiche in einem Unternehmen. Da folglich verschiedene Personen bzw. Abteilungen im Unternehmen beteiligt sind, die untereinander koordiniert werden müssen, bietet es sich an, ein Projekt mit dem Ziel zu initiieren, die Datenschutzkonzeption anhand eines Soll-Ist-Abgleichs zu aktualisieren.
Die Kernaufgabe wird dabei sein, herauszufinden, welche Prozesse im Unternehmen anzupassen sind.

1. Bestandsaufnahme
Um ein genaues Verständnis davon zu bekommen, wie in einem Unternehmen mit personenbezogenen Daten umgegangen wird, sollten die aktuell realisierten Rahmenbedingungen aller Datenverarbeitungen analysiert werden (Ist-Zustand). Dies betrifft u. a.

- die derzeitigen Prozesse im Unternehmen, in denen personenbezogene Daten verarbeitet werden (bestehende Dokumentationen, beispielsweise ein Verfahrensverzeichnis, können hierfür einen Ausgangspunkt bilden),
- die dazugehörigen Rechtsgrundlagen (die Verarbeitung personenbezogener Daten ist nur dann zulässig, wenn entweder ein Gesetz oder eine Rechtsvorschrift dies erlaubt oder der Betroffene eingewilligt hat),
- die Datenschutzorganisation (d. h. alle Vorkehrungen und Maßnahmen, die im Unternehmen zum Schutz personenbezogener Daten getroffen werden),
- die Dienstleistungsbeziehungen (wie etwa Verträge über eine Auftragsdatenverarbeitung),
- die Dokumentation (z. B. Verfahrensverzeichnisse, Vorabkontrollen, Datenschutzkonzepte, IT-Sicherheitskonzepte, Sicherheitsvorfälle) und
- sofern vorhanden Betriebsvereinbarungen, denn diese können auch Regelungen zum Umgang mit den Daten der Beschäftigten enthalten.

2. Handlungsbedarf eruieren

Nunmehr ist der Soll-Zustand zu ermitteln und im Anschluss daran eine Lückenanalyse zwischen dem jetzigen Ist-Zustand und dem künftigen Soll-Zustand durchzuführen. Dabei sind u. a. folgende Punkte vor dem Hintergrund der DS-GVO zu beachten (zu den einzelnen Themen erscheinen weitere Kurzpapiere):

- **Rechtsgrundlagen:**
  Auch unter der DS-GVO ist für die Verarbeitung personenbezogener Daten eine Legitimationsgrundlage erforderlich. Folglich ist zu prüfen, ob das neue Recht für alle Prozesse eine Rechtsgrundlage bereitstellt. Sofern sich die Datenverarbeitung auf eine Einwilligung stützt, ist zu prüfen, ob die Anforderungen des Art. 7 DS-GVO erfüllt sind (bei Einwilligung eines Kindes in Bezug auf Dienste der Informationsgesellschaft ist zudem Art. 8 DS-GVO zu beachten).
- **Betroffenenrechte:**
  Den betroffenen Personen stehen umfangreiche Rechte zu, die der Verantwortliche zu beachten hat (z. B. Informationspflichten des Verantwortlichen gegenüber den betroffenen Personen nach Art. 13 und Art. 14 DS-GVO, Auskunftsrecht nach Art. 15 DS-GVO, Recht auf Berichtigung nach Art. 16 DS-GVO, Recht auf Löschung nach Art. 17 DS-GVO, das neue Recht auf Datenübertragbarkeit nach Art. 20 DS-GVO, Widerspruchsrecht nach Art. 21 DS-GVO).
- **Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen:**
  Die DS-GVO enthält spezifische Rahmen-bedingungen für die Art und Weise, wie die Anforderungen der DS-GVO schon bei der Prozessgestaltung und bei den Voreinstellungen umzusetzen sind (Art. 25 DS-GVO: Data Protection by design und Data Protection by default).
- **Dienstleistungsbeziehungen:**
  Dabei sollten insbesondere die bestehenden Verträge zur Auftragsverarbeitung überprüft werden. Die Art. 28 und 29 DS-GVO enthalten Vorgaben für Vereinbarungen mit Auftragsverarbeitern.
- **Dokumentationspflichten:**
  Die DS-GVO verpflichtet in Art. 5 Abs. 2 DS-GVO den Verantwortlichen zum Nachweis, dass personenbezogene Daten rechtmäßig verarbeitet werden (Rechenschaftspflicht). Zusätz-

lich sieht die DS-GVO an unterschiedlichen Stellen Dokumentationspflichten vor (z. B. für das Verarbeitungsverzeichnis in Art. 30 DS-GVO, für die Dokumentation von Datenschutzvorfällen in Art. 33 Abs. 5 DS-GVO oder für die Dokumentation von Weisungen im Rahmen der Auftragsverarbeitung in Art. 28 Abs. 3 Buchstabe a DS-GVO).

- **Datenschutz-Folgenabschätzung:**
  Die aus dem BDSG bekannte Vorabkontrolle wird durch die Datenschutz-Folgen-abschätzung nach Art. 35 DS-GVO abgelöst und erfordert eine umfangreiche Dokumentation. Die Datenschutz-Folgenabschätzung kann zudem eine Konsultation der Aufsichtsbehörde nach sich ziehen (Art. 36 DS-GVO).
- **Meldepflichten:**
  Nach Art. 37 Abs. 7 DS-GVO muss der Verantwortliche oder der Auftragsverarbeiter die Kontaktdaten des Datenschutzbeauftragten der zuständigen Aufsichtsbehörde melden. Ebenso ist der Aufsichtsbehörde die Verletzung des Schutzes personenbezogener Daten zu melden (Art. 33 Abs. 1 DS-GVO).
- **Datensicherheit:**
  Unternehmen müssen ein angemessenes Schutzniveau in Bezug auf die Sicherheit der Verarbeitung gewährleisten und die dafür implementierten Sicherungsmaßnahmen einer regelmäßigen Überprüfung unterziehen (Art. 24 und 32 DS-GVO).
- **Zertifizierung:**
  Schlussendlich besteht im Rahmen eines Zertifizierungsverfahrens die Möglichkeit, den Nachweis zu erbringen, dass die Datenverarbeitung im Einklang mit der DS-GVO erfolgt.

3. Umsetzung bis zum 25. Mai 2018

Bei der Umsetzung sind dann u. a. folgende Punkte wieder zu beachten:

- Anpassung der betroffenen Prozesse und Strukturen,
- Festlegung der Rechtsgrundlagen und des Zwecks der Datenverarbeitung sowie Dokumentation von Interessenabwägungen (sofern erfolgt),
- Implementierung von Informationspflichten, Betroffenenrechten und Löschkonzepten,
- Anpassung der Datenschutzorganisation,
- ggf. Bestellung eines Datenschutzbeauftragten,

- Reaktionsmechanismen auf Datenpannen,
- Organisation von Meldepflichten,
- Anpassung der Dienstleistungsbeziehungen,
- Aufbau der Dokumentation,
- Anpassung der IT-Sicherheit und
- ggf. Anpassung der Betriebsvereinbarungen.

Anlage 69

Kurzpapier Nr. 9
Zertifizierung nach Art. 42 DS-GVO

Dieses Kurzpapier der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) dient als erste Orientierung insbesondere für den nicht-öffentlichen Bereich, wie nach Auffassung der DSK die Datenschutz-Grundverordnung (DS-GVO) im praktischen Vollzug angewendet werden sollte. Diese Auffassung steht unter dem Vorbehalt einer zukünftigen - möglicherweise abweichenden - Auslegung des Europäischen Datenschutzausschusses.

Sinn und Zweck von Zertifizierungen
Im Datenschutzalltag trifft man häufig auf eine grundlegende Fragestellung: *„Woher weiß man, ob datenschutzrechtliche Vorgaben von einem Unternehmen oder einer Behörde eingehalten werden?“*. Eine auf den ersten Blick einfache und pragmatische Lösung wäre, sich dies durch entsprechende Zertifizierungen nachweisen zu lassen. Mit den Artikeln 42 und 43 der DS-GVO legt der Gesetzgeber einen rechtlichen Grundstein für europäisch einheitliche Akkreditierungs- und Zertifizierungsverfahren, die dazu dienen, die Einhaltung der DS-GVO bei Verarbeitungsvorgängen nachzuweisen.

Bisherige Erfahrungen der Aufsichtsbehörden
Die Aufsichtsbehörden haben in ihren Kontrollen zwar festgestellt, dass Organisationen oft verschiedenste Zertifikate vorweisen konnten – jedoch war häufig unklar, inwieweit die gesetzlichen Anforderungen an den Datenschutz ausreichend berücksichtigt wurden. Manche bestehende Zertifizierungsverfahren, wie beispielsweise das Informationssicherheitsmanagement nach ISO 27001, decken nur einen Teilbereich des Datenschutzes ab und haben mitunter auch die betroffenen Personen mit ihren Rechten und Freiheiten nicht im Mittelpunkt der Betrachtung.

Förderung von Zertifizierungen
Einleitend weist Art. 42 Abs. 1 DS-GVO darauf hin, dass unter anderem auch die Aufsichtsbehörden auf Unionsebene die Einführung von datenschutzspezifischen Zertifizierungsverfahren, Datenschutz-

siegeln und -prüfzeichen fördern sollen. Diese dienen dazu, nachzuweisen, dass die DS-GVO bei Verarbeitungsvorgängen von Verantwortlichen oder Auftragsverarbeitern eingehalten wird. Bis es jedoch so weit ist, dass die Verordnung umgesetzt und angewandt werden kann, müssen die Mitgliedstaaten in einer engen Zusammenarbeit die in der DS-GVO geforderten Mechanismen und Kriterien entwickeln. Dies ist zeitlich, räumlich und kapazitiv eine große Herausforderung für alle Beteiligten.

Vorteile einer Zertifizierung
Die DS-GVO nennt explizit einige Anwendungsbereiche, bei denen eine Zertifizierung für den Nachweis der Einhaltung der Grundverordnung als Faktor mit herangezogen werden kann:

- Erfüllung der Pflichten des Verantwortlichen (Art. 24 Abs. 3)
- Erfüllung der Anforderungen an Technikgestaltung und datenschutz-freundliche Voreinstellungen des Art. 25 Abs. 1 und 2 (vgl. Abs. 3)
- Garantien des Auftragsverarbeiters nach Art. 28 (vgl. Abs. 5 und 6)
- Sicherheit der Verarbeitung (Art. 32 Abs. 3)
- Datenübermittlung an ein Drittland (Art. 46 Abs. 2 Buchstabe f)
- Datenschutz-Folgeabschätzung (ErwGr. 90)

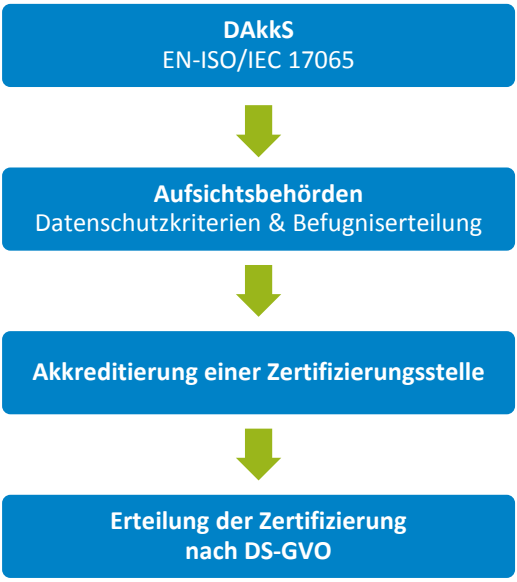
Daneben kann ein Zertifikat auch für Marketingzwecke genutzt werden, um sowohl Geschäftskunden, Verbrauchern als auch Bürgern gegenüber die Beachtung des Datenschutzrechts darzustellen.

Einhaltung der DS-GVO – auch mit Zertifikat
Art. 42 Abs. 4 hebt hervor, dass eine erfolgreiche Zertifizierung eine Organisation (unabhängig davon, ob Verantwortlicher oder Auftragsverarbeiter) nicht von der Verantwortung für die Einhaltung der DS-GVO befreit. Ebenso verdeutlicht Art. 42 Abs. 4, dass die Aufgaben und Befugnisse der zuständigen Aufsichtsbehörden von einer Zertifizierung unberührt bleiben. Ein nach DS-GVO genehmigtes Zertifizierungsverfahren kann jedoch bei aufsichtlichen Kontrollen von Vorteil sein und die Prüfung erleichtern.

Zertifizierungsstellen

Nach Art. 42 Abs. 5 DS-GVO können sowohl akkreditierte Zertifizierungsstellen als auch die zuständigen Aufsichtsbehörden eine Datenschutz-Zertifizierung nach DS-GVO erteilen. Die Akkreditierung nimmt in Deutschland die Deutsche Akkreditierungsstelle GmbH (DAkkS) zusammen mit den Aufsichtsbehörden gemäß § 39 Akkreditierung DSAnpUG („BDSG-neu“) vor. Die Kriterien für die Akkreditierung werden von den Aufsichtsbehörden entwickelt und beruhen u.a. auf einschlägigen ISO-Normen (siehe Abbildung). Eine einvernehmliche Entscheidung der beiden Parteien in einem eigens dafür eingerichteten Ausschuss ist Voraussetzung für die Akkreditierung einer Zertifizierungsstelle. Erst danach und nach der Erteilung der Befugnis durch die zuständige Aufsichtsbehörde, kann die Zertifizierungsstelle tätig werden. Sie darf im Anschluss, nach entsprechender Prüfung der Einhaltung der DS-GVO, Zertifizierungen erteilen.

Gesamtverfahren im Überblick



Voraussetzung für eine Zertifizierung

Damit eine Zertifizierung durchgeführt werden kann, muss die zu zertifizierenden Stelle alle für die Durchführung des Zertifizierungsverfahrens erforderlichen Informationen zur Verfügung stellen und

Zugang zu den betroffenen Verarbeitungstätigkeiten gewähren (Art. 42 Abs. 6 DS-GVO). Somit wird es künftig umso wichtiger, die eigenen Verarbeitungsvorgänge zu kennen und transparent zu dokumentieren. Unternehmen, die bereits jetzt Informationssicherheit leben, über ein Datenschutz-Managementsystem verfügen und sich mit der Umsetzung der DS-GVO befassen, erfüllen bereits wesentliche Voraussetzungen.

Rahmenbedingungen
Art. 42 Abs. 7 DS-GVO weist darauf hin, dass eine Zertifizierung zeitlich begrenzt zu erteilen ist. So besteht eine Höchstdauer von drei Jahren, die bei Erfüllung der einschlägigen Voraussetzungen verlängert werden kann. Die zuständige Zertifizierungsstelle und die Aufsichtsbehörde können die Zertifizierung widerrufen, wenn die Voraussetzungen für die Zertifizierung

Ausblick zu Datenschutz-Zertifizierungen
Zertifizierungen nach der DS-GVO bieten das Potenzial, künftig bei Verarbeitungsvorgängen (u. a. bei Auftragsverarbeitung) Klarheit darüber zu verschaffen, ob die gesetzlichen Datenschutzanforderungen eingehalten werden. So können etwa Cloud-Dienste entscheidend profitieren, da deren Kunden und vor allem auch betroffene Personen sich selbst leichter ein Bild von einem bestimmten Produkt hinsichtlich der Einhaltung der DS-GVO machen können. Voraussetzung hierfür sind jedoch auf die DS-GVO ausgerichtete, praxistaugliche Zertifizierungsverfahren. Bei bestehenden Zertifizierungsverfahren muss zwangsläufig eine Überarbeitung hinsichtlich der neuen Vorgaben stattfinden.

Die Aufsichtsbehörden des Bundes und der Länder arbeiten derzeit intensiv an der Entwicklung abgestimmter, länderübergreifend geltender Kriterien, damit auch im Vollzug der Aufsichtsbehörden eine einheitliche Bewertung im Sinne der DS-GVO ermöglicht wird. Ein Wildwuchs zahlreicher unter-schiedlicher Zertifizierungsverfahren sollte gerade mit Blick auf ein einheitliches europäisches Datenschutzniveau im Interesse aller Beteiligten vermieden werden.

Anlage 70

Kurzpapier Nr. 10
Informationspflichten bei Dritt- und Direkterhebung

Dieses Kurzpapier der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) dient als erste Orientierung insbesondere für den nicht-öffentlichen Bereich, wie nach Auffassung der DSK die Datenschutz-Grundverordnung (DS-GVO) im praktischen Vollzug angewendet werden sollte. Diese Auffassung steht unter dem Vorbehalt einer zukünftigen – möglicherweise abweichenden – Auslegung des Europäischen Datenschutzausschusses.

Bedeutung der Informationspflichten
Die Informationspflichten bilden die Basis für die Ausübung der Betroffenenrechte (insbesondere der Art. 15 ff. DS-GVO). Nur wenn die betroffene Person weiß, dass personenbezogene Daten über sie verarbeitet werden, kann sie diese Rechte auch ausüben. Die Informationspflichten gemäß der DS-GVO gehen daher weit über die bisherige Rechtslage hinaus und müssen beachtet werden, sofern keine Ausnahmevorschriften greifen.

Die DS-GVO regelt die Informationsverpflichtungen des Verantwortlichen gegenüber der betroffenen Person in Abhängigkeit davon, ob personenbezogene Daten bei der betroffenen Person (**Direkterhebung**, Art. 13 DS-GVO) oder bei Dritten (**Dritterhebung**, Art. 14 DS-GVO) erhoben werden. Zu beachten ist, dass aus dieser Unterscheidung nicht pauschal abzuleiten ist, wer für die Information verantwortlich ist. Auch der Verantwortliche, der die Daten direkt bei der betroffenen Person erhoben hat, kann über Art. 13 DS-GVO hinaus zur Mitteilung nach Art. 14 Abs. 3 Buchstabe c DS-GVO verpflichtet sein, wenn er die Daten gegenüber einem anderen Empfänger offenbaren möchte.

Informationspflichten bei Direkterhebung
Bei der Informationspflicht im Falle der **Direkterhebung** wird zwischen den Informationen unterschieden, die der betroffenen Person mitzuteilen sind (Art. 13 Abs. 1 DGS-GVO) und solchen, die zur Verfügung zu stellen sind, um eine faire und transparente Verarbei-

tung der personenbezogenen Daten zu gewährleisten (Art. 13 Abs. 2 DS-GVO).

- Name (ggf. Firmenname gem. § 17 Abs. 1 HGB oder Vereinsname gem. § 57 BGB) und Kontaktdaten des Verantwortlichen sowie ggf. dessen Vertreter
- Kontaktdaten des ggf. vorhandenen Datenschutzbeauftragten
- Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen und zusätzlich die Rechtsgrundlage, auf der die Verarbeitung fußt
- das berechtigte Interesse, insofern die Datenerhebung auf einem berechtigten Interesse des Verantwortlichen oder eines Dritten beruht (Art. 6 Abs. 1 Buchstabe f DS-GVO)
- Empfänger oder Kategorien von Empfängern der personenbezogenen Daten (vgl. Art. 4 Nr. 9 DS-GVO)
- Absicht des Verantwortlichen, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln und zugleich Information, ob ein Angemessenheitsbeschluss der Kommission vorhanden ist oder nicht (bei Fehlen eines solchen Beschlusses ist auf geeignete oder angemessene Garantien zu verweisen und die Möglichkeit, wie eine Kopie von ihnen zu erhalten ist, oder wo sie verfügbar sind)

Zusätzlich sind nach Abs. 2 Informationen über

- die geplante Speicherdauer oder, falls dies nicht möglich ist, die Kriterien für die Festlegung der Speicherdauer,
- die Betroffenenrechte (Auskunfts-, Löschungs-, Einschränkungs- und Wider Widerspruchsrechte sowie das Recht auf Datenübertragbarkeit),
- das Recht zum jederzeitigen Widerruf einer Einwilligung und die Tatsache, dass die Rechtmäßigkeit der Verarbeitung auf Grundlage der Einwilligung bis zum Widerruf unberührt bleibt,
- das Beschwerderecht bei einer Aufsichtsbehörde,
- ggf. die gesetzliche oder vertragliche Verpflichtung des Verantwortlichen, personenbezogene Daten Dritten bereitzustellen und die möglichen Folgen der Nichtbereitstellung der personenbezogenen Daten und
- im Falle einer automatisierten Entscheidungsfindung (einschließlich Profiling) aussagekräftige Informationen über die

verwendete Logik, die Tragweite und angestrebten Auswirkungen einer derartigen Verarbeitung

zur Verfügung zu stellen.

Informationspflichten bei Dritterhebung

Auch im Falle einer **Dritterhebung** unterscheidet die DS-GVO zwischen mitzuteilenden Informationen (Art. 14 Abs. 1 DS-GVO) und zusätzlichen Informationen, die zur Gewährung einer fairen und transparenten Verarbeitung zur Verfügung zu stellen sind (Art. 14 Abs. 2 DS-GVO).

Art und Inhalt der mitzuteilenden bzw. der zur Verfügung zu stellenden Informationen entsprechen in wesentlichen Teilen denjenigen, die auch im Falle einer Direkterhebung mitgeteilt werden müssen.

Allerdings hat die betroffene Person im Gegensatz zur Direkterhebung nicht an der Datenerhebung mitgewirkt und somit auch keine Kenntnis darüber, welche personenbezogene Daten erhoben wurden. Daher ist der Verantwortliche nach Art. 14 Abs. 1 Buchstabe d DS-GVO verpflichtet, die Kategorien der verarbeiteten personenbezogenen Daten mitzuteilen. Diese Information muss so konkret sein, dass für den Betroffenen erkennbar wird, zu welchen Folgen die Verarbeitung führen kann. Nur dann kann er eine bewusste Entscheidung darüber treffen, ob er ergänzend von seinem Auskunftsrecht nach Art. 15 DS-GVO Gebrauch machen sollte.

Bei der Dritterhebung ist zudem nach Art. 14 Abs. 2 Buchstabe f DS-GVO die Datenquelle anzugeben und, ob es sich dabei um eine öffentlich zugängliche Quelle handelt. Stammen die Daten aus mehreren Quellen und kann die Herkunft nicht mehr eindeutig festgestellt werden, muss dennoch eine allgemeine Information gegeben werden.

Bei der Dritterhebung ist weiterhin zu beachten, dass Angaben über die berechtigten Interessen des Verantwortlichen oder eines Dritten (Art. 6 Abs. 1 Buchstabe f DS-GVO) nicht – wie bei der Direkterhebung – unter Abs. 1 fallen, sondern im Rahmen der zusätzlichen Informationen nach Abs. 2 zur Verfügung gestellt werden müssen (Art. 14 Abs. 2 Buchstabe b DS-GVO).

Zweckänderung und Übermittlung

Die Informationspflichten im Falle einer Zweckänderung gelten sowohl für die Direkterhebung als auch für die Dritterhebung. Neben der Information über die geänderte Zweckbestimmung sind alle

Informationspflichten gemäß Art. 13 Abs. 2 DS-GVO (Direkterhebung) oder gemäß Art. 14 Abs. 2 DS-GVO (Dritterhebung) erneut zu erfüllen.
Die Übermittlung an einen Dritten ist häufig eine Zweckänderung, so dass schon aus diesem Grund vor der Übermittlung die betroffene Person entsprechend zu informieren ist. Darüber hinaus stellt Art. 14 Abs. 3 Buchstabe c DS-GVO klar, dass bei der Offenlegung an einen neuen Empfänger (einschließlich Auftragsverarbeitern, vgl. Art. 4 Nr. 9 DS-GVO) informiert werden muss, soweit dieser nicht von der bereits nach Artikel 13 Abs. 1 Buchstabe e DS-GVO erteilten Information über Empfänger oder Empfängerkategorien umfasst ist.

Zeitpunkt der Erfüllung der Informationspflichten
Bei der **Direkterhebung** müssen die Informationen zum Zeitpunkt der Erhebung der Daten mitgeteilt bzw. zur Verfügung gestellt werden.
Im Falle der **Dritterhebung** ist der Verantwortliche verpflichtet, die Informationen nachträglich innerhalb einer angemessenen Frist nach Erlangung der Daten mitzuteilen (Art. 14 Abs. 3 DS-GVO). Diese Frist bestimmt sich nach den spezifischen Umständen, darf aber einen Monat nicht überschreiten. Die Monatsfrist ist eine Maximaldauer und sollte nicht pauschal angesetzt werden. Werden die personenbezogenen Daten zur Kommunikation mit der betroffenen Person verwendet, sind die Informationen spätestens zum Zeitpunkt der ersten Kontaktaufnahme mitzuteilen. Falls die Offenlegung an einen anderen Empfänger beabsichtigt ist, müssen die Informationen spätestens zum Zeitpunkt der ersten Offenlegung erteilt werden.

Ausnahmen
Die Informationspflichten nach den Art. 13 und 14 DS-GVO bestehen nicht, wenn und soweit die betroffene Person bereits über die Informationen verfügt. Im Falle der Dritterhebung bestehen darüber hinaus keine Informationspflichten, wenn die Informationserteilung sich z. B. als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordern würde, die Daten einem Berufsgeheimnis unterliegen oder die Erlangung durch Rechtsvorschrift ausdrücklich geregelt ist.
Außerdem sind in den §§ 32 und 33 des neuen Bundesdatenschutzgesetzes (BDSG-neu) weitere Ausnahmen von den Informationspflichten normiert. Die Informationspflicht nach Art. 13 DS-GVO

soll beispielsweise gem. § 32 Abs. 1 Nr. 4 BDSG-neu nicht bestehen, wenn die Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche beeinträchtigt würde und die Interessen des Verantwortlichen an der Nichterteilung der Information die Interessen der betroffenen Person überwiegen.
Es bestehen jedoch Zweifel, ob die in den §§ 32 und 33 BDSG-neu vorgesehenen Beschränkungen der Informationspflichten nach Art. 23 DS-GVO zulässig sind. Jedenfalls sind diese Regelungen grundsätzlich eng und im Sinne einer größtmöglichen Transparenz auszulegen. Ob und in welchem Umfang eine in den §§ 32 und 33 BDSG-neu vorgesehene Beschränkung der Informationspflichten aufgrund des Anwendungsvorrangs der DS-GVO tatsächlich angewendet werden kann, bleibt einer Entscheidung im jeweiligen konkreten Einzelfall vorbehalten.

Form der Informationspflicht
Gemäß Art. 12 Abs. 1 DS-GVO sind die Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form sowie in klarer und einfacher Sprache zu übermitteln. Die Informationen sind schriftlich oder in anderer Form (ggf. elektronisch) zur Verfügung zu stellen. Wird aber auf eine elektronisch verfügbare Information Bezug genommen, dann muss diese leicht auffindbar sein. Hierbei können auch Bildsymbole hilfreich sein.
Die leicht zugängliche Form bedeutet auch, dass die Informationen in der konkreten Situation verfügbar sein müssen. Sollen die Daten also von einer anwesenden Person erhoben werden, darf die Person in der Regel nicht auf Informationen im Internet verwiesen werden. Dies gilt gleichermaßen für eine schriftliche Korrespondenz auf dem Papierweg.

Nachweise der Informationspflichten
Der Verantwortliche hat im Hinblick auf das Transparenzgebot stets den Nachweis einer ordnungsgemäßen Erledigung der Informationspflichten zu erbringen (Art. 5 Abs. 1 Buchstabe a und Abs. 2 DS-GVO).

Folgen eines Verstoßes
Der Verstoß gegen die Informationspflichten kann nach Art. 83 Abs. 5 Buchstabe b DS-GVO mit einer Geldbuße bestraft werden.

Empfehlung
Es ist für Verantwortliche im eigenen Interesse ratsam, rechtzeitig die nach Art. 25 DS-GVO erforderlichen technischen und organisatorischen Maßnahmen für eine zügige und korrekte Erfüllung der Informationspflichten zu treffen.

Anlage 71

Kurzpapier Nr. 11
Recht auf Löschung / „Recht auf Vergessenwerden“

Dieses Kurzpapier der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) dient als erste Orientierung insbesondere für den nicht-öffentlichen Bereich, wie nach Auffassung der DSK die Datenschutz-Grundverordnung (DS-GVO) im praktischen Vollzug angewendet werden sollte. Diese Auffassung steht unter dem Vorbehalt einer zukünftigen – möglicherweise abweichenden – Auslegung des Europäischen Datenschutzausschusses.

Mit dem Inkrafttreten der DS-GVO erfährt die Löschung personenbezogener Daten gegenüber der bisherigen Rechtslage insofern eine Aufwertung, als die diesbezüglichen Bestimmungen detaillierter ausformuliert worden sind und zum Teil auch darüber hinausgehen. Das mit dem Löschungsanspruch der betroffenen Person verbundene „Recht auf Vergessenwerden“ wird zum ersten Mal ausdrücklich gesetzlich geregelt; es ergänzt die Löschung unmittelbar beim Verantwortlichen und die bereits bislang im BDSG verankerten Nachberichtspflichten.

Löschungspflicht
Wie aktuell in § 35 Abs. 2 BDSG-alt vorgesehen, bestimmt auch Art. 17 Abs. 1 DS-GVO, dass personenbezogene Daten auf Verlangen der betroffenen Person und/oder unter bestimmten Voraussetzungen ohne Verlangen der betroffenen Person eigenständig durch den Verantwortlichen unverzüglich gelöscht werden müssen. Art. 17 Abs. 1 DS-GVO benennt dazu folgende Fälle:

a) Die Notwendigkeit der Verarbeitung zur Zweckerreichung ist entfallen.
b) Die betroffene Person hat ihre Einwilligung widerrufen und es besteht auch keine sonstige Rechtsgrundlage.
c) Die betroffene Person legt gem. Art. 21 Abs. 1 oder 2 DS-GVO Widerspruch gegen die Verarbeitung ein; im Falle des Art. 21 Abs. 1 gilt dies nur, soweit keine vorrangigen berechtigten Gründe für die Verarbeitung vorliegen. Das Widerspruchsrecht

nach Art. 21 Abs. 1 DS-GVO besteht ausschließlich bei Verarbeitungen, die auf Art. 6 Abs. 1 Buchstabe e oder f DS-GVO gründen. Für die Löschungsverpflichtung bedarf es dabei einer Interessenabwägung. Anders bei Widersprüchen in Bezug auf Direktwerbung (Art. 21 Abs. 2 DS-GVO): Hier bedarf es keiner Interessenabwägung.

d) Die personenbezogenen Daten wurden unrechtmäßig verarbeitet.
e) Die Löschung ist zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erforderlich, dem der Verantwortliche unterliegt.
f) Die personenbezogenen Daten wurden in Bezug auf angebotene Dienste der Informationsgesellschaft gemäß Art. 8 Abs. 1 DS-GVO erhoben.

Der Verweis auf Art. 8 Abs. 1 DS-GVO (Einwilligung eines Kindes in Bezug auf Dienste der Informationsgesellschaft) impliziert, dass die Daten rechtmäßig erhoben wurden. Eine Löschungspflicht ergibt sich damit allein aufgrund des Löschungsverlangens der betroffenen Person. Weil Diensten der Informationsgesellschaft (z. B. Soziale Netzwerke, Online-Spiele) in Bezug auf Minderjährige weniger Schutzbedarf als den betroffenen Personen zugestanden wird, bedarf es neben dem Löschungsverlangen keiner weiteren Voraussetzung; auch kann dieser Anspruch noch als Erwachsener geltend gemacht werden.

Recht auf Vergessenwerden

Das „Recht auf Vergessenwerden“ gem. Art. 17 Abs. 2 DS-GVO bezieht sich, obwohl der Begriff im ErwGr. 65 als Synonym für „Löschung“ verwendet wird, auf die Tilgung (von Spuren) personenbezogener Daten, die durch Veröffentlichungen, insbesondere im Internet, einer breiten Öffentlichkeit zugänglich sind.

Der Verantwortliche, der die personenbezogenen Daten öffentlich gemacht hat und der gemäß Art. 17 Abs. 1 DS-GVO zu deren Löschung verpflichtet ist, hat unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten angemessene Maßnahmen, auch technischer Art, zu treffen, um für die Datenverarbeitung Verantwortliche, die die personenbezogenen Daten (gleichfalls) verarbeiten, darüber zu informieren, dass eine betroffene Person von ihnen die Löschung aller Links zu diesen personenbezogenen Daten

oder von Kopien oder Replikationen dieser personenbezogenen Daten verlangt hat.

Danach zieht der berechtigte Löschungsantrag einer betroffenen Person bzw. die bestehende Löschungspflicht eines Verantwortlichen dessen Pflicht nach sich, weitere Verantwortliche, die die zu löschenden Daten (noch) verarbeiten, über ein Verlangen des Betroffenen nach Löschung von Links, Kopien oder Replikationen zu informieren. Das Unterlassen entsprechender Bemühungen wird angesichts des Wortlauts der Norm und der fortlaufenden technischen Entwicklung nicht mit einem einfachen Verweis des Verantwortlichen auf unzumutbaren Aufwand begründet werden können.

Ausnahmen von der Löschungspflicht

Die Pflicht zur Löschung nach Art. 17 Abs. 1 und die Pflicht zur Information weiterer Verantwortlicher nach Art. 17 Abs. 2 DS-GVO entfallen, wenn gemäß Art. 17 Abs. 3 DS-GVO die Verarbeitung erforderlich ist

a) zur Ausübung des Rechts auf freie Meinungsäußerung und Information;
b) zur Erfüllung einer rechtlichen Verpflichtung, zur Wahrnehmung einer Aufgabe im öffentlichen Interesse oder zur Ausübung öffentlicher Gewalt;
c) aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit;
d) für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gem. Art. 89 Abs. 1 DS-GVO, soweit die Löschung die Verwirklichung dieser Ziele ernsthaft beeinträchtigt;
e) zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

Allerdings berechtigen die benannten Ausnahmen nicht zu einer zeitlich unbegrenzten Verarbeitung der jeweiligen personenbezogenen Daten. Auch diese Zwecke werden zu einem bestimmten Zeitpunkt erfüllt und die Verarbeitung der Daten wird zur Zweckerreichung nicht mehr erforderlich sein. Dann sind auch diese Daten zu löschen.

Nachberichtspflichten

Die bislang schon bestehenden Nachberichtspflichten zur Löschung (§ 35 Abs. 7 BDSG-alt) bleiben bestehen. Art. 19 DS-GVO verpflichtet den Verantwortlichen, allen Empfängern, denen personenbezogene Daten offengelegt wurden, jede Löschung der personenbezogenen mitzuteilen, es sei denn, dies erweist sich als unmöglich oder ist mit einem unverhältnismäßigen Aufwand verbunden.

Beschränkung des Löschungsanspruchs
Art. 23 DS-GVO befugt die Union und die Mitgliedstaaten, die Löschung gesetzlich zu beschränken, sofern eine solche Beschränkung den Wesensgehalt der Grundrechte und Grundfreiheiten achtet, eine notwendige und verhältnismäßige Maßnahme darstellt und (zumindest) einem der in Art. 23 Abs. 1 Buchstabe a bis j DS-GVO genannten Zwecke dient. Hiervon hat der Bundesgesetzgeber in § 35 BDSG-neu Gebrauch gemacht: Im Fall nicht automatisierter Datenverarbeitung und unter den weiteren dort genannten Voraussetzungen ist statt des Löschungsanspruchs der betroffenen Person ein Anspruch auf Einschränkung der Verarbeitung gemäß Art. 18 DS-GVO vorgesehen.

Anwendbarkeit der Regelungen des BDSG-neu
Es bestehen jedoch Zweifel, ob die in § 35 BDSG-neu vorgesehenen Beschränkungen des Rechts auf Löschung nach Art. 23 DS-GVO zulässig sind. Jedenfalls sind diese Regelungen grundsätzlich eng und im Sinne einer größtmöglichen Transparenz auszulegen. Ob und in welchem Umfang eine in § 35 BDSG-neu vorgesehene Beschränkung des Rechts auf Löschung aufgrund des Anwendungsvorrangs der DS-GVO tatsächlich angewendet werden kann, bleibt einer Entscheidung im jeweiligen konkreten Einzelfall vorbehalten.

Sanktionen
Bei Verstößen gegen die Löschungs- oder Nachberichtspflichten droht die Einleitung eines Bußgeld-verfahrens (Art. 83 Abs. 5 Buchstabe b DS-GVO).

Abkürzungsverzeichnis

Abs.	Absatz
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
AfA	Amt für Ausbildungsförderung
AfV	Amt für Verfassungsschutz
AK	Arbeitskreis
AO	Abgabenordnung
App	Applikation
Art.	Artikel
AsylbLG	Asylbewerberleistungsgesetz
ATDG	Antiterrordateigesetz
Az.	Aktenzeichen
BAföG	Bundesausbildungsförderungsgesetz
BAFzA	Bundesamt für Familie und zivilgesellschaftliche Aufgaben
BAG	Bundesarbeitsgericht
BayLDA	Bayerischer Landesbeauftragter für den Datenschutz
bDSB	Beauftragte/r für den Datenschutz
BDSG	Bundesdatenschutzgesetz
bDSG	behördlicher Datenschutzbeauftragter
BeamtStG	Beamtenstatusgesetz
BEEG	Bundeselterngeld- und Elternzeitgesetz
BfB	Bündnis für Bildung
BfDI	Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
BGB	Bürgerliches Gesetzbuch
BGH	Bundesgerichtshof
BKAG	Bundeskriminalamtgesetz
BLK	Bund-Länder-Kommission

BMAS	Bundesministerium für Arbeit und Soziales
BMBF	Bundesministerium für Bildung und Forschung
BMFSFJ	Bundesministerium für Familie, Senioren, Frauen und Jugend
BMG	Bundesmeldegesetz
BMI	Bundesministerium des Innern
BMJV	Bundesministerium der Justiz und für Verbraucherschutz
BNetzA	Bundesnetzagentur
BR-Drs.	Bundesrat-Drucksache
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSI-KritisV	BSI-Kritisverordnung
BtM	Betäubungsmittel
BVerfG	Bundesverfassungsgericht
BZÄK	Bundeszahnärztekammer
bzgl.	bezüglich
CAN	Controller-Area-Network
d. h.	das heißt
DA	Dienstanweisung
DA AvTgi-ThPol	Dienstanweisung "Aufzeichnung von Telefongesprächsinhalten in der Thüringer Polizei"
DAkkS	Deutsche Akkreditierungsstelle GmbH
DFI	Dynamische Fahrgastinformationsanzeiger
DSAnpUG-EU	Datenschutz-Anpassungs- und Umsetzungsgesetz EU
DSFA	Datenschutz-Folgenabschätzung
DS-GVO	Datenschutz-Grundverordnung
DSK	Datenschutzkonferenz
DV	Dienstvereinbarung
e. V.	eingetragener Verein

eAkte	elektronische Akte
EDSA	Europäischer Datenschutzausschuss
EES	Entry-Exit-System
EG	Erwägungsgrund
eGK	elektronische Gesundheitskarte
eID	elektronische Identifikationsmöglichkeit
ESF	Europäischer Sozialfond
EstG	Einkommenssteuergesetz
ESU	Einschulungsuntersuchung
ETIAS	Reiseinformations- und -genehmigungssystem
EU	Europäische Union
EuGH	Europäischer Gerichtshof
FA	Finanzamt
FBS-TH	Fallbearbeitungssystem Thüringen
FDR	Falldatei Rauschgift
FH	Fachhochschule
FlugDaG	Fluggastdatengesetz
FPStaG	Finanz- und Personalstatistikgesetz
FSU	Friedrich-Schiller-Universität
FZA	Funkzellenabfrage
G-BA	Gemeinsamer Bundesausschuss
gem./Gem.	gemäß/Gemäß
GenDG	Gendiagnostikgesetz
GFAW	Gesellschaft für Arbeits- und Wirtschaftsförderung des Freistaates Thüringen mbH
GG	Grundgesetz
ggf.	gegebenenfalls
GKDZ	Gemeinsames Kompetenz- und Dienstleistungszentrum
GKR	Gemeinsames Krebsregister
GmbH	Gesellschaft mit beschränkter Haftung

GOLT	Geschäftsordnung des Thüringer Landtags
GRCh	Grundrechtecharta
GS-EWS	Gebührensatzung zur Entwässerungssatzung des Zweckverbandes
HeimPersV	Heimpersonalverordnung
HmbBfDI	Hamburgischer Beauftragte für Datenschutz und Informationsfreiheit
i. d. R.	in der Regel
i. S. d.	im Sinne des/der
i. V. m.	in Verbindung mit
IBIS	Integriertes Bordinformationssystem
IfSG	Infektionsschutzgesetz
IGVP	Integrationsverfahren Polizei
IMI	Binnenmarktinformationssystem
INPOL	Informationssystem der Polizei
InsO	Insolvenzordnung
InsOBekV	Verordnung zu öffentlichen Bekanntmachungen in Insolvenzverfahren
ITP	Integrierte Teilhabeplanung
JVA	Justizvollzugsanstalt
JVEG	Justizvergütungs- und -entschädigungsgesetz
KFRG	Krebsfrüherkennungs- und -registergesetz
KfZ	Kraftfahrzeug
KITA	Kindertagesstätte
KJÄD	Kinder- und Jugendärztlicher Dienst
KK	Krankenkasse
KMK	Kultusministerkonferenz
KoWo	Kommunale Wohnungsgesellschaft
KV	Kassenärztliche Vereinigung
LEZ	Landeseinsatzzentrale
LFD	Landesfinanzdirektion

LfDI Bremen	Bremer Landesbeauftragte für Datenschutz und Informationsfreiheit
LKHG	Landeskrankenhausgesellschaft Thüringen
LPD	Landespolizeidirektion
LPI	Landespolizeiinspektion
LQS	Landesgeschäftsstelle für Qualitätssicherung
LRA	Landratsamt
LZÄKTh	Landeszahnärztekammer Thüringen
MB-APrV	Ausbildungs- und Prüfungsverordnung für Masseure und medizinische Bademeister
MDA-Geräte	Mobile Datenerfassungsgeräte
MDK	Medizinischer Dienst der Krankenkassen
MDR	Mitteldeutscher Rundfunk
MZG	Mikrozensusgesetz
NetzDG	Netzwerkdurchsetzungsgesetz
NIS	Netz- und Informationssysteme
Nr.	Nummer
NRW	Nordrhein-Westfalen
o. ä.	oder ähnliches
o. g.	oben genannt(e, es, er)
OBG	Ordnungsbehördengesetz
ÖGB	Öffentlich geförderte Beschäftigung
OH	Orientierungshilfe
OLG	Oberlandesgericht
ÖPNV	Öffentlicher Personennahverkehr
OWiG	Ordnungswidrigkeitengesetz
OZG	Onlinezugangsgesetz
PAG	Polizeiaufgabengesetz
PAuswG	Personalausweisgesetz
PI	Polizeiinspektion
PIAV	Polizeilicher Informations- und Analysever-

	bund
PlanQI-RL	Richtlinie zu planungsrelevanten Qualitätsindikatoren
PNR	Passenger Name Records
QSKH-RL	Richtlinie über Maßnahmen der Qualitätssicherung in Krankenhäusern
Rdnr.	Randnummer
RiStBV	Richtlinien für das Strafverfahren und das Bußgeldverfahren
RZ	Randziffer
SächsDSDG	Sächsisches Datenschutzdurchführungsgesetz
SCA	Stored Communication Act
SGB	Sozialgesetzbuch
SpielhG He	Spielhallengesetz Hessen
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
StVG	Straßenverkehrsgesetz
StVO	Straßenverkehrsordnung
TAB	Thüringer Aufbaubank
TB	Tätigkeitsbericht
ThAVEL	Thüringer Antragssystem für Verwaltungsleistungen
ThEx	Thüringer Zentrum für Existenzgründungen und Unternehmertum
ThILLM	Thüringer Institut für Lehrerfortbildung, Lehrplanentwicklung und Medien
ThürAGSGB II	Thüringer Ausführungsgesetz des SGB II
ThürBestG	Thüringer Bestattungsgesetz
ThürBG	Thüringer Beamtengesetz
ThürBO	Thüringer Bauordnung
ThürDG	Thüringer Disziplinargesetz
ThürDSAnpUG	Thüringer Datenschutz-Anpassungs- und Umsetzungsgesetz

ThürDSG	Thüringer Datenschutzgesetz
ThürDSG-E	Neufassung des Thüringer Datenschutzgesetzes
ThürHDatVO	Thüringer Hochschul-Datenschutzverordnung
ThürHeilBG	Thüringer Heilberufegesetz
ThürHG	Thüringer Hochschulgesetz
ThürIFG	Thüringer Informationsfreiheitsgesetz
ThürImO	Thüringer Immatrikulationsordnung
ThürJVollzGB	Thüringer Justizvollzugsgesetzbuch
ThürKAG	Thüringer Kommunalabgabengesetz
ThürKGG	Thüringer Gesetz über die kommunale Gemeinschaftsarbeit
ThürKHG	Thüringer Krankenhausgesetz
ThürKJHAG	Thüringer Kinder- und Jugendhilfe-Ausführungsgesetz
ThürKO	Thüringer Kommunalordnung
ThürKRG	Thüringer Krebsregistergesetz
ThürLaufbG	Thüringer Laufbahngesetz
ThürMeldeVO	Thüringer Meldeverordnung
ThürPAG	Thüringer Polizeiaufgabengesetz
ThürPersVG	Thüringer Personalvertretungsgesetz
ThürRettG	Thüringer Rettungsdienstgesetz
ThürSchAG	Thüringer Gesetz über die Schulaufsicht
ThürSchFG	Thüringer Schulfinanzierungsgesetz
ThürSchulG	Thüringer Schulgesetz
ThürSchulgespfl-VO	Thüringer Verordnung über die Schulgesundheitspflege
ThürSchulO	Thüringer Schulordnung
ThürUIG	Thüringer Umweltinformationsgesetz
ThürVerfSchG	Thüringer Verfassungsschutzgesetz
ThürVwVfG	Thüringer Verwaltungsverfahrensgesetz
ThürWTG	Thüringer Wohn- und Teilhabegesetz

TIM	Thüringer Innenministerium
TKG	Telekommunikationsgesetz
TLfD	Thüringer Landesbeauftragter für den Datenschutz
TLfDI	Thüringer Landesbeauftragter für den Datenschutz und die Informationsfreiheit
TLKA	Thüringer Landeskriminalamt
TLM	Thüringer Landesmedienanstalt
TLRZ	Thüringer Landesrechenzentrum
TLS	Thüringer Landesamt für Statistik
TLV	Thüringer Landesamt für Verbraucherschutz
TLVwA	Thüringer Landesverwaltungsamt
TMASGFF	Thüringer Ministerium für Arbeit, Soziales, Gesundheit, Frauen und Familie
TMBJS	Thüringer Ministerium für Bildung, Jugend und Sport
TMBWK	Thüringer Ministerium für Bildung, Wissenschaft und Kunst
TMG	Telemediengesetz
TMIK	Thüringer Ministerium für Inneres und Kommunales
TMIL	Thüringer Ministerium für Infrastruktur und Landwirtschaft
TMMJV	Thüringer Ministerium für Migration, Justiz und Verbraucherschutz
TMWWDG	Thüringer Ministerium für Wirtschaft, Wissenschaft und Digitale Gesellschaft
TOMs	technische und organisatorische Maßnahmen
TU	Technische Universität
u. a.	unter anderem
u. U.	unter Umständen
UAbs.	Unterabsatz
UAK	Unterarbeitskreis
usw.	und so weiter

VA	Verwaltungsakt
VBS	Vorgangsbearbeitungssystem
VDG	Vertrauensdienstegesetz
VDV	Verband Deutscher Verkehrsunternehmen
VG	Verwaltungsgericht
VG	Verwaltungsgemeinschaft
vgl.	vergleiche
VoIP	Voice over IP
VwGO	Verwaltungsgerichtsordnung
WaffG	Waffengesetz
WEG	Wohnungseigentumsgesetz
z. B.	zum Beispiel
ZStV	Zentrales Staatsanwaltschaftliches Verfahrensregister

Stichwortverzeichnis/Index

§ 163 StPO 8.19
§ 34 ThürDSG 7.5
§ 47 PAG 8.8
Abfotografieren 16.42, 6.45
Abfragen 12.36, 8.14, 6.32, 3.4
Abgabenordnung 6.48, 6.36
Ablichtung 8.7
Abrechnungsstempel 12.11
Abrufbarkeit 6.39
Abwahlantrag gegen einen Bürgermeister 6.15
Abwehr erheblicher Nachteile 12.11, 11.1
Abwesenheit 7.7
Adressierung 7.16
Adressliste 16.24, 11.10
Adressmittlungsverfahren 14.2
Agentur für Arbeit 12.19
Ahndung 6.43, 6.42, 5.4, 3.3
Akten 16.24, 15.4, 15.2, 13.5, 12.44, 12.28, 12.26, 12.25, 11.7, 11.4, 8.20, 8.2, 7.2, 6.45, 6.44, 6.36, 6.25
Akteneinsicht 16.39, 12.16, 12.13, 11.5, 7.2, 6.44, 6.34, 6.25
Aktenentsorgung 16.24
Aktenlager 8.1
Altdatensatz 2.5
Alternative zu WhatsApp 16.7
Ältestenrat 5.4
Amt für Ausbildung 16.26
Amt für Ausbildungsförderung 16.25
Amt für Grundsicherung 12.25
Amt für Verfassungsschutz 19.1, 9.2, 6.1
Amtsarzt 16.43, 12.10, 7.4
amtsärztliches Gutachten 7.4
Amtsblätter 6.16, 6.3
Amtsgericht 17.2, 11.7, 8.17, 8.16, 7.16, 6.46, 6.44
Amtshilfe 8.1
Anamnese 16.41, 16.33, 7.4
Anerkennungsgesetz 15.3
Angehörige 12.39, 12.5
Anmeldeverfahren 16.22

anonymisierte Patientendaten 12.1
Anonymisierung 17.6, 12.40, 12.20
Anonymisierung Schulnoten 16.14
Anonymität 7.12, 6.44
Antiterrordatei 9.2
Antrag 16.33, 16.17, 15.2, 13.7, 13.4, 12.40, 12.39, 12.37, 12.36, 12.22, 12.19, 12.16, 11.2, 11.1, 8.20, 7.13, 7.9, 7.2, 6.46, 6.41, 6.20, 6.15, 5.2
Antragsteller 16.26, 16.25, 15.3, 13.7, 13.6, 13.4, 12.36, 12.27, 12.26, 12.25, 12.22, 11.9, 11.2, 8.16, 8.8, 6.46, 6.38, 6.25, 6.15
Antragstellung 16.25, 12.27, 6.51
Anwendungsvorrang 3.2
Anwesenheit 7.7
Anwohner 13.4, 6.11
Anwohnerparkzone 13.4
Anzeige 18.6, 17.6, 12.7, 8.22, 8.18, 6.50, 6.44
Apotheke 12.11
Apothekerkammer 12.11
Approbation 12.36, 12.33, 12.12
Apps 18.5, 12.3, 2.1
Arbeitskreis Datenschutz und Bildung 2.1
Arbeitslosengeld II 12.26
Arbeitsmedizin 12.44
Arbeitsplattform 15.1
Arbeitsrecht 11.1, 7.17, 7.8
Arbeitsuchende 12.28, 12.26, 12.19, 12.8
Arbeitsunfähigkeitsbescheinigung 16.16
Arbeitsvermittlung 12.4
Arbeitszeit 15.2, 12.42, 8.16, 7.11, 7.5, 7.4
Arbeitszeitdaten 7.7, 7.5
Archiv 16.23, 12.10
ARD und ZDF 6.20, 6.19, 6.19, 4.4
Artikel 29-Gruppe 3.4
Artikel 31-Ausschuss 3.4
Arzt 16.43, 16.16, 12.44, 12.38, 12.37, 12.33, 12.29, 12.12, 12.11, 12.10, 12.1, 7.3, 7.1, 6.34, 6.33
ärztliche Bescheinigung 7.1
Arztstempel 12.11, 7.1
Asyl 6.33
Asylsuchende 6.26

Aufbewahrung 16.42, 15.2, 7.9
Aufbewahrungsfrist 16.23, 15.2, 12.44, 12.10, 7.9, 7.2
Aufgabenerfüllung 16.33, 16.25, 16.17, 16.15, 15.2, 12.43, 12.26, 12.25, 12.24, 12.19, 12.18, 12.16, 12.7, 12.6, 11.2, 8.18, 7.16, 7.15, 7.13, 7.7, 7.6, 7.5, 7.3, 7.2, 7.1, 6.32, 6.3, 6.1, 2.4
Aufklärungsinstrumente des TLfDI 6.37
Auflagen 12.40, 6.30
Aufrufanlage 6.17
Auftragsdatenverarbeitung 16.35, 16.27, 16.18, 16.9, 15.1, 14.3, 13.5, 12.41, 12.40, 12.20, 10.1, 8.4, 6.47, 6.4, 4.2, 3.4, 3.1
Aufzeichnung 12.3, 8.5, 8.2, 7.10, 6.13, 5.2
Ausbildung 16.39, 12.43, 12.41, 12.40, 11.9, 7.11, 6.26, 2.2
Ausbildungsförderung 16.25
Ausgrenzung 16.38
Auskunft 16.43, 16.42, 16.40, 16.38, 16.33, 16.32, 16.23, 16.22, 16.15, 16.2, 13.7, 13.4, 13.1, 12.42, 12.33, 12.32, 12.28, 12.24, 12.21, 12.19, 12.17, 12.15, 12.11, 12.7, 8.20, 8.17, 8.11, 7.16, 7.13, 7.8, 7.7, 7.4, 7.3, 6.47, 6.43, 6.38, 6.33, 6.27, 6.20, 6.19, 6.8, 5.2, 4.4, 2.1
Auskünfte 12.39
Auskunfts- und Recherchesysteme 8.14
Auskunftsanspruch 16.42, 12.17, 8.20, 5.2, 3.1
Auskunftsbegehren 7.6, 6.20, 5.2
Auskunftsersuchen 16.14, 12.18, 8.20, 8.19, 8.8, 6.20
Auskunftspflicht 16.33, 16.32, 12.18, 2.3
Auskunftsrecht 18.5, 8.20, 5.2, 3.4, 3.1
Auskunftsverpflichtung 5.2
Ausnahme 16.38, 16.37, 16.3, 12.32, 11.7, 11.1, 8.16, 6.49, 6.44, 6.38, 6.15, 6.1, 4.5, 3.4, 3.3, 3.2
Auspixeln 6.3
Ausschlussgründe 5.2
Außendienst 12.42, 7.5
Ausübung der gemeinsamen Sorge bei Getrenntleben 6.8
Ausweisinhaber 8.7
Auswertung 18.5, 16.39, 16.2, 13.3, 12.40, 12.20, 12.1, 8.13, 8.12, 8.5, 7.16, 7.14, 7.10, 7.6, 6.50, 6.4
Auswertungsstelle 12.1
Authentizität 16.36, 16.35
automatisierte Verfahren zur Arbeitszeiterfassung 7.5
BAföG 16.26, 16.25

Bagatellkriminalität 8.6
Bankverbindung 6.47, 6.29
Baulastenverzeichnis 13.6
bDSB 16.39, 16.23, 16.18, 16.13, 13.7, 13.5
Beamtenstatusgesetz 16.17, 6.36
Beanstandung 16.29, 16.17, 16.15, 16.3, 14.2, 12.42, 12.16, 12.15, 11.5, 8.22, 8.17, 8.15, 7.17, 7.8, 7.6, 7.4, 7.3, 7.2, 6.42, 6.34, 6.25, 6.8, 6.6, 6.1, 3.3, 1
Beendigung des Beschäftigtenverhältnisses 7.8
Beförderung 11.9
beglaubigte Kopie 8.8
Behinderung 16.32, 15.1, 12.34, 12.18, 12.16, 12.6, 7.13, 7.11
Behörde 20, 18.6, 18.5, 18.3, 17.1, 16.39, 16.27, 16.25, 16.11, 16.7, 15.4, 15.2, 14.2, 13.7, 13.4, 12.36, 12.25, 12.18, 12.10, 11.7, 11.6, 10.1, 9.2, 8.20, 8.19, 8.18, 8.13, 8.6, 8.2, 7.17, 7.16, 7.14, 7.12, 7.5, 6.51, 6.43, 6.41, 6.40, 6.38, 6.36, 6.33, 6.29, 6.27, 6.25, 6.20, 6.14, 6.9, 6.8, 6.7, 6.6, 6.1, 5.2, 3.6, 3.5, 3.4, 3.3, 3.2, 1
Behördenleiter 18.1, 12.21, 6.7
behördlicher Datenschutzbeauftragter 16.39, 16.20, 16.18, 16.13, 13.7, 13.5, 13.3, 11.7, 11.7, 7.14, 7.12, 7.6, 7.3, 6.5, 3.1
Beiakte 7.9, 7.3
Beihilfestelle 12.32
Beitrag 12.24, 6.16, 6.7
Beitragsservice 6.20, 6.19, 4.4
Beitragsservice von ARD, ZDF und Deutschlandradio 6.20
Bekanntgabe 16.38, 16.19, 11.1, 9.1, 8.22, 7.14, 6.41, 6.29, 6.15
Bekanntgabe eines Nebenkostenschuldners 6.22
Belehrungen 18.1, 16.17, 8.14
Benutzer-Account 16.22
Beratungsfunktion 14.3, 7.10
berechtigte Interessen Einzelner 6.15
berechtigtes Interesse 16.32, 13.6, 11.5, 8.22, 6.15, 2.4
Berichterstattung 12.4, 9.1, 8.22, 6.2
Berufsanerkennung 16.39, 12.36
Berufsgeheimnisträger 8.5, 3.2
Berufsgenossenschaft 12.23
Berufsordnung 12.44
Berufsqualifikationsfeststellungsgesetz 15.3
Berufsschule 6.9
Berufsunfall 12.23

Berufsverband 16.20
Berufsverbot 15.3, 7.6
Beschäftigte 16.20, 16.7, 15.2, 13.1, 12.42, 11.7, 8.16, 8.3, 7.15, 7.14, 7.12, 7.11, 7.10, 7.8, 7.7, 7.6, 7.3, 7.2, 6.4, 3.6
Beschäftigtendaten 7.12, 7.6, 7.3
Beschäftigtendatenschutz 7.15, 3.6, 3.2
Beschäftigtenverhältnis 7.7, 7.6
Beschäftigungsverbot 7.1
Beschäftigungsverhältnis 8.12, 7.8
Bescheid 16.39, 16.26, 11.2, 6.30, 6.25
Beschwerde 16.38, 16.26, 16.16, 16.3, 12.37, 12.34, 12.26, 12.25, 12.19, 12.16, 12.15, 11.5, 8.16, 8.14, 7.15, 7.9, 7.4, 7.1, 6.46, 6.45, 6.40, 6.39, 6.37, 6.29, 6.23, 6.15, 6.10, 5.4, 5.3, 4.5, 4.3, 3.6, 3.4
Besichtigungstermin 6.32
Bestellung 13.1, 11.7, 6.49, 4.5, 3.1
Bestimmtheit 8.5
Besucher 14.1, 13.4, 7.12, 6.9, 5.1
Betäubungsmittelgesetz 8.18, 8.14, 8.6
Betreuung 16.40, 15.1, 12.10, 6.8
Betriebsambulatorium 12.44
Betriebshof 6.4
Betriebsvereinbarung 6.4
Betroffenenrechte 16.38, 3.4, 3.2, 3.1
Bevollmächtigung 12.16, 8.17
Bewegungsdaten 6.4
Bewerbung 12.7, 7.17, 7.15
Bezirksschornsteinfeger 14.2
BfDI 16.2, 12.23, 12.19, 12.8, 11.6, 11.3, 2.3
BGB 12.38, 12.17, 6.8
Biene Maja 6.17
Big Data 16.28
Bild- und Tonaufzeichnungen 8.5, 6.14, *6.*12, 6.2
Bilder 16.4, 16.3, 14.1, 13.3, 11.5, 6.13, 5.4
Bildung und Teilhabe 16.38
Bildungs- und Lehrpläne 16.10
Binnenmarktinformationssystem (IMI) 15.3
Biometrie 17.5
blaue Tonne 6.5
Blindkopie 8.15
Bodycam 8.5

Boot-Stick 11.4
Botnetz 4.6
Brennstoffe 14.2
Brief 16.22, 16.17, 12.37, 8.18, 7.16
Bring Your Own Device (BOYD) 2.1
BSI-Gesetz 17.4
BSI-Kritisverordnung 18.4
bulk collection 3.4
Bundesagentur für Arbeit 12.28, 12.26, 12.19, 12.8
Bundesamt für Justiz 11.6
Bundesausbildungsförderungsgesetz 16.26, 16.25
Bundeskriminalamt 9.2, 8.6
Bundesmeldegesetz 6.43, 6.19, 4.4, 2.5
Bundesnaturschutzgesetz 14.4
Bundesrat 17.1, 3.2, 3.1
Bundesregierung 8.9, 3.5
Bundesstatistik 12.30
Bundestag 5.1, 3.2, 3.1, 2.3
bundesunmittelbare Körperschaft 12.23
Bundeszahnärztekammer 12.7
Bund-Länder-Kommission für Informationstechnik in der Justiz 11.3
Bündnis für Bildung 16.5
Bürgerliches Gesetzbuch 12.38, 12.17, 6.47, 6.8
Bürgermeister 7.17, 7.14, 7.8, 7.7, 7.3, 6.45, 6.37, 6.36, 6.24, 6.15, 6.6, 6.5
Bürgerversammlung 6.45
Bußgeldbescheid 8.14
Bußgelder 3.1
Bußgeldverfahren 11.2, 6.44
Cambridge Analytica 16.28
Canvas-Blocker 17.6
CDU 8.1
Cloud 12.31, 12.5
Cloud-Dienste 2.1
Cloud-Nutzung 16.9
Code 16.22
Controlling 12.42
Cookie-Richtlinie 4.1
Cowboy 8.17
Darlehen 12.8

Data protection by default 18.5
Data protection by design 18.5
Daten verarbeitende Stelle 16.20, 16.18, 16.17, 16.12, 16.4, 15.4, 12.42, 12.6, 11.7, 8.14, 6.25, 6.20, 6.4, 5.2, 2.5
Datenabruf 6.39
Datenaustausch 12.34, 12.25, 12.16, 12.4, 3.5
Datenbank 14.3, 8.12, 8.6, 7.13
Datenerhebung 14.3, 14.2, 13.7, 12.33, 12.31, 12.24, 12.23, 12.7, 11.5, 8.19, 8.15, 8.14, 8.2, 7.3, 6.48, 6.34, 6.32, 6.28, 6.22, 6.8, 6.3, 6.1, 5.3, 3.4
Datengeheimnis 16.17, 16.16, 12.13, 8.14
Datenlöschung 18.5, 11.6, 6.30, 6.16, 3.1
Datenminimierung 15.2, 3.1
Datenportabilität 3.1
Datenschutz und Schule 16.11, 16.10, 16.4, 2.1
Datenschutzbeauftragter 18.3, 18.1, 17.5, 17.2, 16.39, 16.20, 16.18, 16.15, 16.13, 16.10, 16.5, 16.4, 16.2, 16.1, 13.7, 13.5, 13.4, 13.3, 13.1, 12.38, 12.36, 12.2, 11.7, 9.2, 8.19, 8.6, 8.5, 7.14, 7.7, 7.6, 7.3, 6.51, 6.49, 6.47, 6.38, 6.20, 6.9, 6.5, 4.5, 4.3, 4.1, 3.4, 3.3, 3.2, 3.1, 2.3, 2.1
Datenschutzerklärung 6.32, 6.28
Datenschutz-Folgenabschätzung 10.1, 3.1
Datenschutz-Grundverordnung 18.5, 16.9, 16.1, 15.2, 12.38, 10.1, 4.5, 4.1, 3.6, 3.3, 3.2, 3.1, 2.4, 2.1
datenschutzrechtliche Beratung 16.30, 15.1, 7.11
Datenschutzrichtlinie 7.9, 3.2, 3.1
Datenschutzverordnung 12.3
Datensicherheit 18.6, 18.5, 17.5, 16.37, 16.22, 16.20, 16.11, 16.9, 16.6, 16.5, 12.12, 12.3, 8.4, 6.32, 3.1, 2.2
Datensparsamkeit 18.5, 16.34, 16.27, 15.2, 12.3, 8.10, 7.5, 6.17, 6.6, 3.1
Datenspeicherung 15.2, 14.3, 8.4, 8.2, 6.25, 6.1
Datenträger 16.24, 12.29, 11.5, 8.3
Datenübermittlung 16.39, 16.34, 16.32, 16.26, 16.2, 15.4, 15.3, 12.41, 12.34, 12.24, 12.21, 12.16, 12.11, 12.8, 12.7, 12.4, 11.2, 8.22, 8.19, 8.18, 8.15, 8.8, 8.4, 7.17, 7.12, 7.7, 7.5, 6.46, 6.43, 6.41, 6.40, 6.38, 6.34, 6.31, 6.29, 6.27, 6.21, 6.19, 6.16, 6.7, 6.6, 6.1, 4.4, 3.4, 2.5
Datenübermittlung aus Kraftfahrzeugen 6.50
Datenverarbeitungsprogramm 12.42, 11.7, 8.17

Datenverarbeitungsprozesse 16.8, 16.4
Datenvermeidung 15.2, 12.3, 3.1
Demokratieverständnis 6.6
deutsche Cloud 16.4
Device Watch 1
DeviceWatch 19.1, 8.3
Diebstahl 16.13
Dienstanweisung 16.24, 16.3, 8.12, 8.2, 7.10, 6.34, 6.31, 6.3, 1
Dienstaufsichtsbeschwerde 12.16, 7.16
Dienstberatung 16.3, 12.42
Dienst-Laptop 6.37
dienstliche Kenntnis 12.16
dienstliche Kommunikation 16.29, 16.15, 16.7
dienstliches Schriftgut 6.5
Dienstrecht 7.17
Dienstvereinbarung 12.42, 12.38, 8.12, 7.14, 7.10, 7.7, 7.5
Dienstvorgesetzter 12.16, 7.16, 7.9, 6.36
digitale Assistenzsysteme 12.31
digitale Bildungsmaterialien 16.5
digitale Kompetenz 18.1
Diskussion 16.11, 16.4, 7.12, 2.2, 2.1
Disziplinarverfahren 8.14, 7.9
DNA 8.12
Dokumentation 16.37, 16.13, 16.3, 12.33, 12.29, 12.14, 12.1, 8.2, 6.25, 6.9, 3.1
Dokumentationspflicht 18.5, 16.42
Dokumentenmanagementsystem 10.1
DS-GVO 18.5, 18.3, 16.9, 16.1, 15.2, 12.38, 12.3, 10.1, 4.5, 4.1, 3.6, 3.2, 3.1, 2.4, 2.1
DSK 13.7, 8.6, 3.2, 3.1
dynamische IP-Adresse 17.2
e-Datenschutz-Richtlinie 4.1
Edwards Snowden 3.4
E-Government 18.1, 17.1, 10.1, 1
Ehegatte 12.18
Ehemann 16.26, 6.27
Ehepartner 12.18, 12.15
eID 6.51
eIDAS-Durchführungsgesetz 17.3
eIDAS-Verordnung 17.3

Eigenbetrieb 12.28, 12.4
Eigentümer 18.5, 14.3, 14.2, 11.10, 6.22, 4.6
Eigentümergemeinschaft 11.10, 6.22
Einbrecher 12.44
Einbruch 16.13
Eingruppierungen 15.2
Einkommen 16.26, 16.26, 12.25, 12.24, 12.22, 12.17, 6.32
Einkommens- und Vermögensverhältnisse 12.17
Einkommensteuer 12.24
Einlasskontrolle 6.9, 5.1
Einsatzfahrzeuge 6.4
Einschulungsuntersuchung 16.41, 12.10
Einsichtnahme 16.42, 16.39, 16.25, 13.6, 12.39, 12.13, 11.5, 11.3, 7.15, 7.2, 6.44
Einsichtsmöglichkeit 11.9
Einwilligung 18.5, 17.2, 16.40, 16.37, 16.36, 16.35, 16.31, 16.27, 16.15, 16.14, 16.11, 16.3, 14.4, 14.3, 13.6, 13.3, 12.43, 12.41, 12.38, 12.34, 12.30, 12.23, 12.17, 12.9, 12.7, 12.5, 12.4, 11.5, 11.1, 8.22, 8.18, 8.15, 8.12, 8.7, 8.2, 7.12, 7.10, 7.8, 7.7, 7.6, 6.47, 6.37, 6.32, 6.28, 6.27, 6.26, 6.21, 6.15, 6.13, 6.8, 6.7, 4.1, 3.6, 3.2, 3.1
Einwilligungserklärung 16.40, 16.3, 12.41, 12.41, 12.38, 12.23, 12.7, 12.3, 11.5, 8.15, 6.32, 6.28, 6.26
Einwilligungsformular 8.12
Einwohnerversammlung 6.45
E-Learning-Plattform 17.5
elektronische Akte 12.27, 12.14, 11.4, 10.1
elektronische Anzeigetafel 6.17
elektronische Fußfessel 8.9
elektronische Gesundheitskarte 12.14, 6.33
elektronische Kommunikationssysteme 7.14
Eltern 16.42, 16.40, 16.37, 16.33, 16.31, 16.29, 16.25, 16.18, 16.17, 16.13, 16.12, 16.11, 16.9, 16.7, 16.6, 16.3, 16.2, 12.35, 12.34, 12.18, 7.6, 6.21, 6.8
Elternbefragung 16.31
Elterngeld Plus 12.30
E-Mail 18.1, 16.35, 16.32, 16.27, 16.22, 16.19, 16.8, 16.4, 15.3, 12.37, 8.15, 8.11, 7.14, 7.6, 7.3, 6.40, 6.39, 6.34, 6.32, 6.28, 6.17, 6.13, 4.1
E-Mail-Account 16.35, 7.14

E-Mail-Adresse 16.35, 16.27, 16.24, 16.22, 16.19, 16.8, 8.15, 7.14, 6.40, 6.32, 6.28, 6.17, 3.5
E-Mail-Verteiler 8.15
Energieversorgungsunternehmen 6.35
Entlassungsbericht 12.9
Entschließung 18.5, 17.1, 12.3, 8.6, 6.51, 3.2
Entsorgungsunternehmen 6.5
Entwurf Thüringer Datenschutzgesetz 3.3
epidemiologisches Krebsregister 12.2
e-Privacy-Richtlinie 4.1
e-Privacy-Verordnung 4.1
Erfassungsprogramm 12.15
Erforderlichkeit 16.34, 16.23, 15.2, 12.27, 12.24, 12.7, 12.6, 11.9, 11.2, 10.1, 8.22, 8.7, 7.13, 7.12, 7.7, 7.5, 6.34, 6.32, 6.25, 6.22, 6.13, 6.10, 6.9, 3.1, 2.5, 2.4
Erforderlichkeitsgebot 5.3
Erhebung 17.2, 16.41, 16.33, 16.31, 16.23, 16.14, 15.2, 14.2, 13.4, 13.3, 13.2, 12.41, 12.39, 12.36, 12.31, 12.30, 12.23, 12.20, 12.13, 12.7, 12.4, 11.5, 11.2, 8.19, 8.15, 8.13, 8.12, 8.7, 8.2, 7.11, 7.3, 7.1, 6.50, 6.48, 6.34, 6.33, 6.32, 6.28, 6.21, 6.8, 6.1, 5.3, 5.2, 5.1, 4.4, 3.1, 2.3
Erhebung von Personalausweisdaten 5.1
Erhebungsformulare 6.32
Ermittlungshandlungen der Polizei 8.19
Ermittlungsverfahren 11.6, 11.5, 11.2, 8.19, 8.17, 8.14, 7.9, 6.18
Erwachsenenbildung 16.30
Erwerbsunfähigkeit 12.18
Erzieher 16.42, 16.16, 16.3, 7.6
Erziehungsberechtigte 16.36, 16.35, 16.33, 16.3
ESF 15.2, 12.41
EuGH 17.2, 8.4, 3.5, 3.4
Europäische Union 15.3, 4.1, 3.6, 3.5, 3.3, 3.2, 3.1
Europäischer Gerichtshof 17.2, 4.2, 3.5, 3.4
Europäischer Sozialfonds 15.2, 15.1, 12.41
europaweiter Datenabgleich *3.5*
europaweiter Erkenntnisaustausch 3.5
Evaluation 16.31, 16.10, 16.6, 12.41
Existenzgründungen 15.1
externer Datenschutzbeauftragter 6.49
Facebook 16.29, 16.15, 16.3, 8.21, 8.11, 6.23, 6.7, 4.3, 3.4

Facebook-Account 16.15, 6.23
Fachkenntnis 16.20
Fachkunde 12.37, 6.49
Fachunterricht 16.10
Fahndungsfotos 8.11
Fahrerlaubnis 8.18
Fahrradfahrer 13.3
Fahrzeug 18.5, 8.21, 8.18, 6.50, 6.47, 6.25, 6.4
Fahrzeugführer 6.43
Fahrzeugströme 6.11
Fallbearbeitungssystem 8.10
Familienkasse 12.43
Familienstand 12.15
Fantasiename 6.17
Fax 12.37
Fehlzeiten 16.12, 7.7
Feuerstätten 14.2
Feuerungsanlagen 14.2
Fingerprinting 17.6
Fitness-Tracker 12.3
Fluggastdaten 3.5
Förderantrag 15.1
Förderbedarf 16.32
Fördergelder 15.2
Förderhöhe 16.26
Fördermaßnahme 15.1, 7.13
Förderperiode 15.2
Förderung 17.4, 16.10, 15.2, 15.1, 12.40, 7.13
Förderungsanspruch 16.26
Förderverein 16.34
Formbogen 16.41
Formerfordernis 16.19
Formular 13.7, 12.25, 12.4, 8.12, 6.32, 3.4
Forschung 16.37, 13.3, 12.40, 12.39, 12.31, 11.1
Forschungsinstitut 12.39, 7.13
Forschungsvorhaben 16.31, 12.40, 12.39, 12.20, 11.1
Forschungszweck 16.37, 13.3, 12.40, 12.39
Forstamt 14.1
Fortbildung 16.20, 11.9
Fortbildungsangebote 16.20, 16.10

Fortbildungsträger 16.20
Foto- und Videoerlaubnis 16.40
Fotografieren 16.40, 6.3
Fotos 16.42, 16.40, 16.24, 16.13, 16.3, 8.17, 6.45, 6.28, 6.23, 6.18, 6.13, 6.7, 6.5, 6.3, 4.3
Fragebogen 16.41, 16.37, 16.33, 16.6, 15.1, 12.24, 12.6, 6.28, 6.26
Fragekatalog 16.6, 16.4
Freeze-in-Erlass 8.17
freie Beweiswürdigung 8.16
freier Datenverkehr 15.2, 3.3, 3.2, 3.1
Freigabeerklärung 8.3
freiheitlich demokratische Grundordnung 6.1
Freiwilligkeit 18.5, 16.41, 16.33, 16.32, 16.31, 12.30, 8.12, 7.8, 7.7, 7.6, 2.3
Führerschein 12.21, 8.18
Funksignal 13.2
Funkzellenabfrage 8.13
Fußgänger 13.3
Fußgängerzone 13.3
Gebietsreform 6.28, 6.7
Gebot der Datensparsamkeit 6.17
Gebot ordnungsgemäßer Aktenführung 6.25
Gebühren 7.5, 6.48
Gebührenbescheid 6.6
Gebührensatzung 7.5, 6.48
Geburtsdatum 15.4, 12.43, 6.43, 6.32, 6.19, 3.5
Gefährder 8.9
Gefährdungssituation 6.27
Gefahrenabwehr 8.5, 8.2, 6.12
Gefangene 11.1
Geheimhaltungsinteresse 12.40, 12.39, 12.39, 12.30
Gemeinderat 6.24, 6.15
Gemeindeverwaltung 6.37
gemeinsamer Bundesausschuss 12.35, 12.29, 12.13
Gemeinsames Kompetenz- und Dienstleistungszentrum auf dem Gebiet der polizeilichen Telekommunikationsüberwachung 8.4
gemeinsames Krebsregister 12.2
Generalverdacht 14.2, *3.5*
Gericht 17.2, 15.4, 12.44, 12.10, 11.9, 11.7, 11.6, 11.5, 11.4, 11.3, 8.16, 8.13, 7.16, 7.15, 6.46, 6.35, 3.6, 2.4

gerichtliche Festsetzung 8.16
Geschäftsordnung des Thüringer Landtags 19.1
geschwärzte Kopien 12.43, 7.1
Gesellschaft für Arbeits- und Wirtschaftsförderung des Freistaats Thüringen mbH (GFAW) 15.1
Gesetzentwurf 16.30, 16.18, 12.1, 8.9, 4.5, 3.6, 3.3, 3.2, 2.3, 1
Gesetzgebungsverfahren 16.30, 8.9, 3.6, 3.2
Gesprächsaufzeichnung 7.10
Gesundheit 18.4, 16.41, 16.33, 16.2, 15.2, 13.7, 12.40, 12.39, 12.38, 12.36, 12.35, 12.33, 12.30, 12.26, 12.22, 12.14, 12.13, 12.10, 12.9, 12.3, 12.2, 12.1, 11.1, 7.13
Gesundheitsamt 16.41, 16.33, 16.32, 16.18, 16.2, 12.44, 12.21, 12.10, 7.4
Gesundheitsbehörde 12.39
Gesundheitsdaten 16.16, 12.38, 12.32, 12.31, 12.10, 12.5, 12.3, 12.1, 7.3, 3.2, 3.1
Gesundheitskarte 12.14, 6.33
Gesundheitsvorsorge 16.33, 16.32, 11.1
Gesundheitswesen 12.39, 12.14, 12.13
Gesundheitszustand 16.41, 16.33, 12.38, 12.33, 7.4
Gewaltenteilung 17.1, 11.8
Gewerbesteuerentwicklung 6.36
Gewerbesteuererhebung 6.36
Gewerbesteuerzahler 6.36
Gewerkschaftszugehörigkeit 12.22, 12.18, 11.1
GFAW 15.2, 15.1, 7.13
Girokonten 16.25, 2.1
GKDZ 19.1, 8.4, 1
Glaube 11.1, 3.1
Glaubensbekenntnis 11.1
Glaubhaftmachung 8.16
Glücksspiel 15.4
Glückwunschschreiben 6.21
Google Analytics 4.2
GPS-System 6.4
Grenzwerte 14.2
Grundbuchamt 11.10
Grundgesetz 18.5, 17.1, 16.16, 13.2, 12.37, 6.16, 6.7, 4.4
Grundrecht auf informationelle Selbstbestimmung 16.11, 13.2, 12.1, 8.12, 6.39, 6.19, 6.9, 6.6, 6.3, 4.4

Grundrecht auf informationellen Selbstbestimmung 1
Grundsatz der Datenerhebung beim Betroffenen 13.7
Grundsatz der Zweckbindung 12.42, 12.25
Grundschule 16.40, 16.34, 16.17, 16.16, 16.14, 6.21
Grundsicherung 12.28, 12.26, 12.19, 12.8
Grundstückseigentümer 13.6, 6.3
Grundstückskaufvertrag 6.31
Gutachterstelle für Gesundheitsberufe 12.36
Guthaben 16.25
Hacker-Angriff 18.6, 18.4, 6.51, 4.6
Haftraumtüren 11.1
Halterangaben 6.43
Halteranhörung 6.43
HAMASYS 11.7
Handakte 12.6
Handelskette 16.40
Handy 18.5, 16.42, 16.7, 6.47, 6.45, 6.9
Handyparken 6.47
Haus- und Abschlussarbeiten 16.27
Hausaufgaben 16.8
Hausbrandanlagen 14.2
Hausdurchsuchung 11.5, 6.18
Hausleitung 8.1
Hausrecht 14.4, 14.1, 13.3, 6.13, 6.10, 6.9, 5.1, 2.4
Haustiere 6.32
Heil- und Kostenplan 12.32
Heimaufsicht 7.11
Heimbewohner 13.7
Heimleitung 13.7
Hessen 15.4
Hinweisschild 13.3, 6.13, 2.4
Historie 12.6
Hochschule 20, 16.28, 16.27, 16.23, 16.22, 16.21, 16.19, 16.10, 13.3, 2.2
Homepage 16.29, 16.27, 16.1, 12.35, 12.5, 6.39, 4.3, 3.4, 3.1, 2.1
Hospitation 16.37
Hundehalter 6.38
hybride Aktenführung 12.6
Identifikation 17.6, 12.15, 6.43, 6.32
Identifikationskarte für Geflüchtete 6.33

IfSG 16.2
IGVP 8.14
Immatrikulation 16.23
Immelborn 8.1
Immissionsschutzbehörde 14.2
Immobilienmakler 11.10
Impfschutz 16.2
Implementation 16.10
Infektionsschutzgesetz 16.2, 12.10
Informant 6.44
informationelles Selbstbestimmungsrecht 16.38, 6.19, 2.3
Informationsblatt 16.29, 2.1
Informationsfreiheitsgesetz 5.2
Informationspflicht 10.1
Informationspflichten 16.40, 16.36, 4.3, 4.1, 3.4, 3.2, 3.1
Informationsübermittlung 6.1
Informationszugang 5.2
informierte Einwilligung 12.41, 12.31, 12.4, 6.13
Info-Stele 6.13
Infotainmentsysteme 18.5
Innenministerium 16.33, 15.4, 13.2, 8.5, 8.3, 8.2, 7.17, 6.42, 3.3, 1
Innenstadt 13.3
INPOL 8.14
INPOL-Datenbank 8.6
Insolvenzgerichte 11.3
Insolvenzordnung 11.3
Insolvenzportal 11.3
Insolvenzregister 11.3
Insolvenzverfahren 11.3
Institut 16.37, 16.31, 16.29, 16.27, 16.15, 16.5, 12.41, 12.40, 12.39, 12.30, 2.2
Integration 12.41, 12.40, 11.4, 6.33, 6.26
Integrierte Teilhabeplanung 12.6
Integrität 16.36, 16.35, 16.32, 16.19, 16.13, 15.3, 12.44, 12.33, 12.12, 6.34, 3.1
Interessenabwägung 17.2, 14.1, 8.22, 2.4
Internat 6.9
Internet 18.2, 17.6, 17.5, 17.2, 16.35, 16.28, 16.22, 16.20, 16.18, 16.15, 16.5, 14.4, 12.32, 12.14, 12.12, 11.3, 7.14, 7.12, 6.44, 6.39, 6.30, 6.19, 6.16, 6.7, 4.6, 4.4, 4.1, 2.1

Internetplattform 11.3
Internetveröffentlichung 6.16, 6.2
IT-Sicherheit 18.4, 18.2, 18.1, 17.4, 16.13, 11.4
IT-Sicherheitsgesetz 18.4
itWatch Endpoint Security Suite 8.3
IT-Wirtschaft 16.5
Jäger 14.1, 6.18
Jahresabrechnung 13.2
JI-Richtlinie 3.6, 3.3
Jobcenter 12.28, 12.27, 12.26, 12.25, 12.22, 12.19, 12.8, 12.4
Jugendamt 12.41, 12.25, 8.18, 6.34, 6.8
Justiz 11.9, 11.6, 11.4, 11.3, 8.16, 8.1, 7.16, 7.15, 6.33, 3.3
Justizvollzugsanstalt 11.1
JVEG 8.16
Kalender 7.7
Kassenärztliche Vereinigung 12.29, 12.11
Kennzeichenanfrage 6.43
Kfz-Kennzeichen 6.47, 6.11
Kinder 16.42, 16.40, 16.37, 16.33, 16.32, 16.11, 16.7, 16.6, 16.3, 15.1, 12.43, 12.35, 12.25, 12.17, 8.18, 7.6, 7.3, 6.21, 6.12, 6.8, 2.2, 2.1
Kinder- und Jugendärztlicher Dienst 16.41, 12.10
Kinder- und Jugendschutz 16.7
Kindergarten 12.10, 7.6
Kindergeld 12.43
Kindertageseinrichtung 16.2, 7.6
Kindertagesstätte 16.3, 16.2, 6.37
Kindeswohlgefährdung 8.18
KITA 16.3, 16.2
Klageverfahren 6.35
Klassenarbeiten 16.42
Klassenbuch 16.36, 16.12, 16.9
Klassenbuchtransport 16.36
Klassenfahrten 2.1
Klausur 16.21
Klinikum 18.4, 12.38, 12.35, 12.15, 12.5
Kommunalaufsicht 6.6
kommunale Sozialplanung 16.14
Kommunale Wohnungsgesellschaft 6.32

Kommunen 14.3, 13.4, 12.41, 12.28, 12.26, 12.19, 12.16, 12.8, 6.47, 6.42, 6.38, 6.33, 6.31, 6.28, 6.22, 6.12, 6.5, 6.2, 6.1, 1
Kommunikationsplattform 12.31
Konfession 12.15
konkrete Gefahren für die öffentliche Sicherheit und Ordnung 6.14
Konkurrentenstreitigkeiten 11.9
Kontoauszug 16.25, 12.27, 12.26, 12.25, 12.22, 12.18
Kontopfändung 6.29
Kontostand 12.22
Kontrollbefugnis 19.1, 12.42, 8.17, 5.4, 3.4
Kontrollbericht 8.6
Kontrolle 18.5, 16.35, 16.17, 16.15, 16.6, 12.41, 12.26, 12.19, 12.8, 12.6, 11.6, 9.2, 8.17, 8.12, 8.6, 8.2, 7.16, 7.14, 7.9, 7.5, 7.4, 7.3, 7.2, 6.50, 6.47, 6.35, 6.25, 6.20, 6.19, 6.18, 6.4, 6.1, 5.4, 4.5, 4.4, 3.2
Kooperation 16.10, 2.2, 2.1, 1
Kopie 16.42, 16.40, 16.39, 16.15, 15.2, 12.43, 12.29, 12.27, 12.26, 12.18, 12.12, 11.5, 8.8, 8.7, 8.3, 7.9, 7.4, 7.3, 7.2, 7.1, 6.28, 6.1
Koran 11.1
Körperverletzungen 8.18
Kostform 11.1
KoWo 6.32
Kraftfahrzeugbundesamt 6.43
Kraniche 14.4
Krankenhaus 18.4, 12.38, 12.20, 12.15, 12.13, 12.5
Krankenhäuser 18.4
Krankenkasse 12.34, 12.24, 12.13, 12.9, 12.2, 7.3, 6.33
Krankenkassenbeitrag 12.24
Krankschreibung 16.16, 7.3
Krebsregister 12.2, 12.1
Kreditinstitut 12.27, 6.29, 3.6
Kreisgebietsreform 5.4
Kriminalpräventiver Rat 2.4
Kryptografie 18.2
Kultusministerkonferenz 16.11, 16.10, 2.1, 1
Kundenerfassungsbogen 6.32
Kündigung 7.3
Kurs Medienkunde 16.6
Kursplan 16.6
KV Thüringen 12.29

länderübergreifend 16.36, 11.3, 8.6, 8.4, 2.1
länderübergreifende Zusammenarbeit 8.4
Landesamt für Verfassungsschutz 9.2, 9.1
Landesapothekerkammer 12.11
Landesärztekammer Thüringen 12.37, 12.33, 12.13, 12.12, 12.7, 6.34
Landesfinanzdirektion 11.9, 7.2
Landesjustizverwaltung 11.3
Landeskooperationsvereinbarung 2.2
Landeskriminalamt 9.2, 8.20, 8.8
Landesmedienanstalt 16.10, 2.2, 2.1
Landespolizei 8.9
Landespolizeidirektion 8.15, 8.14, 8.11, 8.2, 7.9, 7.1
Landespolizeiinspektion 8.18, 8.17, 8.11, 8.7, 8.5, 8.2
Landesprogramme 7.13
Landesverwaltung 18.1, 11.4, 10.1, 8.2
Landeszahnärztekammer 12.7
Landkreis 16.33, 16.16, 16.14, 16.13, 14.4, 13.5, 12.26, 12.21, 12.19, 12.17, 12.8, 6.46, 6.33, 6.26, 6.16, 6.15, 6.9, 6.5, 6.1
Landratsamt 16.33, 16.16, 16.14, 16.13, 13.6, 12.21, 12.16, 12.10, 12.6, 7.12, 7.5, 6.46, 6.41, 6.34, 6.27, 6.26, 6.25, 6.18, 6.16, 6.9, 6.6, 6.5
Landtag 18.1, 16.30, 12.2, 8.17, 8.4, 8.2, 6.33, 6.28, 6.2, 5.4, 5.3, 5.1, 4.5, 3.6
Landtagsabgeordneter 19.1, 5.4
Landtagsverwaltung 5.4
Lehramtsanwärter 16.16, 16.11, 2.2
Lehre 17.2, 16.37
Lehrer 18.1, 16.43, 16.42, 16.38, 16.37, 16.35, 16.31, 16.18, 16.17, 16.16, 16.15, 16.13, 16.12, 16.11, 16.10, 16.9, 16.8, 16.7, 16.6, 16.5, 16.4, 6.9, 6.8, 2.2, 1
Lehrer-App 16.9
Lehrerausbildung 16.37, 16.16, 16.11, 16.10, 1
Lehrerbefragung 16.6
Lehrerbildung 2.2
Lehrern 16.1
Lehrkräfte 16.43, 16.42, 16.38, 16.36, 16.29, 16.28, 16.17, 16.16, 16.15, 16.11, 16.9, 16.8, 16.7, 16.6, 16.4, 6.9, 2.1
Lehrstuhl Professur 16.27
Leichenschauschein 12.2
Leistungsakten 12.28, 12.26

Leistungsempfänger 12.28, 12.8
Leistungserbringer 12.29, 12.6
Leistungsgespräch 16.17
Leistungskontrolle 12.42, 12.33, 6.4
Lernmittel 16.4
Lernplattform 16.15, 16.9, 16.5, 16.4, 16.1, 2.1
Lichtbild 15.4, 6.51, 6.18
Lichtbilder Haussuchung 6.18
Linux 11.4
Livemitschnitt 6.2
Livestream 6.2
Löschfristen 16.23, 12.10, 11.6, 11.3
Lösch-Moratorium 8.17
Löschtermin 11.6
Löschung 16.23, 14.3, 12.38, 12.27, 12.10, 12.4, 11.10, 11.6, 11.3, 8.17, 8.15, 8.5, 6.39, 4.3, 4.2, 3.3, 3.2, 3.1, 2.5
Löschung von Eintragungen 11.6
Luftschadstoffe 14.2
manueller Bedarf 8.2
Marktortprinzip 3.2, 3.1
massenhafte Datenerhebung 3.4
Matrikelnummern 16.21
MDK 12.34, 12.9
MDR 4.5, 2.1
MDR-Landesfunkhaus Thüringen 4.5
Medien 20, 16.29, 16.15, 16.11, 16.10, 16.6, 7.8, 6.2, 2.2, 2.1
Medienbildung 16.28, 16.11, 16.10, 16.6, 2.2, 2.1
Mediendatenbank 16.28, 2.2
Medienkompetenz .. 18.1, 16.35, 16.29, 16.28, 16.10, 16.6, 2.2, 2.1, 1
Medienkunde 16.35, 16.6, 1
Medienunternehmen 6.2
Medizinischer Dienst der Krankenkassen 12.9
Mehrfachanträge 12.36
Meldepflicht 17.4, 16.18, 14.1, 3.1
Melderegister 12.2, 6.43, 6.19, 4.4
Melderegisterabgleich 12.2
Menschen mit Behinderungen 12.40, 12.6, 7.11
Merkblatt 12.41, 7.13
Messenger-Dienste 16.29, 16.15, 16.9, 16.3, 2.1
Messfahrzeug 6.3

Messwerte 14.2
Microsoft 18.6, 18.3, 16.4, 2.1
Microsoft Office 365 ..... 18.3, 16.4, 2.1
Mietinteressent 6.32
Mietkautionsdarlehen 12.8
Mietschulden 6.32, 6.32
Mietshaus 2.4
Mietvertrag 6.46, 6.32
Migrationshintergrund 16.41, 16.33, 7.13
Mikrofiche 12.44
Mikrozensusgesetz 2.3
milderes Mittel 8.7
Missbrauch 16.35, 12.26, 7.14, 6.4
Missbrauchskontrolle 6.4
Mitarbeiter 20, 18.1, 16.39, 16.24, 16.16, 16.11, 16.7, 16.3, 15.2, 13.4, 12.42, 12.38, 12.28, 12.27, 12.21, 12.16, 12.15, 12.13, 12.6, 12.5, 12.4, 8.12, 8.11, 8.7, 8.3, 8.2, 7.17, 7.14, 7.11, 7.7, 7.6, 7.5, 7.4, 7.3, 7.2, 7.1, 6.49, 6.47, 6.40, 6.34, 6.31, 6.28, 6.27, 6.25, 6.23, 6.18, 6.9, 6.5, 6.4, 4.3, 3.6, 3.4, 3.2, 1
Mitbestimmungsrecht 8.3
mobiles Datenerfassungsgerät 12.42
Monitoring 6.13, 6.9, 2.4
Mülltonnenstandplatz 6.10
Multiplikator 11.7
muslimischer Glaube 11.1
Mutter 16.38, 16.26, 16.17, 6.21, 6.8
Mutterpass 12.14, 7.1
Mutterschutzverordnung 7.1
Nachname 16.35, 7.16, 7.12, 6.32, 6.21
Nachricht 16.35, 16.8, 16.4, 7.14
Name 16.42, 16.38, 16.24, 16.21, 16.3, 16.2, 13.4, 12.43, 12.42, 12.30, 12.29, 12.22, 12.16, 12.14, 12.7, 11.10, 11.1, 9.1, 8.22, 8.16, 8.15, 8.3, 7.14, 7.13, 7.12, 7.11, 7.8, 7.1, 6.47, 6.44, 6.43, 6.39, 6.38, 6.36, 6.32, 6.19, 6.17, 6.15, 6.1, 5.3, 3.5
Namensschilder 11.1, 7.12
Namenszug 6.45
Naturparkverwaltung 14.4
Naturschutzgebiet 14.1
Negativprognose 8.6
Netzwerkdurchsetzungsgesetz 4.3

Netzwerkstruktur 15.1
Neugeborene 12.35
nicht öffentlicher Raum 14.4, 14.4
nicht-öffentliche Sitzung 6.15
NIS-Richtlinie 17.4
Nordrhein-Westfalen 16.5, 11.3, 8.19, 8.12, 8.6, 2.4
Notar 6.31
Notebooks 2.1
Noten 16.21, 16.19, 16.15, 16.13, 16.9
Notrufe 8.2, 7.10, 1
Nutzung 18.6, 18.3, 16.41, 16.38, 16.37, 16.35, 16.33, 16.31, 16.29, 16.28, 16.21, 16.18, 16.16, 16.15, 16.11, 16.9, 16.8, 16.7, 16.4, 16.3, 16.2, 15.4, 15.2, 14.3, 13.5, 13.4, 13.3, 12.42, 12.41, 12.36, 12.30, 12.25, 12.14, 12.13, 12.10, 12.7, 12.4, 11.7, 11.5, 11.3, 11.1, 8.22, 8.19, 8.15, 8.12, 8.7, 8.4, 8.2, 7.15, 7.14, 7.7, 7.3, 6.51, 6.50, 6.33, 6.31, 6.30, 6.29, 6.28, 6.26, 6.23, 6.22, 6.21, 6.17, 6.9, 6.6, 6.4, 5.4, 5.3, 3.6, 2.1
Oberbürgermeister 12.44, 6.28, 6.21
Offenbaren steuerlicher Verhältnisse 6.36
öffentlich eingestelltes Foto 6.23
öffentliche Sitzung 6.15
öffentliche Stelle 20, 19.1, 18.3, 17.1, 16.36, 16.20, 16.19, 16.18, 16.17, 16.15, 16.8, 16.1, 15.4, 14.4, 14.4, 14.1, 14.1, 13.3, 12.43, 12.36, 12.34, 12.30, 12.28, 12.25, 12.21, 12.15, 12.14, 12.13, 12.12, 11.7, 11.1, 8.18, 8.17, 8.15, 8.14, 8.8, 7.17, 7.17, 7.15, 7.15, 7.12, 7.12, 7.8, 7.6, 7.3, 6.49, 6.43, 6.29, 6.20, 6.19, 6.16, 6.13, 6.11, 6.10, 6.9, 6.9, 6.7, 6.6, 6.3, 6.3, 6.1, 6.1, 5.4, 5.3, 5.2, 5.2, 5.1, 4.4, 3.6, 3.6, 3.3, 3.2, 3.1, 2.4, 2.4
öffentliche Wege 14.1
öffentliches Interesse 12.39
öffentliches Unternehmen 6.49
Öffentlichkeitsfahndung 8.11
öffentlich-rechtliche Rundfunkanstalt 4.5
Öffnungsklausel 16.1, 4.5, 3.2, 3.1, 2.4
Ombudsstelle 3.4
Onlinedienst 6.51, 4.6, 2.1
Online-Klassenbuch 16.12
Online-Lernplattform 16.9, 16.4, 16.1, 2.1
Online-Wahlen 16.22
Onlinezugangsgesetz 17.1

Optionskommune 12.28, 12.26, 12.19, 12.8
Ordnungsbehördengesetz 6.30, 6.14, 6.12
ordnungsbehördliche Kontrolle 6.18
Ordnungswidrigkeit 16.17, 16.2, 14.1, 8.18, 8.5, 7.17, 6.44, 6.43, 6.42, 6.14, 6.12, 3.3
Ordnungswidrigkeitengesetz 16.17, 6.47, 6.44
Organisationsuntersuchung 12.42, 12.28
Orientierungshilfe 16.15, 16.1, 8.19, 7.14, 6.32, 2.4, 2.1
Originalunterlagen 15.2, 12.44, 12.27
PAG 8.20, 8.18, 8.13, 8.5, 8.2, 8.2, 3.3
Papiercontainer 16.24
Papierentsorgungsunternehmen 6.5
Parkausweis 13.4
Parlamentarische Anfrage 19.1
Parteimitgliedschaft 12.22
Partnerschaftsbonus 12.30
Passwort 16.35, 16.22, 16.13, 16.12, 6.51, 5.3, 4.6
Patient 12.38, 12.37, 12.33, 12.31, 12.29, 12.20, 12.15, 12.14, 12.13, 12.12, 12.9, 12.5, 12.1, 8.16, 6.33
Patientenakte 12.44, 12.14, 12.13
Patientendaten 12.38, 12.37, 12.31, 12.29, 12.20, 12.15, 12.14, 12.13, 12.10, 12.5
Patientendokumentation 12.44
Patientenportal 12.5
Patientensicherheit 12.14
Personalakte 15.2, 11.9, 7.16, 7.15, 7.9, 7.4, 7.3, 7.2
Personalaktendaten 11.9, 7.16, 7.9, 7.8, 7.6, 7.3
Personalakteneinsicht 7.15, 7.4
Personalausweis 13.4, 8.8, 8.7, 6.51, 5.3, 5.1
Personalausweisgesetz 8.7, 6.51, 5.3, 5.1
Personalausweiskopie 15.4, 8.8, 8.7
Personalausweisnummer 5.3, 5.1
Personalausweisregister 6.51
Personaldaten 7.11, 7.8, 7.6, 7.3
Personalhauptakte 7.2
personalisierte Werbung 17.6
Personalkosten 15.2
Personalnebenakte 7.16, 7.15, 7.2
Personalrat 12.42, 8.3, 7.14, 7.12, 7.10, 7.7
Personalunterlagen 15.2, 11.9, 7.16, 7.15

Personalverwaltung 11.7, 7.16, 7.15, 7.9, 7.7, 7.4, 7.3
Personalvorgänge 11.9
personenbezogene Daten 20, 19.1, 18.5, 18.2, 17.5, 17.4, 17.2, 17.1, 16.42, 16.39, 16.38, 16.37, 16.36, 16.34, 16.33, 16.32, 16.30, 16.29, 16.27, 16.26, 16.25, 16.24, 16.23, 16.21, 16.20, 16.19, 16.18, 16.17, 16.16, 16.15, 16.14, 16.13, 16.12, 16.10, 16.9, 16.8, 16.4, 16.3, 16.2, 15.4, 15.3, 15.2, 15.1, 14.4, 14.3, 14.2, 13.7, 13.6, 13.5, 13.3, 13.2, 12.44, 12.42, 12.38, 12.37, 12.36, 12.35, 12.34, 12.33, 12.32, 12.30, 12.28, 12.25, 12.24, 12.22, 12.21, 12.20, 12.16, 12.14, 12.13, 12.12, 12.10, 12.7, 12.6, 12.5, 12.4, 12.3, 12.1, 11.10, 11.7, 11.5, 11.1, 10.1, 9.1, 8.22, 8.21, 8.20, 8.19, 8.18, 8.17, 8.16, 8.15, 8.14, 8.11, 8.10, 8.8, 8.7, 8.6, 8.5, 8.4, 8.3, 8.2, 7.17, 7.16, 7.15, 7.13, 7.11, 7.8, 7.7, 7.6, 7.5, 7.4, 7.3, 6.50, 6.48, 6.46, 6.45, 6.44, 6.43, 6.41, 6.40, 6.39, 6.37, 6.35, 6.34, 6.32, 6.31, 6.30, 6.29, 6.28, 6.27, 6.26, 6.25, 6.23, 6.22, 6.21, 6.20, 6.19, 6.17, 6.16, 6.15, 6.14, 6.12, 6.11, 6.9, 6.8, 6.7, 6.7, 6.6, 6.5, 6.4, 6.3, 6.1, 5.4, 5.3, 5.2, 5.1, 4.5, 4.4, 4.1, 3.6, 3.4, 3.3, 3.2, 3.1, 2.5, 2.4, 1
personenbezogenes Datum 6.40
persönliche Kenntnis 12.16
Pflegekasse 12.34
Pflegschaft 6.34
Pflicht zur Verschwiegenheit 16.17, 6.6
Pilotprojekt 16.27, 11.4, 8.5
PIN 16.22
PISA 16.31
Plagiatsprüfung 16.27
Poliklinik 12.44
Polizei 18.6, 9.2, 8.22, 8.21, 8.20, 8.19, 8.18, 8.13, 8.12, 8.11, 8.10, 8.9, 8.8, 8.7, 8.5, 8.4, 8.3, 8.2, 8.1, 7.10, 7.1, 6.51, 6.14, 3.3, 1
Polizeiaufgabengesetz 8.20, 8.17, 8.13, 8.5, 8.4, 8.3, 8.2, 6.14, 3.3
Polizeibeamter 8.14, 8.12, 8.5, 7.9, 6.18, 1
polizeiliche Telekommunikationsüberwachung 19.1, 8.4
polizeilicher Funkverkehr 8.2
Postgeheimnis 12.37, 7.3
Postweg 12.27, 7.16, 7.3, 6.32, 6.20
Presse 8.22, 8.11, 8.2, 6.19, 6.12, 4.4
Pressemitteilung 14.1, 8.11, 8.4, 7.8, 3.2, 3.1
Pressevertreter 8.22, 8.15, 8.11, 6.19
Privacy Shield 8.4, 4.2, 3.4
private Stelle 15.1, 14.1, 12.1, 7.17

Privatkonten 2.1
Privatperson 18.6, 12.10, 8.21, 6.15, 6.7
Privatunternehmen 8.13
Projektpartner 15.1
Projekttag 16.40
Protokollierung 18.5, 15.4, 12.38, 9.2, 7.14, 3.1, 2.5
Protokollrecherche 8.3
Prüfstellen 15.2
Prüfung 16.41, 16.40, 16.39, 16.34, 16.32, 16.31, 16.30, 16.27, 16.26, 16.22, 16.21, 16.19, 16.18, 16.16, 16.13, 16.12, 16.9, 16.5, 15.4, 15.3, 15.2, 15.1, 14.1, 13.7, 13.5, 13.3, 12.43, 12.42, 12.41, 12.39, 12.38, 12.35, 12.28, 12.27, 12.26, 12.25, 12.22, 12.14, 12.9, 12.5, 11.10, 11.9, 8.21, 8.19, 8.17, 8.16, 8.14, 8.10, 7.16, 7.14, 7.13, 7.9, 7.8, 7.2, 7.1, 6.46, 6.33, 6.32, 6.15, 6.10, 6.6, 6.4, 5.2, 3.5, 3.4, 2.5, 2.4, 2.3, 2.1
Prüfungsunterlagen 16.39
Pseudonymisierung 12.40, 12.38, 12.29, 12.20
psychiatrische Untersuchung 12.33
Qualität 12.29, 12.13, 4.3
Qualitätssicherung 12.29, 12.20, 12.13, 12.1
Rechnungsprüfung 12.28
Recht auf die Berichtigung 3.1
Recht auf informationelle Selbstbestimmung 16.16, 16.2, 12.22, 11.6, 11.2, 8.12, 8.7, 6.16, 4.4, 2.4
Recht auf Vergessenwerden 3.2, 3.1
Rechtsanwalt 11.5, 8.17, 8.14, 7.3, 6.42
Rechtsgrundlage 18.3, 16.43, 16.42, 16.36, 16.34, 16.30, 16.26, 16.23, 16.22, 16.14, 16.7, 16.2, 15.2, 14.4, 13.2, 12.44, 12.41, 12.36, 12.31, 12.29, 12.8, 12.7, 11.5, 11.3, 8.22, 8.19, 8.18, 8.17, 8.15, 8.14, 8.6, 8.5, 8.3, 8.2, 7.13, 7.11, 7.7, 7.6, 7.3, 6.46, 6.40, 6.37, 6.34, 6.31, 6.28, 6.27, 6.24, 6.23, 6.21, 6.20, 6.15, 6.12, 6.8, 6.7, 6.6, 6.2, 6.1, 5.2, 3.4, 3.1, 2.4, 2.1
Rechtsgrundlagen 12.35
Referenzdatei 8.12
Regelschule 16.15, 16.13, 16.11, 2.2
Registerstelle 12.1
Reha 12.34, 12.9
Rehabilitation 12.9
Reichsbürger 7.12, 6.1
Reisende *3.5*, 2.1

Religion 12.22, 11.1
Rente 16.17, 12.24
Renteneintritt 12.24
Repräsentativstatistik über die Bevölkerung und die Arbeitsmarktbeteiligung sowie die Wohnsituation der Haushalte 2.3
Ressortabstimmung 12.2, 3.6, 3.3
Restschuldbefreiung 11.3
Rettungsleitstelle 7.10
Rezept 12.38, 12.11
richterliche Unabhängigkeit 11.8, 6.35
Richtervorbehalt 8.13
Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung 3.3
Robert-Koch-Institut 12.39
Rollen- und Berechtigungskonzept 15.1, 12.38
Rollenkonzept 12.6
Röntgenunterlagen 12.44
Röntgenverordnung 12.44
Rotes Kennzeichen 6.25
Router 4.6
Rücksendung 12.27
Rückzahlung 12.8
ruhender Verkehr 12.42, 6.43
Ruhestand 16.17
Runder Tisch Medienkompetenz 16.11, 2.2
Rundfunkbeitrag 6.19, 4.5, 4.4
Rundfunkbeitragsstaatsvertrag 6.20, 6.19, 4.4
Sachbeschädigung 6.12, 6.9
Sächsischer Datenschutzbeauftragter 4.5
Sachverständigengutachten 12.33
Safe Harbor 8.4, 4.2, 3.4
Sanierung 11.10
Sanktionen 3.2, 3.1
Satzung 16.19, 13.2, 11.10
Schadensersatzansprüche 12.44
Schallschutz 7.3

Schattenkopien 8.3
Schornsteinfegerinnung 14.2
Schriftwechsel 6.6
Schulamt 16.38, 16.34, 16.18, 16.17, 16.16, 16.15, 16.12
Schulcloud 16.5
Schuldner 12.22, 7.12, 6.29, 6.22
Schule 20, 18.3, 18.1, 16.42, 16.40, 16.38, 16.37, 16.36, 16.35, 16.34, 16.32, 16.31, 16.29, 16.28, 16.18, 16.17, 16.16, 16.15, 16.14, 16.13, 16.12, 16.11, 16.10, 16.9, 16.8, 16.7, 16.6, 16.5, 16.4, 16.1, 12.41, 12.10, 6.21, 6.9, 2.2, 2.1, 1
Schuleinführung 6.21
Schuleingangsuntersuchung 16.33, 12.10
Schüler 20, 16.42, 16.38, 16.37, 16.36, 16.35, 16.34, 16.32, 16.31, 16.29, 16.28, 16.18, 16.17, 16.15, 16.14, 16.13, 16.12, 16.11, 16.10, 16.9, 16.8, 16.7, 16.6, 16.5, 16.4, 16.1, 6.21, 2.1
Schüler- und Lehrerdaten 16.4, 16.1
Schulfinanzierungsgesetz 16.18, 16.13
Schulgesetz 16.1
Schulgesundheitspflege 16.41, 16.33, 16.18
schulische Leistung 16.17
Schulkonten 2.1
Schulleitung 16.40, 16.17, 16.13, 16.12, 16.6
Schulnote 16.15, 16.14
Schulpersonal 16.38
Schulpflicht 2.1
Schulserver 16.13, 16.9
Schultagebuch 2.1
Schulträger 16.31, 16.18, 16.16, 16.13, 16.12, 16.9, 16.5, 6.21, 2.1
Schulung 16.20, 12.38, 7.6
Schulunterricht 16.40, 16.4, 2.1
Schuluntersuchung 16.32
Schulverwaltung 16.18, 16.9, 16.1, 6.21
Schulverwaltungsamt 16.16
Schutz des Angezeigten 11.2
Schutzmaßnahmen 16.13, 11.3
Schwangerschaft 7.6, 7.1
Schwärzen 16.25, 12.43, 12.26, 12.22, 8.8, 8.7, 7.1, 6.30
schwarzes Brett 7.6
Schwärzung 16.25, 12.43, 12.26, 12.22, 12.18, 7.1
Schweigepflicht 12.21, 8.16, 7.3

Schweigepflichtentbindung 12.9, 12.4
Schweinefleisch 11.1
Schwerbehindertenangelegenheiten 12.16
Screening 12.35
Segler 14.4
Selbstständige 8.16
Senioren 12.31, 12.30
Sepsis 12.20
Server 16.35, 16.27, 16.22, 16.19, 16.13, 16.7, 16.4, 8.11, 4.6
Serverschrank 16.13
Servicekonten 17.1
Sexualleben 12.22, 11.1
Sicherheitskonzept 16.18, 16.13, 15.1, 14.3, 8.14, 8.3, 1
Sicherheitsmaßnahmen 18.6, 17.4, 16.13
Sicherheits-Updates 18.6
Signalsteuerung 6.11
Signaturgesetz 17.3
Signaturverordnung 17.3
Silver Economy 12.31
Smart Home 12.31
Smartphone 18.5, 16.29, 16.18, 16.9, 12.12, 6.4, 4.6, 2.1
Solarkataster 14.3
Soll-Buchung 12.22
sonderpädagogischer Förderbedarf 16.32
Sozialamt 16.38, 16.7, 12.19, 12.18, 12.17, 12.6
Sozialdaten 16.7, 12.40, 12.30, 12.28, 12.26, 12.23, 12.21, 12.17, 12.9, 6.34, 6.33
soziale Medien 6.23
soziale Netzwerke 18.5, 16.29, 16.28, 16.15, 16.9, 16.8, 16.7, 16.3, 6.7, 4.3, 2.1
Sozialgeheimnis 16.7, 12.30, 12.17, 7.3
Sozialgesetzbuch 17.4, 16.38, 16.26, 16.25, 16.7, 12.40, 12.34, 12.30, 12.29, 12.28, 12.26, 12.25, 12.24, 12.23, 12.22, 12.21, 12.19, 12.19, 12.18, 12.17, 12.14, 12.9, 12.8, 12.6, 12.2, 12.1, 7.11, 6.46, 6.34, 6.33
Sozialhilfe 12.18, 12.17
sozialpsychiatrischer Dienst 12.21, 12.10
Spam 18.1
Speichelprobe 8.12
Speicherdauer 16.40, 12.41, 12.2, 7.10, 6.9, 3.5

Speicherfrist 16.23, 12.41, 3.1
Speicherung 17.2, 16.40, 15.2, 13.3, 12.34, 12.31, 12.26, 12.10, 12.4, 8.17, 8.15, 8.12, 8.6, 8.4, 8.2, 7.10, 7.1, 6.51, 6.50, 6.26, 6.25, 6.22, 6.13, 6.9, 5.3, 5.1
Sperrdatei 15.4
Sperrung 15.4, 12.10, 4.3
Sprachstandserhebung 16.34
Staatsanwaltschaft ... 11.6, 11.5, 11.4, 11.2, 8.14, 7.9, 6.44, 6.37, 6.18
Staatsvertrag 19.1, 12.2, 8.4, 4.5, 2.1, 1
Stadtrat 6.6, 6.2
Stadtverwaltung 12.44, 12.42, 12.41, 7.17, 7.14, 7.8, 7.7, 7.3, 6.43, 6.40, 6.39, 6.31, 6.30, 6.29, 6.28, 6.21, 6.20, 6.13, 6.12, 6.11, 6.8, 6.6, 6.5, 6.4, 6.3, 6.2
Stadtwald 14.1
Stammdatensatz 15.1
Standardvertragsklauseln 3.4
stationäre Aufnahme 12.15
Statistik 16.34, 5.2
Stausee 14.4
Stellenausschreibung 6.39
Stellungnahme 19.1, 16.43, 16.40, 16.39, 16.38, 16.34, 16.30, 16.27, 16.26, 16.25, 16.22, 16.19, 16.18, 16.17, 16.16, 16.15, 16.13, 16.10, 16.9, 16.3, 16.2, 14.1, 12.43, 12.42, 12.39, 12.34, 12.33, 12.29, 12.27, 12.26, 12.15, 12.9, 12.6, 12.4, 12.2, 11.10, 11.6, 11.5, 11.3, 9.1, 8.18, 8.17, 8.12, 8.4, 7.17, 7.16, 7.4, 7.1, 6.45, 6.34, 6.33, 6.27, 6.20, 6.15, 6.11, 6.3, 4.3, 3.6, 3.3, 3.2, 2.3, 2.1, 1
Steuerbehörde 12.24
Steuerdaten 6.38, 6.36
Steuererklärung 12.25
Steuerschuld 6.31
Steuerungsgremium 10.1
Stiftung 16.40
Stimmzettel 16.22
Stoffwechsel 12.35
Strafprozessordnung 11.6, 11.5, 11.2, 8.19, 8.14, 8.13, 8.5, 8.4, 8.2, 7.9, 6.44, 6.18
strafrechtliche Verurteilung 8.22
Straftaten 12.37, 11.2, 8.22, 8.21, 8.19, 8.18, 8.13, 8.6, 8.5, 8.2, 6.18, 6.14, 6.12, 3.5, 3.3
Strafverfolgung 11.2, 8.19, 8.13, 8.2, 3.4

Straßenzustand 6.3
Strategie-Papier 16.10, 1
Streetview 6.3
Streetworker 16.7
Student 16.31, 16.28, 16.24, 16.21, 16.19, 13.3
Studienseminar 16.16, 16.11, 2.2
Studierende 16.27, 16.23, 16.22, 16.21, 16.19
Tablets 16.18, 16.9, 2.1
TAN 16.22
Tatverdächtige 8.13
technische und organisatorische Maßnahmen 18.2, 16.37, 16.36, 16.22, 16.19, 16.18, 16.15, 16.13, 16.7, 16.4, 15.4, 15.3, 12.37, 12.33, 12.31, 12.20, 12.14, 12.13, 12.6, 12.5, 10.1, 9.2, 8.15, 8.14, 8.3, 7.4, 7.3, 6.45, 6.45, 6.30, 6.5, 6.4, 3.1
Teilakte 15.2, 11.9, 7.16, 7.2
Teilnehmerliste 6.45
Telearbeit 11.4
Telekommunikationsdienste 16.29
Telekommunikationsgesetz 17.4, 8.13, 7.10
Telekommunikationsunternehmen 16.35
Telekommunikationsverbindungsdaten 8.13
Telemediengesetz 17.4, 17.2, 5.3
Telemedizin 12.14
Test 16.42
Testbetrieb 8.10, 8.5
ThAVEL 12.6
Theater 6.49
ThürDSAnpUG 3.6, 3.3
Thüringer Bauordnung 13.6
Thüringer Beamtengesetz 16.43, 7.17, 7.16, 7.15, 7.9, 7.8, 7.7, 7.6, 7.4, 7.3, 7.2
Thüringer Bestattungsgesetz 12.39
Thüringer Hochschulgesetz 16.23, 16.22, 16.19
Thüringer Innenministerium 16.33, 8.9, 8.4, 8.2, 8.1
Thüringer Kommunalordnung 6.48, 6.36, 6.22, 6.15, 6.6, 6.2
Thüringer Krankenhausgesellschaft 12.38
Thüringer Krankenhausgesetz 12.38, 12.20, 12.15, 12.13, 12.5
Thüringer Krebsregistergesetz 12.1
Thüringer Landesfinanzdirektion 12.43, 7.2
Thüringer Landeskriminalamt 9.2, 8.20, 8.13, 8.8, 8.6, 8.3, 8.2

Thüringer Landesrechenzentrum 18.1, 13.5
Thüringer Landesverwaltungsamt 16.41, 16.39, 16.33, 15.4, 12.39, 12.12, 7.11, 6.46
Thüringer Laufbahngesetz 16.43
Thüringer Meldeverordnung 2.5
Thüringer Ministerium für Bildung, Jugend und Sport 16.43, 16.42, 16.37, 16.31, 16.29, 16.18, 16.17, 16.15, 16.9, 16.2, 2.1
Thüringer Polizei 19.1, 8.17, 8.14, 8.12, 8.11, 8.10, 8.5, 8.4, 8.3, 8.2, 1
Thüringer Rechnungshof 15.2, 12.26
Thüringer Schulgesetz 16.42, 16.40, 16.38, 16.37, 16.36, 16.31, 16.18, 16.17, 16.16, 16.15, 16.13, 16.11, 16.7, 6.21
Thüringer Schulordnung 16.18, 16.13, 16.11, 16.9, 16.7
Thüringer Umweltinformationsgesetz 6.41
Thüringer Verfassungsgerichtshof 8.1
Thüringer Verfassungsschutzgesetz 19.1, 9.1, 6.1
Thüringer Wohn- und Teilhabegesetz 12.6, 7.11
Thüringer Zentrum für Existenzgründungen und Unternehmertum (ThEx) 15.1
ThürKAG 6.48, 6.38
ThürPersVG 8.3
ThürVerfSchG 9.1, 6.1
TLS 1.2 ..... 18.2
TMASGFF 16.41, 12.40, 12.39, 12.36, 12.35, 12.30, 12.14, 12.13, 12.9, 12.2, 12.1, 7.13
TMIK 19.1, 8.17, 8.12, 8.9, 8.7, 8.5, 8.4, 8.3, 8.2, 7.9, 3.6, 3.3, 2.5, 1
Tochter 12.18, 6.21
Todesursachen 12.39
Tonaufnahmen 16.40, 16.37, 12.33
Toten- und Sektionsscheine 12.39
Tracking 17.6, 4.1
Trackingsystem 6.4
Träger 16.3, 12.9, 7.6
Transfusionsgesetz 12.44
Transparenz 16.15, 6.32, 6.15, 6.4, 3.1
Transportprotokoll 18.2, 6.32
Trugspuren 8.12
Twitter-Account 5.4
überbetriebliche Ausbildungsgesellschaft 12.4

Übermittlung 16.39, 16.38, 16.34, 16.32, 16.27, 16.24, 16.19, 16.17, 16.15, 16.7, 16.2, 15.4, 15.2, 12.41, 12.40, 12.36, 12.35, 12.32, 12.31, 12.30, 12.23, 12.21, 12.17, 12.16, 12.13, 12.12, 12.11, 12.9, 12.7, 12.4, 11.9, 8.22, 8.19, 8.18, 8.15, 8.8, 7.11, 7.7, 7.6, 6.46, 6.41, 6.40, 6.34, 6.32, 6.31, 6.30, 6.29, 6.27, 6.21, 6.19, 6.15, 6.7, 6.6, 6.3, 6.1, 4.4, 3.5, 3.4
Übermittlungsersuchen 11.9
übertragener Wirkungskreis 13.5
Ultraschall-Vereinbarung 12.29
Umsetzung 18.5, 18.1, 17.4, 16.23, 16.22, 16.10, 16.6, 15.4, 14.3, 12.41, 12.38, 12.31, 12.13, 12.1, 8.2, 7.9, 7.1, 4.1, 3.5, 3.4, 3.3, 3.2, 3.1, 1
ungeschwärzte Kontoauszüge 16.25, 12.25, 12.22
Universität. 16.37, 16.27, 16.24, 16.23, 16.22, 16.21, 16.19, 16.6, 2.2
unmittelbar drohende Gefahr 12.11
Unterarbeitskreis Datenschutz und Schule 16.10, 16.4, 2.1, 1
Unterhalt 12.17
Unterhaltsanspruch 12.18, 12.17
unterhaltspflichtige Kinder 12.17
Unterkunft 8.22, 6.46
Unternehmertum 15.1
Unterricht 16.35, 16.16, 16.11, 16.6, 2.2
Unterrichtsgegenstand 16.29
Unterrichtsmaterialien 16.28, 16.8, 1
Unterrichtsvideografie 16.37
Unterrichtung der Öffentlichkeit 9.1
Unterschrift 16.3, 12.38, 8.14, 6.51, 6.45, 6.28, 6.7
Unterschriftenliste 16.21, 6.28, 6.7, 5.4
Unterschriftensammlung 6.28
Untersuchung 17.4, 16.43, 16.41, 16.32, 16.2, 12.35, 12.33, 11.1, 8.2, 7.4
Untersuchungsausschuss 8.17, 8.1
Unzuständigkeit 11.9
Urkundenverifikation 12.12
USA PATRIOT Act 16.27, 16.4
USB-Stick 11.4, 6.37
US-Geheimdienste 3.4, 2.1
US-Sicherheitsbehörden 16.4
valide 12.13, 12.1
Validierung 12.13

Validität....12.13
Vandalismus....6.9
Vater-Kind-Beziehung....16.26
Veranstaltung 20, 18.1, 16.40, 16.38, 16.29, 16.11, 12.14, 6.14, 6.12, 2.2
verantwortliche Stelle 18.6, 16.18, 16.8, 16.7, 15.4, 14.4, 14.1, 13.5, 13.3, 12.31, 12.28, 12.26, 12.23, 12.21, 8.10, 7.13, 7.10, 7.5, 7.4, 6.49, 6.39, 6.33, 6.30, 6.28, 6.13, 6.9, 6.5, 6.3
Verantwortlichen....10.1, 6.43, 3.3, 3.1, 2.4
Verantwortung 18.5, 17.5, 16.36, 16.29, 16.22, 16.18, 16.9, 16.8, 16.6, 16.3, 15.4, 12.12, 11.9, 11.6, 11.3, 8.8, 8.6, 6.51, 6.2, 4.6
Verarbeitung zu journalistischen Zwecken....4.5
Verbeamtung....16.43
Verbraucherzentrale....15.2
Verbunddatei....8.6
Verbundverfahren....15.1, 13.5
Verdienstausfall....8.16
Verfahrensakten....11.9
Verfahrensbeteiligter....11.9
Verfahrensverzeichnis....16.18, 16.12, 15.1, 14.3, 13.5, 11.7, 7.5, 1
Verfahrensverzeichnisblatt....12.6, 8.3
Verfassung des Freistaats Thüringen....19.1, 12.2, 6.2
Verfassungsschutz....9.2, 9.1, 6.51, 6.1
Verfassungsschutzbericht....9.1
Verfügbarkeit....16.36, 16.35
Vergitterung....12.44
Verhaltens- und Leistungskontrolle....12.42, 6.4
Verhältnismäßigkeit....13.6, 12.22, 8.21, 8.5, 6.12, 5.3, 5.1, 3.5
Verkehrsanlagen....6.3
Verkehrsbeobachtung....13.3, 6.11
Verkehrskontrolle....8.18
Verkehrsüberwachung....12.42
Verlagswesen....16.5
Verletzteninteresse....11.5
Vermieter....12.8, 6.32, 6.23
Vernehmung Minderjähriger als Zeugen....6.8
Verneinung Anfangsverdacht bei Strafanzeigen....11.2
vernetztes Fahren....18.5
vernünftige Erwartungen....2.4

Veröffentlichung 19.1, 16.37, 16.36, 16.15, 16.13, 14.3, 12.35, 11.3, 9.1, 8.22, 8.14, 8.11, 7.12, 7.8, 7.6 , 6.16, 6.3, 6.2
Verordnung über die Thüringer Schulgesundheitspflege 16.32
Verschlüsselung 16.19, 16.13, 16.8, 15.3, 12.37, 12.31, 12.20, 12.12, 12.5, 7.3, 6.32, 6.30
Versetzungsentscheidungen 16.42
Verstorbene 12.39
Vertrauensdienstegesetz 17.3
vertrauliche Personalsache 7.16, 7.4
Vertraulichkeit 16.36, 16.35, 16.32, 16.19 , 16.15, 16.13, 16.8, 15.3, 12.44, 8.15, 8.4, 7.3, 6.34, 6.5, 3.1
Vertraulichkeitsgebot 8.15
Verwaltungsangelegenheiten 16.19, 11.7, 7.15, 6.35, 5.1
Verwaltungsaufgaben 11.7
Verwaltungsgemeinschaft 16.3, 6.50, 6.24, 6.15
Verwaltungsgericht 11.9
Verwaltungsrechtsstreit 11.9
Verwaltungstätigkeiten 11.7
Verwaltungsverfahrensgesetz 16.42, 16.19, 6.44, 6.25, 6.8
Verwertungsverbot 7.9
Verzeichnis über Verarbeitungstätigkeiten 3.1
Videoaufnahmen 19.1, 16.37, 16.3, 12.33
Videoaufzeichnung 16.37, 13.3, 12.33, 6.13, 6.9, 2.4
Videobeobachtung 13.3, 6.13, 6.9, 2.4
Videodetektor 6.11
Videodrohnen 2.1
Videokamera 6.24, 6.10, 6.9, 1
Videokameras 13.3
Videos 18.5, 16.28, 16.4, 16.3, 8.21, 4.3
Videoüberwachung 19.1, 14.4, 14.1, 13.3, 8.19, 8.5, 6.24, 6.14, 6.13, 6.12, 6.11, 6.10, 6.9, 3.6, 3.2, 2.4, 2.1, 1
Vier-Augen-Prinzip 8.3
VoIP 17.5, 4.1
Volkszählungsurteil 15.2, 13.3
Vollmacht 12.34
Vorabauskunft 12.32
Voranerkennungsverfahren 12.32
Vordruck 16.41, 16.33, 13.7, 7.11
Vorgangsbearbeitungssystem 8.10
Vorkaufsrecht 6.31

Vorlagepflicht 12.22, 12.18
Vorname..... 15.4, 12.30, 12.15, 8.15, 7.16, 7.12, 6.32, 6.21, 6.19, 5.3
Vorratsdatenspeicherung 17.1, 8.13, *3.5*
Vorsorge 12.35
Vorwarnmechanismus 15.3
Waffenbehörde 6.27, 6.18
Waffengesetz 8.17
Wahlamt 16.22, 6.15
Wahlberechtigte 16.22, 6.19
Wahllichtbildvergleich 8.17
Wahlordnung 16.22
Wahlverfahren 16.22
Waldbesucher 14.1
Waldgebiet 14.1
WannaCry 18.6
Wasser- und Abwasserzweckverband 6.48
Wasserverbrauch 13.2
Wasserzähler 13.2
Wearables 12.3
Webanwendung 16.4
Webcam 14.4, 6.13
Webformular 6.32
Website 18.3, 18.2, 18.1, 17.6, 17.3, 17.2, 6.39, 6.13, 4.2, 4.1, 2.4
Weiterbildung 16.39, 7.7, 2.2
Werbemaßnahmen 16.40
Werbung 17.6, 16.29, 12.7, 6.19
Wertgutachten 6.46
Wertungsteil des Zwischenberichts 8.1
Wettbewerb 6.49, 3.6, 2.1
Wettbewerbsunternehmen 6.49
WhatsApp 16.29, 16.11, 16.7, 16.3, 2.1
Widerruf 16.40, 16.37, 16.31, 12.23, 12.4, 6.34, 3.1
Widerrufsmöglichkeit 16.40
Widerspruchslösung 14.3
Widerspruchsmöglichkeiten 16.37, 6.19, 4.4
Widerspruchsrecht 12.38, 12.23, 12.1, 6.19, 6.3, 4.3, 3.1
Wildkameras 14.1
Windows 10 ..... 18.3
Windows Server 2003 ..... 18.6
WindowsXP 18.6

wirtschaftliche Belastung 2.3
wissenschaftliche Forschung 12.40, 12.30
W-LAN 5.3
Wohngeld 13.7, 13.5
Wohngeldfachverfahren 13.5
Wohngeldstelle 13.5
Wohnsitz 6.8
Wohnumfeld 6.9
Wohnungsbaugesellschaft 6.23
Wohnungseigentümergemeinschaft 6.22
Wohnungseigentumsgesetz 6.22
Wohnungsgesuch 6.32
Workshop 12.38
Zahnarzt 12.11, 12.7
Zahnersatz 12.32
Zeiterfassung 12.42, 7.7, 7.5
Zeitschrift 16.22, 12.7
Zeitung 18.1, 16.43, 12.7, 8.2, 7.8, 6.34, 6.14, 6.13
Zensur 16.42
Zentrales Staatsanwaltschaftliches Verfahrensregister (ZStV) 11.6
Zentralregister 12.36
Zeuge 8.16, 6.44, 6.8
Zeugnis 16.13, 12.43, 7.1
Zugangskontrolle 6.9
Zugriffsrecht 12.38, 12.14, 12.6
Zusatzfragebogen 16.33
Zuständigkeit 18.5, 17.1, 16.18, 15.2, 13.4, 12.43, 12.30, 12.26, 12.23, 12.19, 12.16, 11.9, 11.3, 8.20, 8.18, 7.17, 6.43, 6.42, 6.41, 6.31, 6.25, 6.20, 6.6, 6.1, 3.6, 3.2
Zuständigkeit der Ordnungsbehörden 6.14
Zuständigkeit des TLfDI 12.19, 11.8, 5.4, 5.1
Zustimmung 17.1, 16.40, 16.37, 16.19, 16.11, 16.10, 12.24, 8.13, 8.7, 7.9, 6.8, 4.5, 3.2, 3.1
Zuverlässigkeit 6.49, 6.25
Zuwendungsempfänger 15.2
Zwangsversteigerung 6.46
Zweckänderung 12.42, 12.11, 8.21, 8.19, 8.12, 3.2
Zweckbindung 16.37, 12.28, 8.4, 6.43, 5.2, 3.4, 3.1
Zweite Phase der Lehrerbildung 16.11
Zwischenbericht 8.1

Vorbemerkungen zum Sprachgebrauch

Die verallgemeinernden Personenbezeichnungen in diesem Bericht gelten aus Gründen der Lesefreundlichkeit der Texte jeweils in der männlichen und weiblichen Form.

Impressum

Herausgeber: Thüringer Landesbeauftragter für den Datenschutz und die Informationsfreiheit (TLfDI)
Häßlerstraße 8, 99096 Erfurt
Postfach 900455, 99107 Erfurt
Telefon: 0361/57 3112900, Telefax: 0361/57 3112904
E-Mail: poststelle@datenschutz.thueringen.de
Internet: www.tlfdi.de

Druck: ReproPartner GbR
Liebknechtstr. 18
99085 Erfurt
Telefon: 0361/7891270
E-Mail: info@repropartner.de

Cover und Layout: Druckhaus Gera GmbH
Jacob-A-Morand-Straße 16, 07552 Gera
Telefon: 0365/737520
E-Mail: info@druckhaus-gera.de

Redaktionsschluss: 31. Januar 2018

Bildnachweis: TLfDI

TLfDI

Thüringer Landesbeauftragter
für den Datenschutz und die Informationsfreiheit



3. Tätigkeitsbericht zum Datenschutz: Nicht-öffentlicher Bereich

3. Tätigkeitsbericht zum Datenschutz: Nicht-öffentlicher Bereich

des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit

Berichtszeitraum: 1. Januar 2016 bis 31. Dezember 2017
Zitiervorschlag: 3. TB LfDI Thüringen

Der 3. Tätigkeitsbericht steht im Internet unter der Adresse www.tlfdi.de zum Abruf bereit.

Erfurt, im Dezember 2017

Dr. Lutz Hasse
Thüringer Landesbeauftragter für den Datenschutz
und die Informationsfreiheit

Inhaltsverzeichnis

Vorwort **12**

1 Schwerpunkte im Berichtszeitraum **16**

2 Der betriebliche Datenschutzbeauftragte **19**
2.1 Europäische Datenschutz-Grundverordnung: Unternehmen fragen – TLfDI informiert 19
2.2 Darf ein IT-Mitarbeiter gleichzeitig betrieblicher Datenschutzbeauftragter sein? 21
2.3 Darf ein IT-Sicherheitsbeauftragter gleichzeitig Datenschutzbeauftragter des Unternehmens sein? 24
2.4 Zu viele auf einmal: Bestellung einer Rechtsanwalts-Partnerschaft zum Datenschutzbeauftragten 26
2.5 Bestellung eines Datenschutzbeauftragten 28
2.6 Die Europäische Datenschutz-Grundverordnung kommt – und die Unternehmen machen sich so ihre Gedanken 31
2.7 Einbruchdiebstahl in der Kita 33

3 Umgang mit Kundendaten **36**
3.1 Immelborn – Ad Acta: Zwischenbericht des Untersuchungsausschusses 6/2 liegt jetzt vor: Handeln des TLfDI rechtmäßig – Amtshilfeverweigerung durch das ehemals CDU-geführte Innenministerium rechtswidrig! 36
3.2 Nerviges Meinungsforschungsinstitut 37
3.3 Daten-Theater 39
3.4 Der Anwalt als Datenschleuder? 41
3.5 Reparatur inklusive Datenverlust – wer richtig liest, erspart sich viel Ärger 43
3.6 Datenerhebung zur Beitreibung rechtmäßiger offener Forderungen ist kein Datenschutzverstoß 45
3.7 Bewerbung erfolglos – Daten löschen! 47
3.8 Hotelinsolvenz: Gehören die Kundendaten dem neuen Eigentümer? 48
3.9 Das Probeabonnement einer Zeitung als Türöffner für Werbeattacken 52
3.10 Baumarkt verlangt Adressangabe beim Umtausch 54

3.11 Versteckte Einwilligungserklärung....56
3.12 Pkw-Stellplatz gegen Ausweiskopie – was ist in der Mieterselbstauskunft zulässig?....58
3.13 Bestattungskosten: Datenschutz kein Kostenschutz..60
3.14 Unzulässige Kopie des Personalausweises – keine Bombenidee....61
3.15 Ver(un)sicherung....64
3.16 Einmal hin, einmal her – Versicherungsvermittlung ist manchmal schwer....66
3.17 Seminararbeit im Netz: nur ohne Personenbezug....67
3.18 Welche Mitgliederdaten darf ein Verein erheben und an seinen Dachverband weitergeben?....68
3.19 Zahlartensteuerung – nein, danke!....73
3.20 Der TLfDI macht viel – aber nicht alles....75
3.21 Pressefreiheit versus Datenschutz?....76
3.22 Wie oft muss man der Hausbank den Personalausweis vorlegen?....78
3.23 Wenn die Hausbank keine Auskunft erteilt....79
3.24 Frage eines Software-Entwicklers: Veröffentlichung von Vertretungsplänen sowie Stundenplänen innerhalb einer App für Schulen....80
3.25 Mitgliedsbeiträge am schwarzen Brett?....81
3.26 Der Übergang von Kundendaten bei Unternehmensverkäufen....82
3.27 Datenschutz für Pseudonym?....85
3.28 Bürgerinitiative ratlos – der TLfDI kann helfen....86
3.29 Aktenlager überall....88
3.30 Umfrage des TLfDI – Thüringer Unternehmen zeigen sich hinsichtlich Datenschutzanforderungen höchst vorbildlich....89
3.31 Weitergabe von Kundenverbrauchsdaten durch Versorgungsunternehmen....95
3.32 Schrott sammeln = Daten sammeln? Fortsetzung II..97
3.33 Handy als Navigator im Einkaufzentrum – beim TLfDI läuten die Alarmglocken....98
3.34 Öffentlich zugänglich aufgestellte Container mit Akten eines Steuerbüros in Gera....100
3.35 Onlineshops: Kreditkartendaten frei Haus?....102
3.36 Datenschutz auch beim Schornsteinfeger....105

3.37 Datenübermittlung von Makler zu Makler – Der TLfDI bezieht Stellung! 106
3.38 Digitale Unterschriften versus Datenschutz 108
3.39 Schreddern? – Aber richtig? 109
3.40 Hilferuf eines Vereins aus dem datenschutzrechtlichen Dickicht 111
3.41 Vereinsberatunng 114
3.42 Herrenlose Akten eines Bauunternehmers 115
3.43 Nachhilfe: Bürger erhält Auskunft 117
3.44 Keine Lastschrift ohne Daten 118
3.45 Jeder kennt jeden – Hausverwaltung gibt Daten weiter 120
3.46 Ich bin du, du bist ich? 123
3.47 Geheimnis: Akten einer Steuerberatungskanzlei 124
3.48 TLfDI kontrolliert Weihnachtsmann ;-) 126

4 Datenschutzkonformität von unternehmensinternen Unterlagen 128
4.1 Datenschutz auch bei Korruptionsbekämpfung 128
4.2 Datenschutz im Sportverein – was dürfen SV, FC und Co.? 131
4.3 Da wird der Hund in der Pfanne verrückt 133
4.4 Falscher Adressat TLfDI 137
4.5 Datenschutz bei der App-Entwicklung 138

5 Meldungen nach § 42a 140
5.1 Leaks 140

6 Videoüberwachung 143
6.1 „1984“ war gestern! 143
6.2 Meldungen nicht nur von Wildkameras 145
6.3 Selbstbedienungsladen ohne Personal, aber mit problematischer Überwachungstechnik? 147
6.4 Rundumüberwachung einer Wohnungsanlage 150
6.5 Video versus Vandalismus – Videogaga? 154
6.6 Pizza mit Draufsicht – Videogaga 1 156
6.7 Big Brother auf dem Marktplatz – Videogaga 2 159
6.8 Videoüberwachung auf Firmengelände – Videogaga 3 161
6.9 Tanken mit Stummfilm – Videogaga 4 164

6.10 Smart-Home-Präsentation: inklusive Videoüberwachung 166
6.11 Video für Baufortschritt – kein Fortschritt – Videogaga 5 167
6.12 Videoüberwachung der Insolvenzmasse 169
6.13 Der (Tür)Spion, der die Nachbarn nicht liebte; Videogaga 6 170
6.14 Man kann den Pelz nicht waschen, ohne sich nass zu machen: Videogaga 7 174
6.15 Bei Klingeln Aufnahme: BDSG? 175
6.16 Fenster zum Hof 176
6.17 Auskunftsverweigerungs(un)recht 179
6.18 Der abgeschottete Nachbar 180
6.19 Postkartenmotiv „Videokamera“ 184
6.20 Videoüberwachung eines öffentlichen Raumes der Stadt Rudolstadt durch Privatperson 185
6.21 Videoüberwachung nicht über den Maschendrahtzaun hinaus? 187
6.22 Videoüberwachung auf eigenem Grundstück zulässig? 190
6.23 Achtung: Im Vogelhaus nistet eine Kamera! – Videogaga 8 191
6.24 Dome 194
6.25 Wanderer zeigen Bein: Videogaga 9 196
6.26 Kamera im Mehrfamilienhaus beliebt: Videogaga 10 197
6.27 Störung des Hausfriedens durch Videoüberwachung – Videogaga 11 198
6.28 Rund um die Uhr ein Blick ins Unternehmen – Videogaga 12 202
6.29 Campingplatzatmosphäre – Videogaga 13 204
6.30 Zeugnisverweigerungsrecht schließt Vorgehen des TLfDI nicht aus 205
6.31 Videoüberwachung – der TLfDI hilft, wenn er weiß, wo: Videogaga 14 206
6.32 Hotelgäste und Mitarbeiter pausenlos auf Video? Videogaga 15 208
6.33 Grundstücksgrenze = Ende der Beobachtungsbefugnis 209
6.34 Und weg ist die Attrappe: Videogaga 16 210

6.35 Kamera als Abschreckung zulässig?: Videogaga 17212
6.36 Videoüberwachung durch Rechtsanwaltskanzlei 213
6.37 Allgemeine Anfragen zur Videoüberwachung 215
6.38 Videoüberwachungsverbesserungsgesetz – Verbesserung? – Anwendbarkeit? 218
6.39 Keine Meldepflicht bei Firmenüberwachung?.....221
6.40 Baden und Entspannen unter Beobachtung – Videogaga 18.....222
6.41 Videoüberwachung im Restaurant – bei nebulösen Angaben keine Beratung.....225
6.42 Datenschutz: durchgesetzt! – Videogaga 19.....227
6.43 Wenn der Datenschutz zweimal klingelt 227
6.44 Videoüberwachung versus Vandalen.....229
6.45 Insolvenz schützt nicht vor Datenschutz – Videogaga 20.....231
6.46 Hinweis auf Videoüberwachung, aber wo ist die Kamera?.....232
6.47 Betreiber einer Videoüberwachung? – Ja Nein Vielleicht; Videogaga 21 233
6.48 Geschützte Fassaden.....235
6.49 Die überwachte Datsche 238
6.50 Hausrecht – Video 239
6.51 Mein schöner Garten! 241
6.52 Video bleibt datenschutzrechtlich schwierig! 242
6.53 Alle Wege führen zum Kindergarten: Videogaga 22 244
6.54 Bewachter Parkplatz 246
6.55 Planung einer Videoüberwachung – der TLfDI hilft auch hier 248
6.56 Nette Familie 249
6.57 Kamerainstallation oder nicht, das ist hier die Frage 250
6.58 Ich glaub, ich steh im Wald 251
6.59 Problemzonen im Autohaus – Fortsetzung.....254
6.60 Ob der Lkw richtig steht, sieht man, wenn die Kamera angeht – Videogaga 23 256
6.61 Streetview outsourced – davon wird’s nicht besser; Videogaga 24.....258
6.62 Die (Un)zulässigkeit von Dashcams oder Die Leiden des (jungen) Hobbyfilmers 259

6.63 Nicht alle Wege führen zum Friedhof 264
6.64 Rundumüberwachung durch den Nachbarbetrieb? .. 265
6.65 Wertvoller Schrott im Fokus – Fortsetzung 268
6.66 Videoüberwachung als Auszugsgrund? 270
6.67 Videoüberwachungskamera auf der anderen Straßenseite 271
6.68 Apotheken-Video – Videogaga 25 273
6.69 Wenn der Thermenbesuch beobachtet wird – Videogaga 26 274
6.70 Wildtierkameras 276
6.71 Spielhalle: Videogaga 27 278
6.72 Fahrgäste im Visier – Videogaga 28 281
6.73 Kameras im Imbiss – Videogaga 29 285
6.74 Mieter unter Beobachtung – Videogaga 30 287
6.75 Videokameras als Türsteherersatz? – Videogaga 31 290

7 Beschäftigtendatenschutz 293
7.1 Videoüberwachung im Freizeitpark 293
7.2 Frau am Facebook-Pranger 295
7.3 (K)ein Kraftaufwand: Videoüberwachung im Fitnessstudio 297
7.4 Mit GPS immer ein Auge auf die Mitarbeiter? 298
7.5 Was ist vor der Inbetriebnahme einer Kamerainstallation zu beachten? 300
7.6 Datenschutz in der Altenhilfe: Wer hat wo- wann-wem geholfen? 303
7.7 Bewerbungsverfahren abgeschlossen – Bewerberdaten gelöscht? 304
7.8 Wenn der Chef weiß, dass der Mitarbeiter zur Konkurrenz will 306
7.9 Betriebsärztliche Untersuchungen: keine automatische Schweigepflichtentbindung im Arbeitsvertrag 308
7.10 Auskunftspflicht von Unternehmen 309
7.11 GPS für Arbeitgeber attraktiv – aber oft unzulässig 311
7.12 Lehrlinge im Fokus – kein Videogaga bei Nichterkennbarkeit 312
7.13 Anfrage zum Passwortschutz von Arbeitsplatzrechnern 313
7.14 Veröffentlichen von Bildern behinderter Menschen 315

7.15 Beschäftigtendatenschutz – lückenlose Leistungs- und Verhaltenskontrolle unzulässig....316
7.16 Satte Rabatte contra Beschäftigtendatenschutz 317
7.17 Arbeitszeitüberwachung: nur datenschutzgerecht, wenn ... – Videogaga 32 319
7.18 Leistungsdruck durch GPS 321
7.19 Gab ein Arbeitsvermittler die Bewerbungsunterlagen seiner Mitarbeiterin ungefragt weiter?....322
7.20 Kündigung wegen Bewerbung in einem anderen Unternehmen?....324
7.21 Jobsuche und alle wissen es....325
7.22 Kontrolle in einem Logistik-Unternehmen....327

8 Werbung....330
8.1 Beschwerde über aufdringliche Telefonwerbung....330
8.2 Auch Werbe-E-Mails entgehen dem Datenschutz nicht 332

9 Auskunfteien....334
9.1 Verhindert die SCHUFA Dispositionskredit? 334
9.2 Überraschung: Ware nur nach Bonitätsabfrage....335
9.3 Schweigen eines Versandhandels....337

10 Gesundheit....340
10.1 Ansteckende Krankheiten sind Privatsphäre, oder nicht? 340
10.2 Antworten zum betriebsärztlichen Datenschutz 342
10.3 Der Apotheker als Ermittlungshelfer der Polizei?...345
10.4 Datenschutz bald verschreibungspflichtig? 347
10.5 Patientendaten unverschlüsselt im IT-Dschungel....348
10.6 Einsicht in die Patientenakte – beim Therapeuten oder bei dessen Anwalt? 351
10.7 Fotoshooting in der Arztpraxis – wenn der Patient ungewollt zum Model wird....354
10.8 Fotoshooting in der Arztpraxis 355
10.9 Datenspeicherung in Apotheke: Kommerz versus Recht....357
10.10 Daten im Wartezimmer?....359
10.11 Datenschutz beim Zahnarzt: TLfDI bohrt nach....360
10.12 Auch Krankenhäuser von DS-GVO betroffen....362

10.13 Schreddern im Krankenhaus 364
10.14 Einwilligungserklärung bei Ärzten – So einfach geht das nicht! 366
10.15 Erwachsene familienversicherte Patienten sind mündig – eine Erhebung von Hauptversichertendaten entfällt damit! 368
10.16 Beratung durch den Amtsarzt verstößt nicht gegen den Datenschutz 369
10.17 Ist die Weitergabe der Personaldaten an die Heimaufsicht erlaubt? 371
10.18 Datenverarbeitung im Auftrag – ein Klinikum war gut vorbereitet 372
10.19 Bestellung von Arzneimitteln mit WhatsApp 375
10.20 Wearables und Gesundheits-Apps immer datenschutzkon-form? 376
10.21 Beschwerde über ein Reinigungsunternehmen wegen nicht korrekt vernichteter Nachweisblätter 377
10.22 Urkundenverifikationsdienst Approbationsurkunden 378

11 Ordnungswidrigkeiten 381
11.1 Bußgelder nehmen stetig zu 381

12 Technischer und organisatorischer Datenschutz 384
12.1 Windows 10, Microsoft-Cloud Deutschland und Windows Office 365 384
12.2 Kritische Infrastruktur – Sektor Gesundheit 386
12.3 Heiße Debatte um den Entwurf einer EU-e-Privacy-Verordnung 387
12.4 Datenschleudern – vom vernetzten Auto 389
12.5 Pflichten sozialer Netzwerke 393
12.6 Google-Analytics 395
12.7 Speicherung von IP-Adressen – Sicherheit oder Datenschutz? 396
12.8 eIDAS – was ist das? 399
12.9 EU- und nationale Cybersicherheit 400
12.10 Internationale Arbeitsgruppe zum Datenschutz in der Tele-kommunikation („Berlin Group“) 402
12.11 Wenn Kühlschränke eiskalt angreifen 403
12.12 Canvas-Fingerprinting 405

12.13 Neues Personalausweis-Gesetz: Daten in Hülle und Fülle für den Staat....407
12.14 WannaCry....408
12.15 Zerstören Sie die Cayla-Puppe – wenn das Spielzeug mithört....410

13 Veranstaltungen....412
13.1 Profiling....412
13.2 Zusammenarbeit mit dem ERFA-Kreis Thüringen..414

14 Vorträge – der TLfDI ist unterwegs!....416

Anlagen

Beschluss der obersten Aufsichtsbehörden im Datenschutz im nicht-öffentlichen Bereich
(Düsseldorfer Kreis am 13./14. September 2016)

Anlage 1 Fortgeltung bisher erteilter Einwilligungen unter der Datenschutz-Grundverordnung....429

Entschließung der 91. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 6./7. April 2016 in Schwerin

Anlage 2 Wearables und Gesundheits-Apps –Sensible Gesundheitsdaten effektiv schützen!....430

Entschließung zwischen den Konferenzen 2017

Anlage 3 Novellierung des Personalausweisgesetzes – Änderungen müssen bürger- und datenschutzfreundlich realisiert werden!....433

Pressemitteilungen 2016

Anlage 4 Gericht bestätigt: Videoüberwachung durch Private in öffentlich zugänglichen Räumen meldepflichtig!....435

Pressemitteilungen 2017

Anlage 5 Meldepflicht für (Wild-)Kameras bestätigt! 436
Anlage 6 Microsoft trifft TLfDI-Wirtschaft und Datenschutzaufsicht – geht das zusammen?-.....437
Anlage 7 Immelborn – AdActa 438

Kurzpapiere

Anlage 8 Verzeichnis von Verarbeitungstätigkeiten –Art. 30 DS-GVO 440
Anlage 9 Aufsichtsbefugnisse/Sanktionen.....444
Anlage 10 Verarbeitung personenbezogener Daten für Werbung 448
Anlage 11 Datenübermittlung in Drittländer.....452
Anlage 12 Datenschutz-Folgenabschätzung, Art. 35 DS-GVO 458
Anlage 13 Auskunftsrecht der betroffenen Person, Art. 15 DS-GVO 467
Anlage 14 Marktortprinzip: Regelungen für außereuropäische Unternehmen 471
Anlage 15 Maßnahmenplan „DS-GVO“ für Unternehmen.....475
Anlage 16 Zertifizierung nach Art. 42 DS-GVO 480
Anlage 17 Informationspflichten bei Dritt- und Direkterhebung 484
Anlage 18 Recht auf Löschung / „Recht auf Vergessenwerden“ 490

Abkürzungsverzeichnis.....494

Stichwortverzeichnis/ Index 498

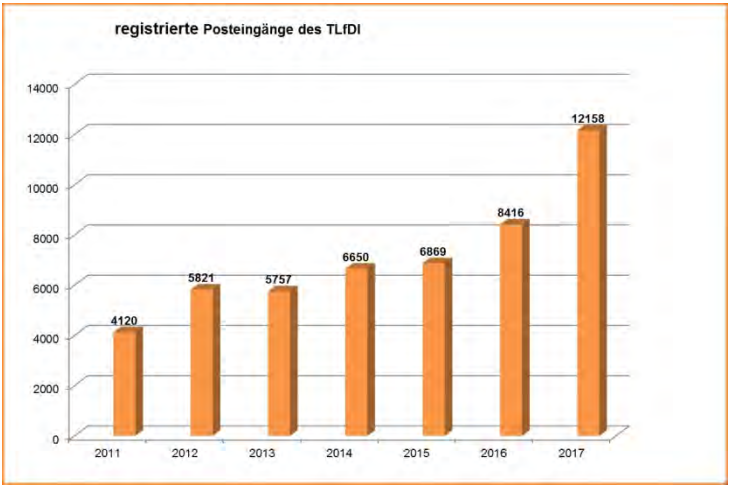
B Nicht-öffentlicher Bereich



Dr. Lutz Hasse

Vorwort

Dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) ist es offenbar gelungen, den Datenschutz im Freistaat Thüringen zu etablieren. Dies zeigt sich nicht nur am erneut signifikanten Umfang des Tätigkeitsberichts, sondern eben auch an der erfreulichen Statistik der Posteingänge.



Hier wird nicht nur optisch deutlich, dass die Nachfrage nach Datenschutz deutlich und stetig steigt, sondern hervorzuheben sind zudem zwei Aspekte: Von 2011 bis 2017 hat sich die Zahl der Posteingänge verdreifacht! Zudem macht der deutliche Anstieg im Jahr 2017 deutlich: Bürgerinnen und Bürger, aber auch Unternehmen, haben nachhaltig die Scheu vor dem TLfDI verloren. Zum anderen wirft die Europäische Datenschutzgrundverordnung (EU-DS-GVO), die im Mai 2018 wirksam werden wird, ihre Schatten voraus. Deutlich spürbar ist in der Behörde des TLfDI der Anstieg der Anfragen von Bürgerinnen und Bürgern und Unternehmen zu dieser neuen Rechtsmaterie. Das alte Bundesdatenschutzgesetz wird zu dem genannten Zeitpunkt ausgedient haben; allerdings enthält die EU-DS-GVO sogenannte Öffnungsklauseln, die es den nationalen Gesetzgeber erlauben, im Rahmen der EU-DS-GVO-Vorgaben eigene Regelungen zu treffen. In einem neuen Bundesdatenschutzgesetz, das ebenfalls im Mai 2018 Wirkung entfalten wird, hat der Bundesgesetzgeber dies getan; das Werk kann nicht durchweg als geglückt angesehen werden, sodass der Fall eintreten kann, dass ein der EU-DS-GVO widersprechendes Bundesdatenschutzgesetz aufgrund des Anwendungsvorrangs des Europarechts nicht zur Umsetzung gelangt. Misslich für den deutschen Rechtsanwender ist zudem, dass künftig nicht mehr ein Blick in das neue Bundesdatenschutzgesetz oder die unmittelbar geltende EU-DS-GVO genügt, sondern ein

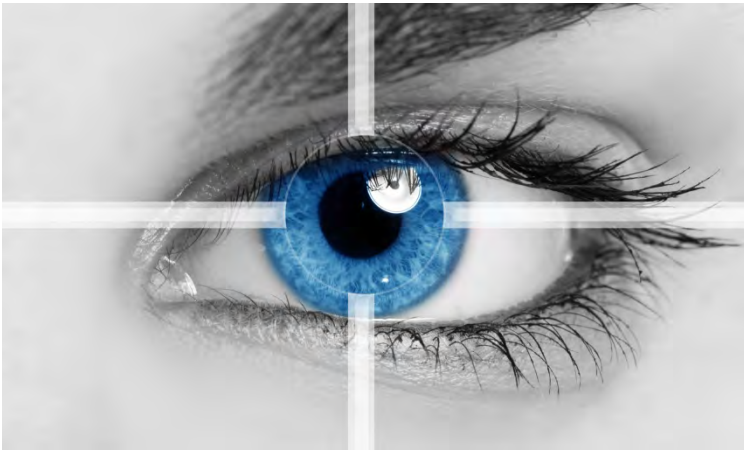
Zusammenlesen beider Gesetzesmaterien erforderlich ist, um den Willen der Gesetzgeber zu ermitteln. Das dürfte auch für spezialisierte Juristen kein leichtes Unterfangen werden – die Bürgerinnen und Bürger dürften hiermit überfordert sein. Der TLfDI ist hier natürlich die richtige Anlaufstelle, um auch komplexe Rechtsfragen zu beantworten.

Ein weites Feld tut sich auf bei der Digitalisierung von Fahrzeugen (Connected Cars), Arbeit 4.0, Industrie 4.0, Internet of Things (IOT) und Internet of Bodies (IoB). Die Bemerkung der Bundeskanzlerin Merkel, Daten seien der Rohstoff der Zukunft, hat aus Datenschutzsicht unheilvolle Aktivitäten ausgelöst und hier und da den Eindruck erweckt, man dürfe alles Menschenmögliche unternehmen, um Daten zu ökonomisieren. In den Hintergrund gerückt ist hierbei offenbar, dass die Daten-Kommerzialisierung nur im Rahmen des rechtlich Möglichen erfolgen darf. Hier ist sorgsam darauf zu achten, dass das Grundrecht der informationellen Selbstbestimmung nicht unter die Räder gerät. Technische Entwicklungen und deren Anwendungen setzen Fakten, die datenschutzrechtlich nicht abgeklopft sind. Das ist nicht nur eine Meinung des TLfDI und anderer Landesbeauftragter, sondern auch Meinung der Akteure selbst. Der Kontakt zwischen TLfDI und Thüringer Wirtschafts-Digitalministerium steht, um in Thüringen datenschutzrechtskonforme Wege zu beschreiten, was durchaus möglich ist, ohne Wirtschaftsinteressen übermäßig zu belasten. Dessen ungeachtet hat der TLfDI die Kontakte zu den Industrie- und Handelskammern sowie zur Handwerkskammer intensiviert, was sich nicht nur in der gemeinsamen Erstellung von Flyern und Informationsblättern niederschlägt, sondern von zunehmender Bedeutung dafür ist, dass über die genannten Organisationen die erwähnten Neuerungen im Datenschutzrecht an die Wirtschaftsakteure auch künftig in verstärktem Maße gesteuert werden können. Der TLfDI sieht seine Aufgabe auch künftig darin, die Verarbeitung personenbezogener Daten im Vorfeld mit den Unternehmen zu erörtern, um allen Beteiligten Verwaltungs- und Bußgeldverfahren zu ersparen.

Auch an dieser Stelle möchte ich es nicht versäumen meinen Mitarbeiterinnen und Mitarbeitern herzlich für ihr Engagement und ihre Motivation, für den Datenschutz zu streiten, zu danken! Ohne ein solches schlagkräftiges Team stünde der Datenschutz im Freistaat Thüringen im Vergleich mit den anderen Bundesländern nicht auf einem der vorderen Plätze.

Zur einfacheren Navigierbarkeit wurden die in diesem Tätigkeitsbericht verwendeten Links zusätzlich mit QR-Codes codiert. Die QR-Codes enthalten den Link in gerätelesbarer Form (beispielsweise der QR-Code links: https://www.tlfdi.de/tlfdi/). Dadurch kann auf Geräten mit Kamera (z. B. Smartphones oder Tablets) und einer entsprechenden Software der Link durch das Gerät wieder decodiert und „Abschreibfehler“ können vermieden werden. Für Android-Smartphones kann der „Barcode Scanner“ des Entwicklers Marty Mouse in der Version 1.0 empfohlen werden, da hier Open-Source-Software genutzt wird und die App nur minimale Funktionen besitzt. Für iOS ist dem TLfDI keine datenschutzgerechte App bekannt.





Eye close-up - © Minerva Studio / Fotolia.com

1 Schwerpunkte im Berichtszeitraum

Leider ungebrochen ist der Trend in Thüringen, Videotechnik im privaten Bereich, aber auch in Unternehmen einzusetzen. Verstärkt wird dieser Trend durch den Einsatz von sogenannten Dashcams in Fahrzeugen, durch Kameras in Fahrrad- und Motorradhelmen und durch Drohnen mit ausgefeilter Videotechnik. Dass Videokameras einer Meldepflicht gemäß § 4d Bundesdatenschutzgesetz unterliegen – so jüngst das OVG Saarlouis –, scheint noch nicht bei jedem Videobetreiber angekommen zu sein, trotz mehrfacher Hinweise des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) dazu. Das Versäumen der genannten Meldepflicht stellt eine Ordnungswidrigkeit dar. Die Rechtsprechung insbesondere zu Dashcams ist noch uneinheitlich, aus Sicht des TLfDI zeichnet sich indes inzwischen die Tendenz ab, Dashcams grundsätzlich für datenschutzrechtswidrig zu erklären, wenn fortlaufend personenbezogene Daten Dritter erhoben und weiterverarbeitet werden. Zahlreiche Verwaltungsgerichts- und Bußgeldverfahren nicht nur in Videoangelegenheiten hat der TLfDI neuerdings zu bearbeiten, sodass der Gedanke naheliegt, in der Behörde ein eigenes Justiziariat einzurichten.
Der TLfDI bleibt auch von Wahlkämpfen nicht verschont und war bzw. ist gehalten, den datenschutzrechtskonformen Einsatz von Wahlkampf-Apps zu überprüfen. Mehrere Landesdatenschutzbeauf-

tragte sind in diesen Prozess involviert, und man wird am Ende dieses Prozesses sehen, ob wir auch in diesem sensiblen Bereich unter Auswertung von Big Data auf dem Weg in amerikanische Verhältnisse sind, wo der gläserne Bürger längst die neue Spezies ist. „No Privacy“ mag für viele schick sein, steht indes im Wiederspruch zum Grundrecht der informationellen Selbstbestimmung, dessen Bedeutung den Bürgerinnen und Bürgern offenbar immer deutlicher wird.
Die Landesdatenschutzbeauftragten stehen mit der Versicherungswirtschaft in intensiven Verhandlungen, um auch vor dem Hintergrund der künftigen Europäischen Datenschutz-Grundverordnung (EU-DS-GVO) Datenübermittlungen in das außereuropäische Ausland abzustimmen. Die Digitalisierung macht auch im Beschäftigtendatenschutz nicht halt. Der Einsatz von Videotechnik, GPS und anderen Leistungskontrollmechanismen beschäftigt den TLfDI in zunehmendem Maße. Nicht selten wird eine verdeckte Leistungskontrolle der Mitarbeiterinnen und Mitarbeiter kaschiert mit dem Scheinargument, die eingesetzte Technik sorge für die Sicherheit des Mitarbeiters bzw. der Mitarbeiterin. Der TLfDI konnte im Berichtszeitraum Auswüchsen in dieser Richtung wirksam entgegenwirken.
Auch im Gesundheitsbereich hält die Digitalisierung an. Die Krankenhausinformationssysteme werden leistungsfähiger, können damit den Datenschutz immer besser abbilden, sind allerdings auch in der Lage, immer größere Datenmengen zu bestimmten Zwecken zu verarbeiten. Datenflüsse zwischen verschiedenen Einrichtungen des Gesundheitswesens bedürfen klarer Regelungen bzw. der Einwilligung eines informierten Patienten. Beides lässt bisweilen zu wünschen übrig, allerdings ist es dem TLfDI in Kooperation mit der Landeskrankenhausgesellschaft Thüringen e. V. gelungen, datenschutzrechtskonforme Lösungen zu finden, die auch in der Praxis Akzeptanz finden.
Die große Dynamik bei der Kommerzialisierung von Daten, die von Big Data, Datamining und dem intransparenten Einsatz von Algorithmen befeuert wird, sollte nicht nur die Landesdatenschutzbeauftragten zum Nachdenken zwingen. In fortschreitendem Tempo setzen Entwicklungen ein, denen der Gesetzgeber nicht mehr Herr zu werden scheint. Das Grundrecht der informationellen Selbstbestimmung – so das Bundesverfassungsgericht – wurzelt in der Menschenwürde. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt (Artikel 1 Abs. 1 Satz 2 Grundgesetz). Die augenfälligen Bedrohungen des Grundrechts der informationellen Selbst-

bestimmung, gerade auch im Unternehmensbereich, könnten und sollten daher durchaus deutlichere staatliche Aktivitäten zum Schutz dieses Grundrechts auslösen.



Datenschutz (Anwalt, Datenschutzbeauftragter) - © fotodo / fotolia.com

2 Der betriebliche Datenschutzbeauftragte

2.1 Europäische Datenschutz-Grundverordnung: Unternehmen fragen – TLfDI informiert

Im Berichtszeitraum wandte sich ein Mitarbeiter eines Unternehmens an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und erkundigte sich nach den Voraussetzungen der Bestellpflicht eines behördlichen Datenschutzbeauftragten (bDSB) nach der europäischen Datenschutz-Grundverordnung (DS-GVO). Er wollte wissen, inwieweit Datenschutzbeauftragte in Unternehmen bzw. externe Datenschutzbeauftragte unter Geltung der Datenschutz-Grundverordnung noch benötigt werden bzw. ob in der Datenschutz-Grundverordnung das Bestellen eines Datenschutzbeauftragten (intern oder extern) geregelt ist.
Nach derzeitigem Stand stellt sich die Rechtslage folgendermaßen dar:
In Artikel 37 Absatz 1 DS-GVO ist klar definiert, wann Verantwortliche und Auftragsdatenverarbeiter einen internen Datenschutzbeauftragten zu benennen haben. Und zwar in drei Fällen. Zunächst haben

öffentliche Stellen, sofern sie personenbezogene Daten verarbeiten, stets einen Datenschutzbeauftragen zu bestellen. Ausgenommen sind Gerichte im Rahmen rechtssprechender Tätigkeit. Nicht-öffentliche Stellen, also natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts, haben einen Datenschutzbeauftragten zu bestellen, wenn deren Kerntätigkeit oder die Kerntätigkeit desjenigen, der Daten im Auftrag verarbeitet (Auftragsdatenverarbeitung), in einer Datenverarbeitung besteht,

- die aufgrund ihres Zwecks oder ihres Umfangs eine umfangreiche, regelmäßige und systematische Beobachtung von betroffenen Personen erfordert oder
- die eine umfangreiche Verarbeitung von Daten, die nach Artikel 9 oder 10 DS-GVO besonders schutzwürdig sind, umfasst.

Der Erwägungsgrund 97 zum Artikel 37 DS-GVO stellt klar, dass das „Kerngeschäft“ die Hauptaktivität des Unternehmens meint. Bloße Nebentätigkeiten sollen nicht darunter fallen.

Verantwortliche oder Auftragsdatenverarbeiter können selbstverständlich auch freiwillig einen Datenschutzbeauftragten bestellen. Artikel 37 Abs. 4 DS-GVO enthält aber auch eine Öffnungsklausel, mit der den Mitgliedsstaaten die Möglichkeit eingeräumt wird, im nationalen Recht für weitere Fälle die Bestellung eines Datenschutzbeauftragten vorschreiben zu können.

Hiervon hat der Bundesgesetzgeber Gebrauch gemacht und in § 38 des neuen Bundesdatenschutzgesetzes (BDSG) eine Regelung geschaffen, die über die o. g. Bestellpflichten hinausgeht. Hier heißt es im Absatz 1, ergänzend zum Artikel 37 Absatz 1 Buchstabe b und c DS-GVO, die Verantwortlichen und der Auftragsdatenverarbeiter haben einen Datenschutzbeauftragten zu benennen, soweit sie in der Regel mindestens 10 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen. Des Weiteren haben sie einen Datenschutzbeauftragten zu benennen, wenn Verarbeitungen vorgenommen werden, die einer Datenschutzfolgenabschätzung nach Artikel 35 DS-GVO unterliegen. Auch wenn personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Marktforschung verarbeitet werden, haben die Verantwortlichen unabhängig von der Anzahl der mit der Verarbeitung beschäftigten Personen einen Datenschutzbeauftragten zu benennen.

Artikel 37 Abs. 1 DS-GVO regelt die Benennung eines Datenschutzbeauftragten. Zu beachten sind die in Absatz 4 benannten Öffnungsklauseln. Zum einen können Datenschutzbeauftragte freiwillig bestellt werden und zum anderen haben die Mitgliedstaaten die Möglichkeit, im nationalen Recht weitere Fälle der Bestellung eines Datenschutzbeauftragten zu regeln. § 38 BDSG besagt, dass – ergänzend zum Artikel 37 Absatz 1 Buchstabe b und c DS-GVO – die Verantwortlichen und der Auftragsverarbeiter einen Datenschutzbeauftragten zu benennen haben, soweit sie in der Regel mindestens 10 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen. Des Weiteren haben sie einen Datenschutzbeauftragten zu benennen, wenn Verarbeitungen vorgenommen werden, die einer Datenschutzfolgenabschätzung nach Artikel 35 DS-GVO unterliegen. Auch wenn personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Marktforschung verarbeitet werden, haben sie unabhängig von der Anzahl der mit der Verarbeitung beschäftigten Personen einen Datenschutzbeauftragten zu benennen.

2.2 Darf ein IT-Mitarbeiter gleichzeitig betrieblicher Datenschutzbeauftragter sein?

Im Berichtszeitraum bat ein IT-Mitarbeiter eines Unternehmens den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) um Mitteilung, ob er im Hinblick auf die Qualifikationsvoraussetzungen für die Position des betrieblichen Datenschutzbeauftragten (bDSB) seiner Firma in Betracht käme. Die Geschäftsführung seiner Firma würde dieser Tätigkeit zustimmen, sofern der Mitarbeiter eine entsprechende Fortbildung absolviert und keine Bedenken im Hinblick auf Interessenkonflikte bestünden.
Der IT-Mitarbeiter war bei einer Ingenieursgesellschaft angestellt, die zu einer Firmengruppe gehörte und vollständig in deren Netzwerk integriert war. Alle relevanten IT-Entscheidungen wurden vom Hauptsitz getroffen und von den Standorten umgesetzt. Der Mitarbeiter war an „seinem“ Standort IT-Verantwortlicher und nur der dortigen Geschäftsführung als Mitarbeiter unterstellt. Ein Weisungsrecht im Rahmen seines Arbeitsverhältnisses bestand nur seitens der Geschäftsführung an „seinem“ Standort und nicht von Seiten des Hauptsitzes.

Nach Angaben des IT-Mitarbeiters wurden alle relevanten IT-Entscheidungen vom Hauptsitz der Firmengruppe vorgegeben, die lokalen Administratoren erhielten die Berechtigungen von dort und mussten die IT-Richtlinien an den jeweiligen Standorten umsetzen. Ebenfalls wurden die User-Protokolle sowie die persönlichen Daten der User über Gruppenrichtlinien zentral vom Hauptsitz administriert. Die jeweiligen Standortadministratoren haben keinen eigenen Zugriff; die Rechtevergabe erfolgte vom Hauptsitz aus, lediglich die Vergabe der Zugriffsrechte auf Projektdaten erfolgte eigenständig an den Standorten.
Der TLfDI hatte gegen die Bestellung des IT-Mitarbeiters zum betrieblichen Datenschutzbeauftragten keine Bedenken. Er wies jedoch darauf hin, dass das Unternehmen darauf achten müsse, dass beide Aufgabenbereiche des Mitarbeiters – als bDSB und als nachgeordneter IT-Administrator in der Ingenieursgesellschaft – klar voneinander getrennt sind. Die klare Trennung dieser Positionen voneinander muss gewährleistet und dokumentiert werden; hierfür trägt das Unternehmen die Verantwortung ebenso wie für die ordnungsgemäße Bestellung des bDSB.
Seine Auffassung begründete der TLfDI folgendermaßen: Der Gesetzgeber hat in § 4f Abs. 2 Satz 1 Bundesdatenschutzgesetz (BDSG) zwei Qualifikationsmerkmale für einen bDSB festgelegt: Fachkunde und Zuverlässigkeit. Hieraus lässt sich jedoch kein festes Anforderungsprofil für diese Funktion bilden. Eine ausreichende Fachkunde kann nur dann angenommen werden, wenn die Person sowohl über entsprechende rechtliche als auch organisatorische und technische Kenntnisse verfügt. Um die Anforderungen und Ziele von datenschutzrelevanten rechtlichen Regelungen zu erkennen und deren Konsequenzen für die verantwortliche Stelle bewerten zu können, sind ausreichende rechtliche Kenntnisse zwingend erforderlich. Allgemeine überblicksartige Kenntnisse wären hierfür nicht ausreichend.
Dies liegt darin begründet, dass das Bundesdatenschutzgesetz (BDSG) durch eine ungewöhnlich hohe Zahl an Generalklauseln gekennzeichnet ist. Daher muss der bDSB in der Lage sein, eine datenschutzkonforme Interpretation dieser Klauseln auch dann zu vertreten, wenn die vom Gesetzgeber geschaffenen Normen nur auf den ersten Blick keine klare Lösung aufzeigen, bei näherer Betrachtung jedoch Interpretationsspielraum zulassen.

Ein zu ernennender bDSB muss darüber hinaus sehr zuverlässig sein, sowohl in objektiver wie in subjektiver Hinsicht. Dabei beziehen sich die subjektiven Aspekte auf persönliche Eigenschaften und die objektiven Faktoren auf mögliche Interessenkollisionen. Diesbezüglich ist darauf zu achten, dass kein Interessenkonflikt zwischen der arbeitsstellenbezogenen Tätigkeit als IT-Mitarbeiter und den inhaltlichen Aufgaben des bDSB im Unternehmen besteht. Die subjektiven Aspekte hingegen können vom TLfDI nicht überprüft werden. Dabei handelt es sich um in der Person liegende Gründe, die zu einer Unzuverlässigkeit führen, wie beispielsweise dem aus der Vergangenheit bekannten sorglosen Umgang mit personenbezogenen Daten.
Grundsätzlich ist davon auszugehen, dass ein IT-Leiter und ein bDSB widerstrebende Interessen haben, sodass ein IT-Mitarbeiter nicht als bDSB bestellt werden sollte. Dies legt auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) auf seiner Website dar: „*Interessenkonflikte können insbesondere dann auftreten, wenn der bDSB gleichzeitig Aufgaben in den Bereichen Personal, Informationstechnik oder in Organisationseinheiten mit besonders umfangreicher oder sensitiver Verarbeitung von personenbezogenen Daten wahrnimmt oder Geheimschutzbeauftragter ist.*“

(vgl.https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02502.html). Jedoch gibt das BSI auf seiner Website unter M 2.502, Regelung der Verantwortlichkeiten im Bereich Datenschutz, im Abschnitt „Bestellung eines Datenschutzbeauftragten“ auch nähere Hinweise, wie entsprechende Interessenkonflikte gelöst werden können: *„Möglich ist (…) die Zusammenlegung der Funktionen des bDSB mit denen des IT-Sicherheitsbeauftragten. Ist der IT-Sicherheitsbeauftragte organisatorisch unabhängig von der für die IT verantwortlichen Organisationseinheit eingerichtet, ist die Zusammenfassung in einer Hand empfehlenswert.“ (vgl. a.a.O.)*
Aufgrund der vom IT-Mitarbeiter beschriebenen Firmenorganisation und seines Arbeitsbereiches bestand aus Sicht des TLfDI ein Abhängigkeitsverhältnis des Mitarbeiters als Teil des regionalen IT-Bereichs zum IT-Leiter der Firmengruppe am Hauptsitz. Daher sollte

ergänzend dokumentiert werden, wie die Handlungsfähigkeit als bDSB gegeben ist, wenn IT-Richtlinien des Hauptstandorts gegen die Interessen des bDSB verstoßen. Weiterhin ergibt sich der notwendige Ergänzungsbedarf aufgrund der Tatsache, dass die Ingenieursgesellschaft eigenständig arbeitet und IT-bezogen lediglich Richtlinien und Vorgaben der Firmengruppe in Bezug auf IT-Strategie, Sicherheitseinstellungen, User-Rechte umsetzt.
Da Dienstleistungen gegenseitig in Rechnung gestellt werden, war nach Ansicht des TLfDI auch vertragsbezogen davon auszugehen, dass eine formale Unabhängigkeit zwischen der Ingenieursgesellschaft und der Firmengruppe bestand. Die Ausführungen des IT-Mitarbeiters zu seiner Arbeit als Softwareentwickler ließen zweifelsfrei erkennen, dass in Bezug auf diese Tätigkeit kein Widerspruch zu einer möglichen Bestellung zum bDSG vorlag.
Der TLfDI empfahl dem IT-Mitarbeiter abschließend, vor der Berufung zum bDSB für das Erlangen der entsprechende Fachkunde eine Schulung zu belegen, sofern die nötigen Kenntnisse noch nicht vorhanden sein sollten, da mangelnde Sachkunde dazu führt, dass die Bestellung unwirksam ist.
Klarstellend wird darauf hingewiesen, dass ein IT-Mitarbeiter nichts mit der Position IT-Sicherheitsbeauftragter zu tun hat. Bei Letzterem besteht wegen der Kollision von Aufgaben und Beratungsverpflichtungen immer ein Interessenskonflikt, mit der Folge der Unzulässigkeit der Bestellung als bDSB, s. a. Beitrag 2.3.

In Einzelfällen kann ein Mitarbeiter der IT-Abteilung auch bDSB des Unternehmens sein. Es muss jedoch sorgfältig sichergestellt werden, dass keine Interessenskollisionen bestehen. Stellt der TLfDI bei einer späteren Prüfung solche Kollisionen fest, ist die Bestellung ab Bestehen dieser Kollisionen als unwirksam zu bewerten. Dies führt, wenn das Unternehmen zur Bestellung eines bDSB verpflichtet ist, in der Regel auch zu einem Ordnungswidrigkeitenverfahren.

2.3 Darf ein IT-Sicherheitsbeauftragter gleichzeitig Datenschutzbeauftragter des Unternehmens sein?

Im Berichtszeitraum richtete der Mitarbeiter eines Unternehmens an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit TLfDI) die Anfrage, ob die Funktionen des IT-Sicherheitsbeauftragten und die des internen betrieblichen Daten-

schutzbeauftragter (bDSB) von dem gleichen Mitarbeiter ausgeübt werden können oder ob dies zu Interessenkonflikten führe.
Nach Prüfung des Sachverhalts gelangte der TLfDI zu der Ansicht, dass in dieser Konstellation Interessenkonflikte drohen und daher eine Bestellung des besagten Mitarbeiters zum bDSB nicht wirksam wäre. Nach Auffassung des TLfDI ist nicht pauschal davon auszugehen, dass ein IT-Sicherheitsbeauftragter nicht zuverlässig im Sinne des § 4f Abs. 2 Satz 1 Bundesdatenschutzgesetz (BDSG) ist. Das Bundesdatenschutz (BDSG) hat in § 4f Abs. 2 Satz 1 BDSG die Bestellung des Beauftragten an zwei Qualifikationsmerkmale geknüpft: Fachkunde und Zuverlässigkeit. Bei der Zuverlässigkeit sind subjektive genauso wie objektive Faktoren zu bedenken. Die subjektiven Aspekte beziehen sich auf persönliche Eigenschaften, die objektiven auf mögliche Interessenkollisionen. Eine Bestellung zum bDSB kann daher nur erfolgen, wenn neben den subjektiven Voraussetzungen keine Interessenkollisionen zwischen den unterschiedlichen Arbeitsfunktionen vorliegen.
Die Kenntnisse und Erfahrungen des IT-Sicherheitsbeauftragten im Bereich der Datensicherheit sprechen zwar für eine Bestellung zum bDSB, jedoch wird die Zuverlässigkeit durch mögliche Interessenkonflikte infrage gestellt. Der IT-Sicherheitsbeauftragte eines Unternehmens ist gemäß seiner Position und Funktion berechtigt, Grundsätze festzulegen, nach denen sich das Unternehmen als verantwortliche Stelle zur Bestellung des bDSB richten muss. Insofern trägt er hierfür auch die Verantwortung. Darüber hinaus besitzt er eine unabhängige und organisatorisch herausgehobene Stellung. Er ist in dieser Rolle der Unternehmensführung direkt unterstellt und berichtet an diese. Sollte er eigenverantwortlich für die Umsetzung der IT-Sicherheitsstandards zuständig und somit direkt dem Leiter der EDV unterstellt sein, würde dies im Widerspruch zur unabhängigen Stellung eines Datenschutzbeauftragten stehen. Die Zuverlässigkeit im Sinne des § 4f Abs. 2 Satz 1 BDSG könnte daher nicht mehr sichergestellt werden.
Darüber hinaus muss bei der Abgrenzung, wann die erforderliche Zuverlässigkeit aufgrund bestehender Interessenkollision nicht mehr gegeben ist, der Einsatzbereich der betroffenen Person als Arbeitnehmer besonders berücksichtigt werden. Dies betrifft insbesondere die Frage, ob die Person auch damit betraut ist, die datenschutzkonforme Verarbeitung personenbezogener Daten (Einzelangaben über persönliche und wirtschaftliche Verhältnisse der Beschäftigten ge-

mäß § 3 Abs. 1 BDSG), zu sichern. In einer solchen Konstellation würde die parallele Wahrnehmung der gesetzlichen Aufgaben als bDSB auf eine Kontrolle der eigenen Arbeit hinauslaufen (vgl. BDSG/Simitis, 8. Aufl., § 4f Rn. 100 ff.). Denn im Rahmen seiner Tätigkeit muss der bDSB auf die Einhaltung aller datenschutzrechtlichen Bestimmungen im Bereich personenbezogener Daten hinwirken (§ 4f Abs. 1 Satz 1 BDSG).
Grundsätzlich sind daher beide Funktionen nach Auffassung des TLfDI nicht miteinander vereinbar.

Die Funktionen des IT-Sicherheitsbeauftragten und die des betriebsinternen Datenschutzbeauftragten (bDSB) eines Unternehmens durch den gleichen Mitarbeiter kann zu Interessenkollisionen führen. Dies ist insbesondere der Fall, wenn der regelmäßige Arbeitsbereich des Mitarbeiters sich auch auf die Sicherung der datenschutzkonformen Verarbeitung personenbezogener Daten bezieht. In diesem Falle würde die parallele Wahrnehmung der Aufgaben des bDSB auf eine Kontrolle der eigenen Arbeit hinauslaufen. Beide Funktionen sind daher grundsätzlich nicht miteinander vereinbar.

2.4 Zu viele auf einmal: Bestellung einer Rechtsanwalts-Partnerschaft zum Datenschutzbeauftragten

Im Berichtszeitraum wandte sich eine Rechtsanwalts-Partnergesellschaft mit einem Beratungsersuchen an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Kern der Beratungsanfrage war, ob der TLfDI es für zulässig erachtet, dass sich eine Partnerschaftsgesellschaft selbst zum betrieblichen Datenschutzbeauftragten bestellen lässt.
Die Rechtsanwalts-Partnerschaftsgesellschaft vertritt dabei die Auffassung, dass sie als Partnerschaft natürlicher Personen als externer Datenschutzbeauftragter auftreten kann. Sie sei keine juristische Person und verfüge über Fachkunde und Zuverlässigkeit, wie es vom Bundesdatenschutzgesetz (BDSG) gefordert wird. Sie stelle eine Bündelung von Expertenwissen bei wachsendem Bedarf an Professionalisierung und Spezialisierung des Datenschutzbeauftragten dar und gewährleiste darüber hinaus im Gegensatz zu einzelnen juristischen Personen höhere Kontinuität und Verfügbarkeit in der Beratung von Mandanten.

Grundsätzlich ist es nach dem BDSG möglich, dass nicht-öffentliche Stellen statt eines internen einen externen Datenschutzbeauftragten bestellen. Problematisch bei der Bestellung einer Rechtsanwalts-Partnergesellschaft ist jedoch, dass die Funktion des Datenschutzbeauftragten durch eine unbestimmte Personengruppe mit gegebenenfalls wechselndem Personenbestand wahrgenommen würde.
Das BDSG regelt hierzu in § 4f Abs. 2 Satz 3, 1. HS Folgendes:

[…]Zum Beauftragten für den Datenschutz kann auch eine Person außerhalb der verantwortlichen Stelle bestellt werden;[…]

Zunächst ist dem Gesetzeswortlaut zu entnehmen, dass es sich beim externen Beauftragten um eine Person handeln muss. Dem deutschen Recht sind nur zwei Arten von Personen bekannt, die natürliche wie auch die juristische Person.
Dabei sind natürliche Personen alle Menschen. Juristische Personen hingegen sind eine Erfindung des Gesetzgebers. Sie existieren nur auf dem Papier und werden, um handlungsfähig zu sein, von natürlichen Personen vertreten. Gängigster Vertreter einer juristischen Person ist Beispielsweise die GmbH.
Bei einer Partnerschaftsgesellschaft handelt es sich jedoch um eine Personengesellschaft und damit um einen Zusammenschluss aus mehreren natürlichen und/oder juristischen Personen. Eine Personengesellschaft ist daher bereits nach dem Wortlaut des Gesetzes ausgeschlossen.
Dies lässt sich ebenfalls historisch und europarechtlich untermauern. Weder das BDSG 77 noch das BDSG 90 (in beiden Fällen handelt es sich um alte Versionen des Bundesdatenschutzgesetzes) kannten den externen Datenschutzbeauftragten. Es war lediglich vom Datenschutzbeauftragten als Angestelltem innerhalb der verantwortlichen Stelle die Rede, also ausschließlich von einer natürlichen Person.
§ 4f Abs. 2 Satz 3 BDSG wurde erst durch Umsetzung der Datenschutzrichtlinie in das BDSG aufgenommen. Im Erwägungsgrund 49 zu dieser Richtlinie heißt es:
„Ein solcher Beauftragter, ob Angestellter des für die Verarbeitung Verantwortlichen oder externer Beauftragter, muss seine Aufgaben in vollständiger Unabhängigkeit ausüben können“.
Dem kann entnommen werden, dass auch der europäische Gesetzgeber ausschließlich natürliche Personen als interne wie auch externe betriebliche Datenschutzbeauftragte im Sinn hatte, als die entsprechende Richtlinie verfasst wurde.

Der TLfDI hat mitgeteilt, dass er dieser Auffassung nicht folge und die Bestellung einer Gesellschaft als betrieblicher Datenschutzbeauftragter nicht für zulässig erachtet.

Wenn Sie einen betrieblichen Datenschutzbeauftragten bestellen, muss es sich dabei um eine natürliche Person handeln. Andernfalls – etwa im Falle der Bestellung einer Personalgesellschaft – ist eine eventuelle Bestellung unwirksam. Mögliche Folge ist dann ein Bußgeldverfahren.

2.5 Bestellung eines Datenschutzbeauftragten

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) haben im Berichtszeitraum immer wieder Anfragen zur Bestellpflicht, zu den Aufgaben und der Stellung des betrieblichen Datenschutzbeauftragten (bDSB) im Unternehmen erreicht.
Der bDSB ist von nicht-öffentlichen Stellen, also von Unternehmen, immer dann notwendigerweise zu bestellen, wenn die Anzahl der mit der automatisierten Verarbeitung beschäftigten Personen mehr als neun beträgt, § 4f Abs. 1 Satz 4 BDSG. Bei einer nicht-automatisierten Verarbeitung personenbezogener Daten ist ein Beauftragter immer dann zu bestellen, wenn mindestens zwanzig Personen dabei beschäftigt werden, § 4f Abs. 1 Satz 3 BDSG.
In Bezug auf die „Stelle“, die den Datenschutzbeauftragten bestellen muss, handelt es sich um die konkret betroffene juristische Person, Personengesellschaft oder Einzelperson. Gleichgültig ist, wie das Unternehmen organisatorisch im Einzelnen ausgestaltet ist und ob es aus einem oder mehreren Betrieben besteht. Für die Bewertung, wer „Stelle“ im Sinne des § 4f ist, zählt als Anknüpfungspunkt nur die jeweils rechtliche Einheit. Soweit ein Unternehmen also in mehrere rechtlich selbstständige Einheiten unterteilt ist, hat jede von ihnen einen eigenen bDSB zu bestellen.
Es kann sowohl ein interner Datenschutzbeauftragter als auch ein externer Datenschutzbeauftragter ernannt werden. Der interne Beauftragte übt seine Kontrollfunktion immer nur im Rahmen einer bestimmten verantwortlichen Stelle aus, bei der er selbst auch tätig ist. Der externe Beauftragte übt regelmäßig für mehrere oder eine Vielzahl von verantwortlichen Stellen die Kontrolle aus. Er ist selbst nicht in dem Unternehmen beschäftigt, sondern ist im Rahmen seiner

selbstständigen Tätigkeit für mehrere Unternehmen zuständig. Interne sowie externe Beauftragte unterliegen dabei jedoch den gleichen rechtlichen Anforderungen, vgl. Simitis, BDSG-Kommentar, § 4f, Rn. 46f.

Bei der Ernennung eines Beauftragten sind die Formerfordernisse des § 4f Abs. 1 Satz 2 BDSG zu beachten. Danach muss der Beauftragte spätestens einen Monat nach Beginn der Verarbeitung bei der verantwortlichen Stelle bestellt sein. Diese Bestellung hat schriftlich zu erfolgen, § 4 Abs. 1 Satz 1 BDSG. Das Erfordernis der Schriftlichkeit verlangt daher eine von beiden Parteien unterschriebene Urkunde. Die Schriftform ist zudem konstitutiv, d. h., fehlt es an einer solchen, ist die Verpflichtung zur Bestellung eines Beauftragten als nicht erfüllt anzusehen. Diese Verfehlung ist im Rahmen des BDSG auch mit einem Bußgeld bewehrt, § 43 Abs. 1 Nr. 2 BDSG.

Die Bestellung des Beauftragten ist weiterhin an zwei entscheidende Qualifikationsmerkmale geknüpft: Fachkunde und Zuverlässigkeit.

Die geforderte Fachkunde nach § 4f Abs. 2 Satz 1 BDSG beinhaltet Kenntnisse in rechtlicher, organisatorischer und technischer Hinsicht. Der Beauftragte muss über ausreichende rechtliche Kenntnisse verfügen, um den Hintergrund, Anforderungen und Ziel der datenschutzrelevanten rechtlichen Regelungen erkennen zu können und damit auch Rückschlüsse auf die möglichen Konsequenzen für die verantwortliche Stelle ziehen zu können. Allein summarische Kenntnisse sind an dieser Stelle nicht ausreichend.

Weiterhin sind organisatorische Kenntnisse notwendig, um Entscheidungsabläufe und Strukturen nachvollziehen und die ggf. notwendigen Korrekturen zur Erhaltung der datenschutzrechtlichen Konformität vornehmen zu können.

Schlussendlich muss der Beauftragte auch über technische Kenntnisse verfügen, da diese zu den Grundvoraussetzungen der Kontrollkompetenz eines jeden Beauftragten zählen.

Die geforderte Zuverlässigkeit des Beauftragten ist sowohl in subjektiver als auch in objektiver Hinsicht zu bewerten. Der Beauftragte sollte sich also in seinem bisherigen Verhalten hinsichtlich etwaiger datenschutzrechtlicher Verstöße unauffällig gezeigt haben.

In objektiver Hinsicht setzt eine verlässliche Kontrolle eine klare Trennung zwischen der verantwortlichen Stelle und dem Beauftragten voraus. Durch diese Trennung werden Interessenkonflikte vermieden. Diese entstehen immer dann, wenn der Beauftragte im Rahmen seiner Tätigkeit Entscheidungen zu treffen hat, die auch

datenschutzrechtliche Belange berühren. Der Interessenkonflikt ist am deutlichsten bei Firmeninhabern, Geschäftsführern, Vorständen oder sonstigen mit der Leitung der verantwortlichen Stelle betrauten Personen. Durch ihre Funktion und Position sind sie berechtigt, Grundsätze festzulegen, nach denen sich die Stelle bei ihrer Tätigkeit richten muss. Im Fokus stehen daher die Ziele und Interessen der verantwortlichen Stelle. Der Datenschutz würde hinter diesen an zweiter Stelle stehen und die Gefahr besteht, dass er aus der Sicht der Erwartungen der verantwortlichen Stelle interpretiert wird, was eine massive Interessenkollision darstellt. Diese Interessenkollision steht auch bei leitenden Angestellten wie Leitern der EDV-Abteilung, Marketingleitern, Personalleitern, Leitern der Rechtsabteilung, Leitern der Revisionsabteilung, Vertriebs- und Betriebsleitern im Raum, da diese sich im Rahmen ihrer Tätigkeit mit der Verarbeitung von personenbezogenen Daten beschäftigen und daher ebenfalls Situationen ausgesetzt sind, in denen sie aufgrund von unternehmensbezogenen Entscheidungen, die sie zu treffen haben, den Datenschutz dahingehend auslegen und dieser dadurch nicht immer die notwendige Berücksichtigung und Aufmerksamkeit findet.

Organisatorisch ist der Datenschutzbeauftragte direkt der Geschäftsleitung unterstellt und ausschließlich dieser rechenschaftspflichtig. Der Beauftragte kann sich jederzeit an die Leitung der verantwortlichen Stelle wenden und auf notwendige Maßnahmen und festgestellte Verstöße aufmerksam machen. Er ist weisungsfrei, § 4f Abs. 3 Satz 2 BDSG, in der Wahrnehmung seiner gesetzlichen Aufgaben. Die verantwortliche Stelle hat ihn bei der Erfüllung seiner Aufgaben zu unterstützen und mit der notwendigen materiellen und personellen Ausstattung zu versorgen.

Die Bestellung des Beauftragten endet mit dem Ablauf der vereinbarten Bestellfrist oder, wenn eine solche nicht vereinbart wird mit der Amtsniederlegung durch den bDSB selbst oder mit dem Widerruf aus wichtigem Grund durch die verantwortliche Stelle, § 4 Abs. 3 Satz 4 BDSG. Der Widerruf kann bei nicht-öffentlichen Stellen auch auf Verlangen der Aufsichtsbehörde erfolgen.

Schlussendlich hat jeder Betroffene das Recht, den Beauftragten anzurufen, das heißt, sich mit seinem Anliegen an ihn zu wenden, § 4f Abs. 5 Satz 2 BDSG. Das Gesetz räumt damit die Möglichkeit ein, dass sich die Betroffenen Klarheit über den Umgang mit ihren

Daten verschaffen und damit ihre Rechte im Datenschutz besser wahren können.
Der Beauftragte für den Datenschutz wirkt auf die Einhaltung des BDSG und anderer Vorschriften über den Datenschutz hin. Er überwacht die ordnungsgemäße Anwendung von Datenverarbeitungsprogrammen mit deren Hilfe personenbezogene Daten verarbeitet werden sollen. Er hat insbesondere auch die Personen die mit der Verarbeitung von personenbezogenen Daten beschäftigt sind, über die datenschutzrelevanten Vorschriften zu informieren.

Der betriebliche Datenschutzbeauftragte ist das Bindeglied zwischen den Interessen der verantwortlichen Stelle auf der einen Seite und den Rechten der Betroffenen auf der anderen Seite. Um einen verantwortungsbewussten Ausgleich im Rahmen der gesetzlichen Bestimmungen zwischen diesen beiden Positionen herzustellen muss der Beauftragte die nötigen Fachkenntnisse und die notwendige Zuverlässigkeit für diese Tätigkeit mitzubringen.

2.6 Die Europäische Datenschutz-Grundverordnung kommt – und die Unternehmen machen sich so ihre Gedanken

Im Berichtszeitraum wandte sich der Landesbeauftragte für den Datenschutz aus dem Saarland (LfD SL) an die Datenschutzbeauftragten des Bundes und der Länder. Grund hierfür war ein Schreiben eines extern bestellten Datenschutzbeauftragten (bDSB) an den LfD SL, der für ein deutschlandweit vertretenes Aktenvernichtungsunternehmen tätig sei. Der bDSB stellte das Unternehmen als renommierten und seriösen „Premium-Dienstleister“ im Bereich der Akten- und Datenträgervernichtung, der Archivierung und der Digitalisierung (wie Scan-Dienste) sowie als einen Garant für vorbildlichen Datenschutz und Datensicherheit vor. Das Unternehmen sieht sich als Mithelfer seiner Kunden und der Aufsichtsbehörden für den Datenschutz, um die Persönlichkeitsrechte der Betroffenen zuverlässig zu schützen. Der bDSB bat darum, die Verarbeitungsvorgänge Vernichtung, Archivierung und Digitalisierung von personenbezogenen Daten in die Liste gemäß Art. 35 Abs. 4 Datenschutz-Grundverordnung (DS-GVO), nach dem eine Datenschutzfolgeabschätzung durchzuführen ist, aufzunehmen. Danach ist in den Fällen, in denen die Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge haben könnte,

eine Rechtmäßigkeitsprüfung durchzuführen. Kernpunkt ist darin eine Auflistung der geplanten Abhilfemaßnahmen, durch die der Schutz der personenbezogenen Daten sichergestellt wird und damit die Risiken für die Betroffenen eingedämmt werden. Insbesondere wird die Erbringung eines Nachweises gefordert, dass die DS-GVO eingehalten wird. Der bDSB meint, dass die Verarbeitungsvorgänge der Vernichtung, Archivierung und Digitalisierung personenbezogene Daten beinhalten, die grundsätzlich ein hohes Risiko für die Rechte und Freiheiten der Betroffenen darstellen und in der Regel eine Datenschutz-Folgenabschätzung durchgeführt werden sollte. Mit der Aufnahme dieser Verarbeitungen in die o. g. Positivliste wäre dies für die Verantwortlichen vorgegeben.
Die Landesbeauftragten des Bundes und der Länder tauschten sich über die Einschätzung des bDSB aus. Da die Zentrale des Unternehmens, für das der bDSB tätig war, ihren Hauptsitz in Hamburg hat, wurde der hamburgische Datenschutzbeauftragte gebeten, stellvertretend für alle Datenschutzbeauftragten dem bDSB zu antworten. Dem bDSB wurde mitgeteilt, dass das angesprochene Thema, die Erarbeitung von Listen gemäß Art. 35 Abs. 4 und 5 zur Datenschutz-Folgenabschätzung, ausgesprochen wichtig sei und große praktische Bedeutung für die Unternehmen erlangen wird. Allerdings habe die Vorbereitung auf diese Problematik gerade erst begonnen. Deshalb könne zum jetzigen Zeitpunkt eine nähere Auseinandersetzung mit den Vorschlägen noch nicht erfolgen. Man könne jedoch davon ausgehen, dass insgesamt sehr deutliche Differenzierungen der aufzunehmenden Verarbeitungsvorgänge erforderlich würden. Die Anregungen des bDSB werden aber nicht verloren gehen und in die künftigen Überlegungen mit einfließen.

Eine Datenschutz-Folgenabschätzung (DSFA) hat gemäß Art. 35 Absatz 1 DS-GVO immer dann zu erfolgen, wenn eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und des Zwecks der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat. Weiterhin hat dann eine DSFA zu erfolgen, wenn eine systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen erfolgt, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese

in ähnlich erheblicher Weise beeinträchtigen. Auch bei der umfangreichen Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Artikel 9 Absatz 1 DSG-VO oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 DSG-VO oder systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche ist eine DSFA erforderlich. Die Aufsichtsbehörde erstellt eine Liste der Verarbeitungsvorgänge, für die diese Datenschutz-Folgenabschätzung durchzuführen ist (sog. Blacklist) und veröffentlicht diese dann. Die deutschen Aufsichtsbehörden arbeiten derzeit mit Hochdruck an einer gemeinsamen Liste. Der Veröffentlichungszeitpunkt ist derzeit jedoch noch unbekannt.

2.7 Einbruchdiebstahl in der Kita

Im Berichtszeitraum informierte eine Kindertageseinrichtung (im folgenden Kita) über einen Einbruch und den Diebstahl sämtlicher Technik mit personenbezogenen Daten sowie digitalen Fotos. Die Eltern wurden sofort informiert. Die Kita bat über deren Träger den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) um Begleitung im Prozess der Aufklärung. Im ersten Schritt wollte der TLfDI wissen, welche technischen und organisatorischen Maßnahmen die Einrichtung getroffen hat, um diese Daten künftig zu schützen. Nach § 9 Abs. 1 Bundesdatenschutzgesetz (BDSG) in Verbindung mit der Anlage zu § 9 Satz 1 haben nicht-öffentliche Stellen technische und organisatorische Maßnahmen zum Datenschutz und zur Datensicherheit zu treffen, die erforderlich sind, um den Festlegungen des Gesetzes zu genügen. Hier geht es insbesondere darum, je nach Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignete Maßnahmen zu treffen, Beispielsweise:
Zutrittskontrolle – Nach der Anlage zu § 9 BDSG sind unter der Zutrittskontrolle Maßnahmen zu verstehen, die verhindern, dass Unbefugte Zutritt (räumlich zu verstehen) zu Datenverarbeitungsanlagen erhalten, mit welchen personenbezogene Daten verarbeitet werden (z. B. Gebäudesicherung durch Zäune, Sicherung der Räume durch Sicherheitsschlösser, Chipkartenleser, Alarmanlagen, Codeschlösser usw.). Durch den Einbruchsdiebstahl hatten Unbefugte Zutritt zur Kita und damit zur betreffenden Technik erlangt. Damit waren die ergriffenen Maßnahmen im Hinblick auf die Zutrittskontrolle nicht wirksam gewesen.

Zugangskontrolle – Nach der Anlage zu § 9 BDSG sind unter der Zugangskontrolle Maßnahmen zu verstehen, die verhindern, dass Datenverarbeitungsanlagen von Unbefugten benutzt werden können, wobei allerdings das Wort „nutzen“ sich nicht auf die Legaldefinition des § 3 Abs. 5 BDSG beschränkt (z. B. Zugang zu Rechnern/Systemen, Authentifizierung, Benutzerkennung mit Passwort, Firewall, zertifikatsbasierte Zugangsberechtigung etc.). Durch den angezeigten Diebstahl könnten Unbefugte Zugang zu den gespeicherten personenbezogenen Daten erhalten.
Zugriffskontrolle – In Bezug auf die Zugriffskontrolle muss gewährleistet werden, dass die zur Benutzung von Datenverarbeitungsanlagen berechtigten Nutzer ausschließlich auf Inhalte zugreifen können, für welche sie berechtigt sind. Des Weiteren muss sichergestellt sein, dass personenbezogene Daten bei der Verarbeitung und Nutzung sowie nach dem Speichern nicht unbefugt kopiert, verändert oder gelöscht werden können (z. B. Berechtigungskonzept, Benutzerkennung mit Passwort, gesicherte Schnittstellen etc.).
Weitergabekontrolle – Im Rahmen der Weitergabekontrolle muss verhindert werden, dass personenbezogene Daten bei der elektronischen Übertragung oder beim Transport oder bei der Speicherung auf Datenträgern unbefugt gelesen, kopiert, verändert oder gelöscht werden können und das festgestellt werden kann, an welchen Stellen eine Übermittlung solcher Daten im DV-System vorgesehen ist.
Eine Sicherung bei der elektronischen Übertragung kann zum Beispiel durch Verschlüsselung, VPN, Firewall, beim Transport mittels verschlossene Behälter und bei einer Übermittlung durch Verfahrensverzeichnis oder Protokollierungsmaßnahmen erfolgen.
Die Kita bezog daraufhin Stellung und teilte in Bezug auf die Zugangs- und Zugriffskontrolle mit, dass das Gebäude durch einen Zaun sowie eine zentrale Schließanlage gesichert ist. Eine Alarmanlage hat sich allerdings im Haus nicht befunden. Die Täter haben die Zaunanlage überstiegen und sind durch ein verschlossenes Fenster eingebrochen. lm Zuge der Einbruchsmeldung erfolgte mit der zuständigen Polizeidienststelle eine Begehung des Objektes. Diese hatte die Installation einer Alarmanlage empfohlen. Im Übrigen teilten die Zuständigen der Kita mit, dass sich zum Beispiel der Laptop in einem verschlossenen und mit Pincode versehenen Büroschrank befunden hatte. Der Laptop war mit einem Passwort geschützt. Dieses Passwort sei allen Mitarbeitern bekannt, die im Zuge ihrer Tätigkeit mit Dokumentationen und Auswertungen zu tun ha-

ben und diesen dadurch nutzen. Die einzelnen erfassten Dateien personenbezogener Daten waren auf dem gemeinschaftlich genutzten Laptop nicht nochmals separat verschlüsselt. Auf dem Laptop selbst war nicht ersichtlich, wer welche Daten zu welchem Zeitpunkt erfasst, verändert oder auch gelöscht hat. Dies könnte nur über die Dienstpläne nachvollzogen werden.
Auf die o. a. Probleme bezogen rät der TLfDI, die Zugriffe über eine entsprechende Dienstanweisung zu dokumentieren. So kann eindeutig nachvollzogen werden, wer den Laptop und die Daten genutzt hat. Der Laptop, der ausschließlich von der Einrichtungsleitung genutzt wurde, war ebenfalls mit einem Passwort versehen. Letzteres war alleine der Einrichtungsleitung bekannt. Stark zu bemängeln hatte der TLfDI, dass die personenbezogenen Daten auf beiden Laptops selbst nicht noch einmal geschützt worden sind. Hier wäre es ratsam, die Daten durch eine Festplattenverschlüsselung extra zu sichern und somit noch besser vor unbefugtem Zugriff zu schützen.
Die Kindertageseinrichtung folgte dem Rat des TLfDI und installierte eine entsprechende Software auf den Laptops.
Auch wenn die Schäden des Diebstahls im vorliegenden Fall nicht mehr rückgängig zu machen sind, so ist die Kindertageseinrichtung nun ein ganzes Stück besser aufgestellt, um alle personenbezogenen Daten besser zu schützen.

Nach § 9 Abs. 1 BDSG sowie der Anlage zu § 9 Satz 1 haben nichtöffentliche Stellen technische und organisatorische Maßnahmen zum Datenschutz und zur Datensicherheit zu treffen, die erforderlich sind, um den Festlegungen des Gesetzes zu genügen. Hier geht es insbesondere darum, je nach Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignete Maßnahmen zu treffen.



Papierschnitzel Stichwort Kundenliste - ©Gina Sanders / Fotolia.com

3 Umgang mit Kundendaten

3.1 Immelborn – Ad Acta: Zwischenbericht des Untersuchungsausschusses 6/2 liegt jetzt vor: Handeln des TLfDI rechtmäßig – Amtshilfeverweigerung durch das ehemals CDU-geführte Innenministerium rechtswidrig!

Nun liegt er vor: Der 739 Seiten umfassende **Zwischenbericht des Untersuchungsausschusses** (UA) 6/2 zur Causa Immelborn (Drucksache 6/4641 v. 23. Oktober 2017), der das **rechtmäßige Amtshilfeersuchen** des TLfDI und dessen **rechtmäßiges Vorgehen** in der Aktenlager-Angelegenheit feststellt sowie die **skurrilen Vorgänge im Thüringer Innenministerium** offenlegt inklusive der **rechtswidrigen Ablehnung des Amtshilfeersuchens**.

Die Plenardebatte offenbarte zudem, dass die CDU im Untersuchungsausschuss ein externes Rechtsgutachten zu sämtlichen Rechtsfragen einholen wollte. Diese Idee scheiterte indes wiederum an der **Justiz**, die es für **offensichtlich abwegig** hielt, die **Aufgabe des Untersuchungsausschusses**, nämlich zu ermitteln und zu bewerten, auf einen externen Gutachter zu verlagern.

Der Untersuchungsausschuss gelangt überdies zu dem Ergebnis: Der von der CDU-Fraktion geäußerte Verdacht, der TLfDI habe die Klage auf Amtshilfe erhoben, um im Wahlkampf der TIM-Hausleitung schaden zu wollen, hat sich nicht erhärtet (Zwischenbericht, Rn. 1041).

Wer Interesse daran hat, nachzulesen, auf welchen krummen Wegen die CDU-Hausleitung des Innenministeriums gezielt, unter Verkennung vorliegender Rechtsgutachten und in rechtswidriger Weise darauf hingewirkt hat, dem TLfDI die Amtshilfe zu versagen, der sei auf die Rn. 1031 ff. des Zwischenberichts verwiesen.

Das Sondervotum der CDU-Fraktion finden Sie auf den Seiten 727 ff.

Der TLfDI dankt der Thüringer Polizei für ihre korrekte Bereitschaft zur rechtmäßigen Amtshilfe bei dem Mammut-Projekt Aktenlager-Immelborn.

3.2 Nerviges Meinungsforschungsinstitut

Den Thüringischen Landesbeauftragten für den Datenschutz und die Informationsfreiheit erreichte eine Beschwerde über aufdringliche Werbeanrufe durch ein Meinungsforschungsinstitut an eine private Telefonnummer, die nicht im Telefonbuch gespeichert war.
Daraufhin wandte der TLfDI sich mit einem Auskunftsverlangen nach § 38 Abs. 3 Bundesdatenschutzgesetz (BDSG) an das Meinungsforschungsinstitut mit der Bitte um Stellungnahme zu den datenschutzrechtlich relevanten Abläufen im Unternehmen (z. B. Generierung der Kontaktinformationen, Speicherung der Daten). Ebenso fragte der TLfDI nach der Melderegisteranmeldung gem. § 4d BDSG.
Das Unternehmen teilte dem TLfDI mit, dass es als Markt- und Sozialforschungsinstitut telefonische Umfragen in ganz Deutschland durchführe. Hierbei würden keine Verkaufsgespräche geführt. Es hätte jedoch vermehrt Probleme mit dem Missbrauch seiner Telefonnummer, was zu gehäuften Beschwerden führte. Darüber sei auch schon mit der Polizei gesprochen worden.
Zu den Verfahren äußerte sich das Unternehmen folgendermaßen: Die Telefonnummern würden dem Telefonbuch entnommen, wobei

die letzten beiden Ziffern nach dem Last-Digit-Verfahren per Zufall ersetzt werden. Sobald eine Kontaktperson die Teilnahme an einer Umfrage verweigere, würde die Rufnummer auf eine Sperrliste gesetzt, damit diese nicht mehr im Nummernpool für weitere Anrufe gespeichert sei. Außerdem gab das Unternehmen an, dass keine Melderegisterpflicht nach § 4d BDSG bestehe, da es einen betrieblichen Datenschutzbeauftragten bestellt hätte und keine personenbezogenen Daten verarbeiten würde. Da dies nicht alle aufgeworfenen Fragen klärte, entschied sich der TLfDI zu einer Vor-Ort-Kontrolle der automatisierten Datenverarbeitung.

Während der Kontrolle wurde das Markt- und Sozialforschungsinstitut darauf hingewiesen, dass gem. § 4g Abs. 4 BDSG Unternehmen, die mithilfe von automatisierten Verarbeitungen geschäftsmäßig personenbezogene Daten für Zwecke der Markt- und Meinungsforschung speichern, grundsätzlich verpflichtet sind, dies zu melden. Des Weiteren erhebt das Unternehmen durch die vorgenommene Generierung der Telefonnummern sehr wohl personenbezogene Daten. Gem. § 3 Abs. 1 BDSG sind personenbezogene Daten Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Bei Telefonnummern handelt es sich zumindest um Einzelangaben einer bestimmbaren Person, da trotz Weglassens des Namens und der Anschrift des Betroffenen dieser immer noch bestimmbar bleibt. Da die Telefonnummern in einem Block zu dem dazugehörigen Projekt gespeichert werden, verarbeitet das Unternehmen auch personenbezogene Daten. Die Speicherung der Nummern erfolgt jedoch getrennt von der Speicherung der Interviewantworten, womit das Unternehmen den Anforderungen bei der geschäftsmäßigen Datenerhebung und -speicherung für Zwecke der Markt- oder Meinungsforschung aus § 30 a BDSG nachkommt.

Das Markt- und Sozialforschungsinstitut wurde aufgefordert, seiner Meldepflicht nachzukommen, der es auch folgte.

Der Versuch des Auffindens der Telefonnummer des Beschwerdeführers in der Sperrliste blieb erfolglos. Auch stellte sich heraus, dass das Unternehmen zu dem Zeitpunkt des Anrufes keine Befragungen in diesem Ortsbereich durchgeführt hatte. Dies legte den Schluss nahe, dass es sich vorliegend doch um ein Problem mit dem Missbrauch der Telefonnummer des Unternehmens handelte und die störenden Anrufe nicht durch das Meinungsforschungsunternehmen selbst generiert worden sind.

Gemäß § 4d Abs. 1 BDSG sind Verfahren automatisierter Verarbeitungen vor ihrer Inbetriebnahme von nicht-öffentlichen Stellen der zuständigen Aufsichtsbehörde, sprich dem TLFDI, zu melden. Die Anforderungen für geschäftsmäßige Datenerhebung und -speicherung zum Zweck der Markt- oder Meinungsforschung sind in § 30a BDSG normiert.

3.3 Daten-Theater

Eine Bürgerin wandte sich an den Thüringer Landesbeauftragten für den Datenschutz (TLfDI). In der Vorweihnachtszeit hatte sie Theaterkarten gekauft, um diese zu verschenken. Beim Kauf der Karten wurde sie nach ihrem Namen, der Anschrift und ihrer Telefonnummer gefragt, was sie schon seltsam fand. Auf ihre Frage, warum sie diese Angaben machen müsse, bekam sie an der Kasse die Antwort, dass man ihre Daten benötige, falls es zu einer Absage der Veranstaltung kommen würde. Ein Vierteljahr später kamen die Beschenkten zur Veranstaltung. Am Einlass wurden sie nach ihrem Namen gefragt, der, wie man sich denken kann, natürlich nicht auf der internen Anwesenheitsliste des Veranstalters zu finden war. Sie nannten dann den Namen ihrer Bekannten. Diese fand den Abgleich ihres Namens auf der Anwesenheitsliste merkwürdig und fragte nunmehr schriftlich beim Veranstalter an, warum ihre personenbezogenen Daten erhoben bzw. abgeglichen worden waren. Sie forderte den Veranstalter auf, ihre Daten zu löschen. Dieser Forderung und der Beantwortung ihrer Fragen kam der Veranstalter bis zum Zeitpunkt des Anschreibens an den TLfDI nicht nach.
Der TLfDI ist nach § 42 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) in Verbindung mit § 38 Abs. 6 Bundesdatenschutzgesetz (BDSG) Aufsichtsbehörde über die Einhaltung des BDSG sowie anderer Vorschriften über den Datenschutz nach § 38 Abs. 1 BDSG bei nicht-öffentlichen Stellen. In dieser Funktion wandte er sich mit einem Auskunftsersuchen an den Veranstalter. Er forderte den Veranstaltungsservice auf, unter Einhaltung von Fristen mitzuteilen, wie er mit den personenbezogenen Daten seiner Kunden umgeht. Er fragte weiter nach, in welcher Art und Weise die Käuferdaten erhoben und für welchen Zweck diese personenbezogenen Daten verwendet werden und wie die Löschung dieser Daten erfolgt. Nach

dem Eingang der erforderlichen Informationen kam der TLfDI zu folgender datenschutzrechtlicher Einschätzung:
Grundsätzlich muss es den Käufern möglich sein, Eintrittskarten für Veranstaltungen ohne Angabe ihrer personenbezogenen Daten zu erwerben. Das Erheben, Verarbeiten und Nutzen von personenbezogenen Daten ist nach § 4 Abs. 1 BDSG grundsätzlich unzulässig, es sei denn, es gibt eine Erlaubnisnorm in- oder außerhalb des BDSG oder der Betroffene hat in den Vorgang eingewilligt (sogenanntes Verbot mit Erlaubnisvorbehalt). Eine gesetzliche Grundlage zur Erhebung der Käuferdaten liegt nicht vor. Die personenbezogenen Daten der Käufer sind weder für die Begründung, Durchführung oder Beendigung des rechtsgeschäftlichen Schuldverhältnissen noch zur Wahrung ihrer berechtigten Interessen erforderlich, § 28 Abs. 1 Nr. 1 und 2 BDSG. Selbst wenn berechtigte Interessen dargelegt werden, überwiegen in jedem Fall die schutzwürdigen Interessen der Käufer an dem Ausschluss der Datenerhebung. Jedenfalls bei Barzahlung und bei Nutzung der üblichen Bezahlverfahren (EC-Karte, Kreditkarte) beim Kauf von Eintrittskarten ist die Erhebung der Käuferdaten nicht erforderlich. Lediglich bei Zahlung per Rechnung ist die Angabe der Adressdaten notwendig.
Eine solche Erforderlichkeit lässt sich auch hier nicht mit organisatorischen Gründen begründen. Zum einen sind die Käufer der Veranstaltungstickets oftmals nicht die Besucher der Veranstaltungen. Auch ist es nicht unüblich, die Karten bei Krankheit oder Urlaub an Freunde/Bekannte weiter zu verschenken. Zum anderen würde zu organisatorischen Gründen auch die reine Anzahl der Gäste einer Gruppe ausreichen. Deshalb stellte sich die Frage, weshalb die beim Kartenverkauf erhobenen Daten beim Einlass der jeweiligen Veranstaltung mit den Daten der Eingelassenen abgeglichen werden. Die Besucher können sich auch ohne Angabe ihres Namens, zum Beispiel unter Angabe der Personenzahl, ihre Plätze oder Tische aussuchen. Diese Zuordnung kann über beim Kauf vergebene Nummern erfolgen. Gerade bei Beschenkten führt die Namensangabe nicht zum Ziel und kann auch nicht mit einer internen Liste abgeglichen werden. Gleiches gilt für die Besucher, welche die Eintrittskarten von Beschenkten bekommen haben. Da hier keine gesetzliche Grundlage für die Erhebung der personenbezogenen Daten der Käufer vorliegt und diese Erhebung auch nicht für einen Veranstaltungsbesuch erforderlich ist, kommt daher nur eine Datenerhebung aufgrund der Einwilligung der Käufer in Betracht.

Diese Einwilligung der Käufer ist wiederum nur wirksam, wenn sie auf deren freien Entscheidung beruht und schriftlich erfolgt, § 4a Abs. 1 BDSG. Wenn der Kartenverkauf schon an die Bedingung der Preisgabe von Käuferdaten geknüpft ist, ist diese Einwilligung unwirksam. Die Käufer sind vor der Angabe ihrer personenbezogenen Daten darauf hinzuweisen, dass deren Angabe freiwillig erfolgt und für welche Zwecke diese erhoben werden. Die personenbezogenen Käuferdaten sind spätestens dann zu löschen, wenn sie nicht mehr erforderlich sind. Im Regelfall ist dies nach dem Ende einer jeden Veranstaltung der Fall. Der Löschvorgang wird in § 3 Abs. 4 Nr. 5 BDSG näher beschrieben und umfasst das Unkenntlichmachen gespeicherter personenbezogener Daten.
Nach Angaben des Veranstaltungsservices ist es den Käufern zukünftig grundsätzlich möglich, Eintrittskarten für Veranstaltungen ohne Angabe ihrer personenbezogenen Daten zu erwerben. Soweit seitens des Veranstalters doch personenbezogene Daten der Käufer erhoben werden, erfolgt dieses zukünftig mit der Einwilligung der Käufer. Diese Einwilligung der Käufer basiert nunmehr auf deren freien Entscheidung und erfolgt schriftlich im Sinne des § 4a Abs. 1 BDSG. Die dem TLfDI dazu vorgelegte datenschutzrechtliche Mustereinwilligung wurde überprüft und entsprach nunmehr den datenschutzrechtlichen Bestimmungen.

Das Erheben, Verarbeiten und Nutzen von personenbezogenen Daten ist nach § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG) grundsätzlich unzulässig, es sei denn, es gibt eine Erlaubnisnorm innerhalb oder außerhalb des BDSG oder der Betroffene hat in den Vorgang eingewilligt (sog. Verbot mit Erlaubnisvorbehalt).

3.4 Der Anwalt als Datenschleuder?

Im Juni 2016 bat ein Veranstaltungsunternehmen den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) um datenschutzrechtliche Überprüfung, ob das Übermitteln von Kundendaten des Unternehmens und seiner anwaltlichen Prozessvertreter an Dritte, im vorliegenden Fall an das Gericht, im Rahmen eines Klageverfahrens gegen die Grundsätze des Datenschutzes verstoße. Nach Auffassung des Unternehmens würden die Betroffenen durch die Übermittlung dieser Daten in ihrem Recht auf informationelle Selbstbestimmung beeinträchtigt. Dies erwecke den

Eindruck, dass die betroffenen Unternehmenskunden ebenfalls am verfahrensgegenständlichen, auf Schadenersatz gerichteten Verhalten ihres Mandanten beteiligt gewesen seien. Darüber hinaus nutze das Veranstaltungsunternehmen diese personenbezogenen Daten zur rechtsmissbräuchlichen Verfolgung eigener Interessen.
Der TLfDI konnte nach Überprüfung des Sachverhalts keinen datenschutzrechtlichen Verstoß feststellen. Ein Eingriff in das Recht der informationellen Selbstbestimmung der betroffenen Kunden lag nach seiner Auffassung nicht vor.
Der TLfDI begründete seine Auffassung folgendermaßen: Die nichtöffentlichen Stellen, unter die auch die Anwaltskanzlei fällt, müssen die Übermittlung personenbezogener Daten grundsätzlich an § 28 Abs. 1 BDSG ausrichten. Danach ist das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke unter bestimmten, in Abs. 1 aufgeführten Voraussetzungen zulässig.
Im vorliegenden Fall ergibt sich die Erlaubnis für die Übermittlung der Daten aus § 28 Abs. 1 Nr. 2 BDSG. Danach ist das Erheben und Übermitteln personenbezogener Daten zulässig, „… soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt…“. Im Sinne von § 28 Abs. 1 Nr. 1 ist es für die Erfüllung der Geschäftszwecke des Anwalts – die effektive Vertretung seiner Mandantschaft – erforderlich, personenbezogene Daten an das Gericht zu übermitteln. Vorliegend werden die Kundendaten an das Gericht zum Zweck der Betreuung des Mandatsverhältnisses als Beweisangebot gegenüber dem Gericht übermittelt. Nach dem BDSG liegt ein berechtigtes Interesse schon immer dann vor, wenn es sich aus vernünftigen Überlegungen ergibt und die vorgesehene Datenverwendung und der damit verfolgte Zweck im Einklang mit der Rechtsordnung stehen. In diesem Rahmen kommen sowohl ideelle als auch wirtschaftliche Interessen in Betracht. Ein rechtliches Interesse wird hierbei nicht vorausgesetzt, fällt jedoch stärker ins Gewicht (vgl. Dammann in Simitis, Kommentar zum BDSG, § 16 Rn. 17, 26).
Gerade die Wahrnehmung der rechtlichen Interessen des Mandanten stellt für die Anwaltskanzlei ein berechtigtes, qualifiziertes Interesse im Sinne des BDSG dar. Die Verfolgung der Rechte des Mandanten hängt im vorliegenden Fall von der Kenntnis der personenbezogenen

Daten der Kunden ab. Ohne diese Kenntnis wären ein Antrag auf Zeugenvernehmung nach § 373 ff. Zivilprozessordnung (ZPO), ein bestimmter Klageantrag mit den anspruchsbegründenden Voraussetzungen im Sinne des § 253 ZPO und dadurch letztendlich überhaupt die Geltendmachung des Schadensersatzanspruchs nicht möglich. Weiterhin sind die Parteien im Zivilprozessrecht verpflichtet, den Sachverhalt darzulegen und mögliche Beweise beizubringen.
Sofern die Anwaltskanzlei personenbezogene Daten verwendet, die sich auf „Gegner“ bzw. Betroffene beziehen, ist auch eine Interessenabwägung vorzunehmen. Die besondere Rolle des Rechtsanwalts nach dem BDSG wird hierbei dahingehend berücksichtigt, dass sogar „besondere Arten“ personenbezogener Daten nach § 3 Abs. 9 BDSG verarbeitet werden dürfen, wenn dies zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung überwiegt, § 28 Abs. 6 Nr. 3 BDSG.
Es wäre nicht nachvollziehbar, wenn ein Rechtsanwalt keine personenbezogenen Daten zur Begründung seiner Klageschrift an das Gericht übermitteln dürfte. Daher stehen im vorliegenden Fall keine schutzwürdigen Interessen der Betroffenen der Datenübermittlung an das Gericht entgegen.

Im Rahmen eines Klageverfahrens dürfen der bzw. die (anwaltlichen) Prozessvertreter im Rahmen des gerichtlichen Verfahrens personenbezogene Daten an das Gericht übermitteln, da dies i. d. R zur Begründung der Klageschrift und im Verfahrensgang zur Aufklärung des Rechtsstreits erforderlich ist. Die Rechtsgrundlage ergibt sich aus § 28 Abs. 1 Nr. 2 BDSG und der Betreuung des Mandatsverhältnisses. Die Datenübermittlung erstreckt sich auch auf „besondere Arten“ personenbezogener Daten nach § 3 Abs. 9 BDSG. In diesen Fällen muss jedoch ganz besonders vorsichtig abgewogen werden und nicht erforderliche Informationen müssen sorgfältig geschwärzt werden.

3.5 Reparatur inklusive Datenverlust – wer richtig liest, erspart sich viel Ärger

Im Berichtszeitraum wurde dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) vom Landes-

beauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen die Beschwerde einer Bürgerin zuständigkeitshalber weitergeleitet. Die Bürgerin hatte ihr Notebook zur Instandsetzung im gekauften Markt abgegeben. Dabei hatte die Bürgerin ausdrücklich darauf hingewiesen, dass das Notebook lediglich hardwareseitig repariert werden solle, jedoch aber keine Software-Updates o. ä. durchgeführt werden sollen.
Nach Erhalt des Gerätes stellte die Bürgerin allerdings fest, dass Updates durchgeführt wurden und sämtliche persönlichen Daten nun gelöscht waren. Anhand der vorliegenden Fakten war eine Bearbeitung seitens des TLfDI noch nicht möglich. Er wandte sich deshalb an die Bürgerin und bat um Übersendung der allgemeinen Geschäftsbedingungen zu Reparaturaufträgen des Marktes.
Zeitgleich wandte sich der TLfDI an das Unternehmen, welches die Reparatur für den Elektronikmarkt durchführte und bat diesbezüglich um Stellungnahme. Das Unternehmen erklärte, dass für jede Reparatur eine Einsendungsbedingung für Garantiereparaturen durch den Kunden unterzeichnet wird und hierin klar definiert ist, dass die Daten durch die Kunden vor Abgabe zu sichern sind. Ebenso wird darauf hingewiesen, dass bei Bedarf nach den Reparaturen ein neues Update aufgespielt wird, falls die Qualitätskontrolle nicht erfolgreich war und der Kunde nach jeder Reparatur ein Recht auf ein einwandfrei funktionierendes Gerät hat. Im Falle eines solchen Updates könnten die Daten nicht wieder beschafft werden. Weiterhin wurde erklärt, dass es für die Reparaturaufträge einen Vertrag zur Datenverarbeitung im Auftrag gibt. Dabei handelt es sich um einen Vertrag, nach dem die weisungsgebundene Datenverarbeitung durch Externe – also nicht durch den Elektronikmarkt selbst, sondern durch einen Dritten – geregelt wird. Die Voraussetzungen für einen solchen Vertrag sind in § 11 Bundesdatenschutzgesetz (BDSG) geregelt. Bei einem wirksamen Abschluss können so personenbezogene Daten zwischen den Vertragspartnern – für den Geltungsbereich des Vertrages – ausgetauscht werden, ohne dass es eines gesetzlichen Erlaubnistatbestandes bedarf. § 11 BDSG beschreibt im Detail, welche Rechte, Pflichten und Maßnahmen im Einzelnen durch Vertrag zwischen Auftraggeber und Auftragnehmer zu treffen sind. Die Verantwortung für die ordnungsgemäße Datenverarbeitung verbleibt dabei beim Auftraggeber.

Nach Sichtung der eingegangenen Unterlagen zu den Geschäftsbedingungen für Garantiereparaturen durch die Bürgerin, konnte sich der TLfDI ein abschließendes Bild machen.
Wie schon von dem Unternehmen mitgeteilt, unterzeichnete die Bürgerin die Einsendungsbedingungen für Garantiereparaturen. In diesen steht – wie bereits oben beschrieben – dass die Kunden dafür Sorge zu tragen haben, das alle Daten vor Abgabe des Gerätes zur Reparatur gesichert werden sollten. Da es einen Vertrag über die Auftragsdatenverarbeitung gab, konnten bei der Verarbeitung der Daten durch das Unternehmen im Zuge dieser Reparaturen keine datenschutzrechtlichen Mängel festgestellt werden.
Hier gab es für den TLfDI nichts zu beanstanden.

Bei Reparaturaufträgen ist es ratsam, auch das Kleingedruckte zu lesen. Damit umgeht man böse Überraschungen. Nicht nur im Hinblick auf wichtige persönliche Unterlagen, sondern auch auf private Erinnerungsfotos wäre es schade, wenn diese wegen einer kleinen, aber durchaus weitreichenden Unachtsamkeit verloren gehen würden.

3.6 Datenerhebung zur Beitreibung rechtmäßiger offener Forderungen ist kein Datenschutzverstoß

Ein Bürger beschwerte sich beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) über ein Autohaus. Er trug vor, dass die Mitarbeiter einer Abschleppfirma des Autohauses seine persönlichen Daten missbraucht und Freiheitsberaubung begangen hätten. Der Beschwerdeführer legte dar, dass er im Parkhaus eines Krankenhauses auf dem Parkplatz des medizinischen Notdienstes geparkt habe und das Auto bei seiner Rückkehr mit einer Parkkralle versehen gewesen sei. Der Mitarbeiter der Abschleppfirma, der die Kralle angebracht hatte, forderte zur Auslösung des Fahrzeugs 50,00 € vom Beschwerdeführer und bezog sich dabei auf eine entsprechende Weisung seines Vorgesetzten, diese Zahlung einzufordern. Der Beschwerdeführer konnte bzw. wollte die 50,00 € jedoch nicht zahlen. Daraufhin habe der Mitarbeiter des Autohauses die Unterzeichnung eines Formulars zur Angabe von Name und Anschrift des Fahrzeughalters gefordert. Dieses Formular habe der Beschwerdeführer ausgefüllt und unterzeichnet. Dennoch habe der Mitarbeiter der Abschleppfirma auch noch den Personalausweis und

die Fahrzeugzulassung des Beschwerdeführers gefordert, um sie zu fotokopieren. Der Beschwerdeführer bezweifelte, dass die Fotodokumentation seiner amtlichen Dokumente rechtmäßig erfolgte und betonte, dass der Mitarbeiter der Abschleppfirma ihn insofern erpresst habe, da er sonst die Parkkralle nicht entfernt hätte. Er bat den TLfDI, diesen Sachverhalt datenschutzrechtlich zu prüfen und das Verhalten des Autohauses ggf. zu ahnden.
Der TLfDI hat das Autohaus um eine Stellungnahme zum vorgetragenen Sachverhalt hinsichtlich der Fotodokumentation des Personalausweises und der Zulassung im Rahmen des Abschleppvorgangs gebeten.
Das Autohaus teilte dem TLfDI mit, dass zum dargelegten Abschleppvorgang keine Bilder, Scanner-Dateien oder Ähnliches vorhanden seien. Seine Erklärung belegte das Autohaus glaubhaft mittels Screenshots der elektronischen Akte des Vorgangs.
Weiterhin teilte das Autohaus dem TLfDI mit, dass es vonseiten des Unternehmens den Abschleppfahrern grundsätzlich untersagt ist, Aufnahmen von Personalausweisen anzufertigen. Zum Zweck der Erfassung von personenbezogenen Daten lassen sich die Abschleppfahrer lediglich den Personalausweis und die Fahrzeugzulassung des Fahrzeugführers vorlegen. Die Fahrer schreiben diese Daten aus den vorgelegten Dokumenten ab und erfassen sie auf dem Auftrag und in der Kundendatei. Als Beleg übersandte das Autohaus dem TLfDI einen Abdruck aus der Kundendatei zum vorgetragenen Sachverhalt. Hieraus war ersichtlich, dass der Abschleppfahrer tatsächlich keine weiteren Daten erfasst hatte.
Aufgrund der Stellungnahme des Autohauses teilte der TLfDI dem Beschwerdeführer mit, dass die Mitarbeiter des Abschleppdienstes im Auftrag des Autohauses lediglich Namen, Anschrift und Geburtsdatum erfassten, um offene Forderungen beizutreiben. Dies begründet jedoch keinen Verstoß gegen datenschutzrechtliche Vorgaben. Gemäß § 28 Abs. 1 Satz 1 Bundesdatenschutzgesetz (BDSG) ist das Erheben personenbezogener Daten oder ihre Nutzung zulässig, wenn ihre Kenntnis zur Erfüllung eigener Geschäftszwecke dient – im vorliegenden Falle zur Beitreibung offener Forderungen des Abschleppdienstes. Gemäß § 28 Abs. 1 Satz 2 BDSG muss der Zweck, für den die Daten erhoben werden, genau angegeben sein, beispielsweise für die Begleichung offener Zahlungsforderungen. Im vorliegenden Falle bestanden keine Anhaltspunkte dafür, dass das Abschleppunternehmen des Autohauses gegen die datenschutzrechtli-

chen Regelungen verstoßen hatte. Somit hatten die Mitarbeiter des Abschleppdienstes nicht rechtswidrig in das Recht des Beschwerdeführers auf informationelle Selbstbestimmung eingegriffen. Parallel dazu informierte der TLfDI das Autohaus darüber, dass kein datenschutzrechtlicher Verstoß festgestellt werden konnte.

Gemäß § 28 Abs. 1 Satz 1 Bundesdatenschutzgesetz (BDSG) ist das Erheben personenbezogener Daten oder ihre Nutzung zulässig, wenn ihre Kenntnis zur Erfüllung eigener Geschäftszwecke dient – im vorliegenden Falle zur Beitreibung offener Forderungen des Abschleppdienstes. Gemäß § 28 Abs. 1 Satz 2 BDSG muss der Zweck, für den die Daten erhoben werden, genau angegeben sein.
Somit stellt die Abschrift von Name, Anschrift und Geburtsdatum aus amtlichen Dokumenten (Personalausweis, Kfz-Zulassung) zur Beitreibung rechtmäßiger offener Forderungen keinen Verstoß gegen datenschutzrechtliche Vorgaben und keinen Eingriff in die informationelle Selbstbestimmung des Dokumenteninhabers dar.

3.7 Bewerbung erfolglos – Daten löschen!

Dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) lag eine Beschwerde eines Bürgers vor. Dieser hatte sich per E-Mail mit einem Auskunftsersuchen nach § 34 Bundesdatenschutzgesetz (BDSG) unter Fristsetzung an ein Thüringer Autohaus gewandt. Hintergrund seines Auskunftsersuchens war seine vorangegangene Bewerbung bei diesem Unternehmen. Auf das geforderte Auskunftsersuchen sei seitens des Autohauses keine Reaktion erfolgt, so der Beschwerdeführer.
Der TLfDI wandte sich mit einem Anschreiben an das Autohaus. Er wies daraufhin, dass nach § 34 Abs. 1 Nr. 1 bis 3 BDSG die verantwortliche Stelle dem Betroffenen auf Verlangen Auskunft über die zu seiner Person gespeicherten Daten, die Herkunft der Daten, den Empfänger der Daten oder die Kategorie von Empfängern, an die Daten weitergegeben werden, und den Zweck der Speicherung zu erteilen hat. Darüber hinaus machte er den Geschäftsführer darauf aufmerksam, dass nach § 43 Abs. 1 Nr. 8a BDSG ordnungswidrig handelt, wer vorsätzlich oder fahrlässig eine Auskunft nicht oder nicht rechtzeitig erteilt. Eine solche Ordnungswidrigkeit kann nach § 43 Abs. 3 BDSG mit einer Geldbuße von bis zu 50.000 € geahndet werden.

Das Unternehmen wurde in diesem Zusammenhang unter Fristsetzung um Stellungnahme gebeten. Der externe Datenschutzbeauftragte des Unternehmens teilte dem TLfDI mit, dass er bereits vor geraumer Zeit dem Beschwerdeführer schriftlich mitgeteilt habe, dass keine personenbezogenen Daten über ihn im betreffenden Autohaus gespeichert sind. Er hatte auf das Auskunftsverlangen des Beschwerdeführers nochmals geantwortet und ausgeführt, dass ein entsprechender Datensatz – hier seine Bewerbung – nicht in den Datenverarbeitungssystemen des Autohauses, sowohl analog als auch digital, gefunden werden konnte. Zwar bestätigte eine Mitarbeiterin, dass von ihm in der Vergangenheit eine Bewerbung beim Autohaus per E-Mail eingegangen war. Diese wurde jedoch gleich nach Auswertung der eingegangenen Bewerbungen wieder gelöscht.
Nachdem das Autohaus den Schriftverkehr mit dem Betroffenen dem TLfDI lückenlos nachweisen konnte und auch die Bestellurkunde des betrieblichen Datenschutzbeauftragten in Kopie vorlegte, sah der TLfDI den Vorgang aus datenschutzrechtlicher Sicht als erledigt an. Ein datenschutzrechtlich rechtswidriges Verhalten war insoweit nicht festzustellen.

Jeder Bewerber hat das Recht, dass seine Bewerberdaten nach Ablauf des Einstellungsverfahrens unverzüglich gelöscht werden. Datenschutzrechtlich ergibt sich diese Verpflichtung aus § 35 Abs. 2 Nr. 3 BDSG, wonach Daten zu löschen sind, sobald ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist.

3.8 Hotelinsolvenz: Gehören die Kundendaten dem neuen Eigentümer?

Ein ehemaliger Hotelbetreiber aus Thüringen bat den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) um Auskunft darüber, ob er als früherer Gesellschafter Kundendaten seines Hotels zurückbekommen könnte und inwiefern eine entsprechende Verfahrensweise rechtmäßig sei. Das Hotel hatte als Unternehmergesellschaft bestanden und der Betreiber musste einen Insolvenzantrag stellen. Im Rahmen des Insolvenzantrags wurde das Hotel von einem anderen Pächter übernommen und weitergeführt. Dabei seien nach Auskunft des ehemaligen Betreibers auch sämtliche Unterlagen und PCs mit gespeicherten Daten in den

Besitz des neuen Pächters übergegangen. Nach Aussage des ehemaligen Betreibers befanden sich darunter auch sämtliche Kundendaten des Hotels (ca. 6.000) sowie Kreditkarten- und Buchhaltungsdaten.
Der TLfDI teilte dem ehemaligen Hotelbetreiber als Beschwerdeführer mit, dass eine mögliche Rückgabe der Daten aus seiner Sicht zivilrechtlich geklärt werden müsse. Der TLfDI wies daraufhin, dass er den vorgetragenen Sachverhalt vorbehaltlich genauerer Informationen jedoch datenschutzrechtlich bewerten wird. Nach § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG) ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit das BDSG oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Bei der „Übertragung" von Kundendaten des Hotels auf den nachfolgenden Pächter handelt es sich um eine Datenübermittlung, die Teil der Datenverarbeitung ist. Gemäß § 4 Abs. 1 BDSG benötigt der Übermittler bzw. der Insolvenzverwalter eine entsprechende Rechtsgrundlage oder die Einwilligung der jeweiligen Kunden, um die Daten von einem Unternehmen auf das Folgeunternehmen zu übertragen.
Als Rechtsgrundlage kam im vorliegenden Fall allenfalls § 28 Abs. 2 Nr. 1 in Verbindung mit § 28 Abs. 1 Nr. 2 BDSG in Betracht, da eine Weitergabe von Daten aufgrund einer Veräußerung des Unternehmens eine Zweckänderung darstellt. Gemäß § 28 Abs. 1 BDSG ist das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig. Die Daten wurden zur Durchführung eines Beherbergungs- und Bewirtungsvertrages erhoben und gespeichert. Die Rechtsnorm zur Datenübermittlung gemäß § 28 BDSG setzt jedoch ein berechtigtes Interesse eines Dritten (Folgepächter) voraus. Im Hinblick darauf war für den TLfDI nicht ersichtlich, inwiefern ein solches Interesse vorliegt. Darüber hinaus darf gemäß § 28 Abs. 2 Satz 1 Nr. 2 BDSG kein Grund zur Annahme bestehen, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Datenübermittlung hat. Dies konnte nach Auffassung des TLfDI im vorliegenden Falle nur zutreffen, wenn die Betroffenen jeweils vor der Datenübermittlung an den neuen Pächter informiert wurden und eine Möglichkeit zum Widerspruch eingeräumt war.
Mit der Insolvenzeröffnung geht die Verwaltungs- und Verfügungsbefugnis auf den Insolvenzverwalter über. Dies betrifft alle Vermögensgegenstände des insolventen Unternehmens. Sobald der Insolvenzverwalter den intakten Unternehmensteil an einen anderen Un-

ternehmer veräußert hat, wechselt auch die verantwortliche Stelle gemäß § 3 Abs. 7 BDSG. Der neue Unternehmer – vorliegend der neue Pächter – führt dann in aller Regel das Unternehmen fort oder integriert es in ein eigenes, bereits bestehendes Unternehmen Erst wenn dies stattgefunden hat, wechselt die verantwortliche Stelle. Aufgrund der Informationen des Beschwerdeführers ging der TLfDI davon aus, dass das Insolvenzverfahren noch nicht abgeschlossen war und der Beschwerdeführer insofern noch als Gesellschafter des insolventen Unternehmens fungierte und damit verantwortliche Stelle im Sinne des BDSG war. Der TLfDI sah nach den ihm vorliegenden Informationen die Datenübermittlung zum neuen Pächter als rechtswidrig an. Daher bat er den Beschwerdeführer gemäß § 38 Abs. 3 BDSG um genauere Informationen zum Sachverhalt, insbesondere darüber, unter welchem Namen das Hotel geführt wurde, wer der neue Pächter war, von welchem Insolvenzverwalter das Insolvenzverfahren geführt wurde und wie der Verfahrensstand ist. Der Beschwerdeführer teilte dem TLfDI die erbetenen Auskünfte schließlich mit.

Nach § 4 Abs. 1 BDSG benötigte der bestellte Insolvenzverwalter eine Erlaubnisnorm oder die Einwilligung der jeweiligen Kunden, um die Daten an den neuen Pächter weiterzugeben. Daher bat der TLfDI den Insolvenzverwalter nach § 38 Abs. 3 BDSG um Stellungnahme zum Sachverhalt und um Information, inwiefern im Rahmen der Insolvenzabwicklung Unterlagen und PCs mit personenbezogenen Daten von Hotelgästen (Kreditkarten- und Buchhaltungsdaten), Mitarbeitern und weiteren Betroffenen in den Besitz des neuen Pächters übergangen sind, auf welcher Rechtsgrundlage dies ggf. erfolgte und ob die betreffenden Kunden zuvor in die Datenübermittlung eingewilligt hatten. Weiterhin bat der TLfDI um Auskunft über die Art und Weise, wie das insolvente Unternehmen an den neuen Inhaber übergegangen ist, d. h., ob das alte Unternehmen fortgeführt oder ob ein neues Unternehmen gegründet wurde, das den (alten) Geschäftsbetrieb fortgeführt hat.

Parallel dazu bat der TLfDI den neuen Hoteleigner um eine Stellungnahme zu den aufgeworfenen Fragen und um folgende Auskünfte: In welcher Form wurde das Hotel an den neuen Pächter überschrieben, wurden die dabei übermittelten Kundendaten im Insolvenzverfahren gesondert verhandelt, auf welcher Rechtsgrundlage wurden diese Daten durch den neuen Pächter erhoben, wurden die jeweiligen Kunden über die Datenerhebung in Kenntnis gesetzt bzw.

haben sie hierin eingewilligt? Der neue Hoteleigner informiert den TLfDI darüber, dass er das Hotel käuflich erworben habe und verwies auf seinen beigefügten Kaufvertrag. Die Inhalte der PCs waren nach Auskunft des neuen Hoteleigners zuvor vollständig, bis auf das Hotelprogramm HS3, vom Insolvenzverwalter gelöscht worden. Alle Abrechnungen, Personalunterlagen und Dokumente, die die Angelegenheit vor der Übernahme durch den neuen Pächter betrafen, hatte der Insolvenzverwalter übernommen und archiviert.
Der Insolvenzverwalter bestätigte dem TLfDI die Übernahme des Hotels durch den neuen Pächter. Er dementierte jedoch, dass der neue Pächter über die Internetseite des Hotels gespeicherte personenbezogene Kundendaten von Hotelgästen der Schuldnerin erhalten hatte.
Aufgrund der vom Insolvenzverwalter gegebenen Informationen teilte der TLfDI dem Insolvenzverwalter die datenschutzrechtliche Erledigung der Angelegenheit mit. Weiterhin informierte der TLfDI den Beschwerdeführer und früheren Hoteleigner darüber, dass sowohl der Insolvenzverwalter als auch der neue Hoteleigner glaubhaft versichert hätten, dass keine Daten an den neuen Hotelbetreiber übermittelt worden seien. Insbesondere hätten keine gespeicherten Kreditkartendaten im insolventen Unternehmen vorgelegen.

Gemäß § 28 Abs. 1 BDSG ist das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder deren Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig. Im Falle der Datenübermittlung darf gemäß § 28 Abs. 2 Satz 1 Nr. 2 BDSG kein Grund zur Annahme bestehen, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Datenübermittlung hat. Sobald ein Insolvenzverwalter im Rahmen des Insolvenzverfahrens den intakten Unternehmensteil an einen anderen Unternehmer veräußert hat, ändert sich auch die verantwortliche Stelle gemäß § 3 Abs. 7 BDSG. Nach § 4 Abs. 1 BDSG benötigt der bestellte Insolvenzverwalter eine Erlaubnisnorm oder die Einwilligung der jeweiligen Kunden, um gespeicherte personenbezogene Daten an den neuen Unternehmenseigner weiterzugeben.

3.9 Das Probeabonnement einer Zeitung als Türöffner für Werbeattacken

Im Juli 2016 beschwerte sich ein Bürger beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) über eine Thüringer Zeitung und teilte mit, dass er von einer Mitarbeiterin der Zeitung mit der Nummer +49 800 … angerufen worden sei. Bei diesem Werbeanruf habe ihm die Mitarbeiterin ein kostenloses Probeabonnement der Zeitung angeboten. Die für den Werbeanruf verwendeten personenbezogenen Daten stammten nach Aussage der Mitarbeiterin aus einem bereits länger zurückliegenden Probeabonnement. Eine Einwilligung in die dauerhafte Speicherung oder in Werbeanrufe hatte der Beschwerdeführer der Zeitung jedoch nicht erteilt. Nach dem Werbeanruf hatte er die Zeitungsmitarbeiterin aufgefordert, seine personenbezogenen Daten zu löschen und wandte sich mit der Bitte um Überprüfung auf das datenschutzkonforme Verhalten der Zeitungsmitarbeiter an den TLfDI.
Der TLfDI wandte sich zunächst an die Mediengruppe, zu der auch die vorgenannte Zeitung gehörte, und bat um eine Stellungnahme zum Sachverhalt gemäß § 38 Abs. 3 Bundesdatenschutzgesetz (BDSG). In ihrer Stellungnahme legte die Mediengruppe dar, dass der Beschwerdeführer über den Leserservice für den Zeitraum vom 8. März bis 18. März 2013 ein Probeabonnement einer Regionalausgabe der Zeitung bestellt und über die Bestellmaske seine Adress- und Kontaktdaten angegeben hatte. Weiterhin legte die Mediengruppe dar, dass sich im Bestellvorgang ein farblich hervorgehobener Datenschutzhinweis mit Werbeerlaubnis befände, den der Kunde selbst durch Setzen des Häkchens aktiviere und damit bestätige, dass er die Bedingungen gelesen habe und damit einverstanden sei.
Somit war auch der Beschwerdeführer im Rahmen des Bestellvorgangs für das Probeabonnement auf die Datenschutzrechte einschließlich der Möglichkeit zum Widerspruch hingewiesen worden. Die übersandte Aufforderung zur Überprüfung der Daten mit dem wiederholten und inhaltlich unveränderten Hinweis auf die Werbeerlaubnis hatte der Beschwerdeführer durch Anklicken des Buttons „JETZT BESTELLEN“ bestätigt.
Anschließend erhielt der Beschwerdeführer eine Bestellbestätigung, die sowohl seine angegebenen Kontaktdaten enthielt als auch einen erneuten Hinweis auf die Werbeerlaubnis (sog. Double-Opt-In-Verfahren). Nach Darlegung der Mediengruppe hatte der Beschwer-

deführer somit wirksam seine Einwilligung in die Nutzung seiner Daten erteilt und er hatte noch die Möglichkeit, die Bestellbestätigung auszudrucken. Der Leserservice übermittelte daraufhin per csv-Datei seine Bestellbestätigung an die Mediengruppe. Im Zeitraum 2013 bis 2016 folgten daraufhin unterschiedliche Briefwerbungen an die angegebene postalische Adresse des Beschwerdeführers.
Aufgrund der Stellungnahme der Mediengruppe prüfte und bewertete der TLfDI den Sachverhalt datenschutzrechtlich und teilte das Ergebnis auch der Mediengruppe mit. Da Double-Opt-In-Verfahren regelmäßig von verschiedenen Firmen verwendet werden und Kunden bei entsprechenden Newsletter-Anmeldungen zum Teil auch Rabatte zugesichert bekommen, bezog der TLfDI in seine Prüfung auch ein grundsätzliches Urteil des Landgerichts München ein.
Nach Auffassung des TLfDI behalten Opt-Ins nicht ewig ihre Gültigkeit. Generell gelten Einwilligungen für den jeweils beschriebenen Umfang. Solange sich der Empfänger nach dem Erhalt eines Newsletters nicht wieder austrägt, gilt seine Einwilligung für jede weitere Ausgabe des Newsletters. Erhält ein Empfänger eine Zeit lang keine Newsletter (mehr), ist davon auszugehen, dass die Einwilligung nicht mehr besteht. Wann dieser Zeitpunkt ist, hängt vom Einzelfall ab. Dazu hat das Landgericht (LG) München mit Urteil vom 8. April 2010 (Az. 17 HK O 138/10) festgestellt, dass die Einwilligung ihre Gültigkeit auch dann verlieren kann, wenn von ihr über einen längeren Zeitraum kein Gebrauch gemacht wird. Dies gelte unabhängig davon, ob die Einwilligung tatsächlich wirksam erteilt wurde. Begründet wird dies damit, dass der Adressat der E-Mail- Werbung nach einer bestimmten Zeit nicht mehr damit rechnen muss, dass er noch weitere Werbung erhalte. Damit würde dann der Zustand vor Erteilung einer Einwilligung eintreten. Somit würde der Versand einer werblichen E-Mail dann eine unzumutbare Belästigung nach § 7 Gesetz gegen den unlauteren Wettbewerb darstellen.
Im vorliegenden Urteil hatte das Gericht keine konkrete Gültigkeitsdauer der Einwilligung benannt; es ging jedoch davon aus, dass eine vor 17 Monaten erteilte und bisher nicht genutzte Einwilligung zur E-Mail-Werbung „ihre Aktualität verliert“ und deshalb keine rechtliche Grundlage mehr ist.
In Anlehnung an das Urteil des LG München kam auch der TLfDI zu der Auffassung, dass die im März 2013 erteilte Einwilligung des Beschwerdeführers ab August 2014 keine rechtliche Grundlage mehr darstellte, weder für Briefwerbung noch für telefonische Werbekon-

takte. Der TLfDI forderte die Mediengruppe auf, ihm mitzuteilen, dass die personenbezogenen Daten des Beschwerdeführers mittlerweile gelöscht wurden bzw. ob dessen Werbewiderspruch berücksichtigt wurde. Im November 2016 bestätigte die Mediengruppe gegenüber dem TLfDI schriftlich, dass der Werbewiderspruch berücksichtigt wurde. Seine personenbezogenen Daten wurden bis zum Ablauf der kaufmännischen Aufbewahrungspflichten gem. § 35 Abs. 3 Nr. 1 BDSG gesperrt. Nach Ablauf der Sperrfrist werden die Daten des Beschwerdeführers gelöscht. Gegen dieses Vorgehen hatte der TLfDI aus datenschutzrechtlicher Sicht keine Bedenken.

Sofern Kunden bei der Bestellung von Probeabonnements oder Probeprodukten per Opt-In-Verfahren die Einwilligung zu einer Werbeerlaubnis erteilen, ist diese Einwilligung nicht dauerhaft gültig. Erhält ein Empfänger eine Zeit lang keine Werbung (mehr), ist davon auszugehen, dass die Einwilligung nicht mehr besteht. In Anlehnung daran geht das Landgericht München davon aus, dass eine 17 Monate zurückliegende und bisher nicht genutzte Einwilligung zur E-Mail-Werbung nicht mehr aktuell und somit keine rechtliche Grundlage für entsprechende Werbung ist. Unabhängig davon ist die Frage, wann eine erteilte Einwilligung in Werbung ihre Gültigkeit verliert, im Einzelfall zu klären.

3.10 Baumarkt verlangt Adressangabe beim Umtausch

Ein Bürger hatte in einem Baumarkt eine 5-Kilo-Propangas-Flasche umgetauscht. Hierzu verlangte der Baumarkt von ihm, seinen Namen und seine Adresse in einem Formular anzugeben. Er war daraufhin verwundert und suchte beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) eine plausible datenschutzrechtliche Erklärung, ob diese Datenerhebung überhaupt zulässig war.
Der TLfDI teilte dem Betroffenen daraufhin Folgendes mit: Gemäß § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG) ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Als Rechtsgrundlage für die Erhebung und Speicherung von Kundendaten bei Umtausch oder Reklamation kommt hier § 28 Abs. 1 Nr. 1 BDSG in Betracht. Dort ist geregelt, dass das Erheben, Speichern, Verändern

oder Übermitteln personenbezogener Daten und ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig ist, wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist. Bei dem Kauf einer 5-Kilo-Propangas-Flasche und dem darauffolgenden Umtausch handelt es sich um einen Kaufvertrag zwischen dem Bürger als Käufer und dem Baumarkt als Verkäufer im Sinne des § 433 Abs. 1 Bürgerliches Gesetzbuch (BGB). Bei einem Umtausch oder einer Reklamation entsteht zwischen den jeweiligen Kunden und dem Einzelhandelsunternehmen ein sog. Rückabwicklungsschuldverhältnis. Für das Rückabwicklungsschuldverhältnis könnte es daher erforderlich sein, die Kundendaten zu erheben bzw. zu speichern. Diese Erforderlichkeit müsste der Baumarkt begründen können. Die Erforderlichkeit für die Erhebung der Kundendaten könnte sich bei einem Umtausch von Waren zum einen daraus ergeben, dass sich eventuell erst nachträglich feststellen lässt, ob die umgetauschte Ware beschädigt ist und dadurch ggf. Regressansprüche aus dem Rückabwicklungsverhältnis entstanden sind. Zum anderen kann dies nötig sein, um in diesem Zusammenhang auftretenden Manipulationen (Missbrauch, Unterschlagung von Geld) durch das Personal vorzubeugen. Oft werden heutzutage in Einzelhandelsunternehmen Waren auch ohne gültigen Kassenbon ohne jegliche weitere Prüfung oder Bewertung eines Anspruchs zurückgenommen und der Kaufpreis wird in bar zurückerstattet. Vor allem handelt es sich dabei um einen besonderen Service bzw. um Kulanz des entsprechenden Einzelhandelsunternehmens. Dafür verlangen die Unternehmen auch eine Bestätigung der Kunden, dass sie für die zurückgegebene Ware den Kaufpreis erstattet bekommen haben. So könnte auch der schon angesprochene Missbrauch durch Mitarbeiter verhindert oder möglicherweise eine begangene Unterschlagung nachgewiesen werden. Liegt eine solche Erforderlichkeit jedoch nicht vor, ist davon auszugehen, dass die Datenerhebung und mithin auch die Speicherung dieser Daten rechtswidrig wäre.
Da der Betroffene sich nicht damit einverstanden erklärte, dass sich der TLfDI an den Baumarkt unter Nennung seines Namens wendet, war es nicht möglich den Einzelfall vollumfänglich aufzuklären. Daher wurde der Fall allgemein betrachtet und dem Betroffenen wurden die Zusammenhänge erklärt.

Nach § 4 Abs. 1 BDSG ist grundsätzlich jeder Umgang mit personenbezogenen Daten nur dann möglich, wenn eine gesetzliche Vorschrift dies erlaubt oder eine Einwilligung des Betroffenen vorliegt. Im dargestellten Fall war einschlägige Rechtsvorschrift § 28 BDSG – Datenerhebung und -speicherung für eigene Geschäftszwecke. Hierfür muss eine der Voraussetzungen des § 28 Abs. 1 Satz 1 Nr. 1 bis 3 BDSG zutreffend sein, damit die Datenerhebung oder -speicherung von personenbezogenen Daten für eigene Geschäftszwecke zulässig ist.

3.11 Versteckte Einwilligungserklärung

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) wurde im Berichtszeitraum durch eine anonyme Beschwerde darauf aufmerksam gemacht, dass in einem Hotel eine Datenschutzerklärung in der Gästemappe vorhanden war, welche nicht den datenschutzrechtlichen Bestimmungen entspreche. Durch Einschreiten des TLfDI konnten die Mängel hinsichtlich der Datenschutzklärung aufgeklärt und abgestellt werden. Zudem verwendete das Hotel einen Meldeschein für Gäste, welcher ebenfalls nicht den Bestimmungen des Datenschutzes entsprach.
Nach § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG) sind das Erheben, Verarbeiten und Nutzen von personenbezogenen Daten nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Rechtsgrundlage für die Erhebung der personenbezogenen Daten der Hotelgäste zur Registrierung ist § 29 Bundesmeldegesetz (BMG). Nach § 29 Abs. 2 BMG haben beherbergte Personen am Tag der Ankunft einen besonderen Meldeschein handschriftlich zu unterschreiben, der die in § 30 Abs. 2 BMG aufgeführten Daten enthält. Hierzu gehören Datum der Ankunft und der voraussichtlichen Abreise, Familienname, Vorname, Geburtsdatum, Staatsangehörigkeiten, Anschrift, Zahl der Mitreisenden und ihre Staatsangehörigkeit, Seriennummer des anerkannten und gültigen Passes. Darüber hinaus hatte das Hotel weitere umfangreiche Daten auch betreffend der Familienangehörigen bzw. Mitreisenden erhoben. Dies war jedoch laut Bundesmeldegesetz und auch auf Grundlage keiner anderen Erlaubnisnorm erforderlich, die Daten konnten nur auf freiwilliger Basis erhoben werden. Daraufhin übersandte die verantwortliche Stelle einen überarbeiteten Meldeschein, welcher eine Datenschutzerklärung mit einer

Einwilligungserklärung zur Erhebung von personenbezogenen Daten enthielt, welche nicht gesondert hervorgehoben, sondern in die Datenschutzerklärung als Fließtext eingebunden wurde. Auch in der Überschrift fand sich kein Hinweis auf eine zu erteilende datenschutzrechtliche Einwilligung des Betroffenen. Zudem musste laut dem Formular die Einwilligung zusammen mit der zwingenden Unterschrift zum Meldeschein erfolgen. Ferner wurde eine sog. Opt-Out-Formulierung gewählt, wonach jederzeit der erteilten Einwilligung widersprochen werden kann. Nach § 4a Abs. 1 BDSG ist eine Einwilligung zusammen mit anderen abzugebenden schriftlichen Erklärungen besonders hervorzuheben. Datenschutzfreundlicher ist es auch, wenn die Einwilligung in einem separaten Kästchen mit separater Unterschrift auf einem Formular als sog. Opt In dargestellt würde. Eine versehentlich erteilte Einwilligung der Kunden und Gäste wäre faktisch ausgeschlossen. Der TLfDI stellt auf seiner Website die „Orientierungshilfe zur datenschutzrechtlichen Einwilligungserklärung in Formularen“ des Düsseldorfer Kreises als Hilfe bei der Formulierung Unternehmen zur Verfügung (https://www.tlfdi.de/mam/tlfdi/gesetze/orientierungshilfen/orientierungshilfe_zur_datenschutzrechtlichen_einwilligung_.pdf)



Der TLfDI wies das Hotel auf die vorzunehmenden Änderungen hin, um eine datenschutzrechtlich wirksame Einwilligung der Betroffenen herbeizuführen. Die verantwortliche Stelle kam der Aufforderung des TLfDI im vollen Umfang nach.

Sofern die personenbezogenen Daten nicht auf Grundlage einer Rechtsvorschrift nach dem BDSG oder anderer Vorschriften über den Datenschutz erhoben und verarbeitet werden können, ist eine Einwilligung der Betroffenen erforderlich, § 4 Abs. 1 BDSG. Die von Unternehmen zumeist verwendeten datenschutzrechtlichen Einwilligungserklärungen in die Datenerhebung und -verarbeitung von personenbezogenen Daten entspricht zumeist nicht den Vorgaben des § 4a Abs. 1 BDSG. Hierfür hat der Düsseldorfer Kreis eine „Orientierungshilfe zur datenschutzrechtlichen Einwilligungserklärung in entsprechenden Formularen“ zur Verfügung gestellt

(https://www.tlfdi.de/mam/tlfdi/gesetze/orientierungshilfen/orientierungshilfe_zur_datenschutzrechtlichen_einwilligung_.pdf).

3.12 Pkw-Stellplatz gegen Ausweiskopie – was ist in der Mieterselbstauskunft zulässig?

Im Januar 2016 beschwerte sich ein Bürger beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) darüber, dass ein Unternehmen für Gebäudeservice im Rahmen einer Mieterselbstauskunft für einen Stellplatz verlangte, eine Kopie vom Personalausweis oder Reisepass abzugeben. Der Beschwerdeführer hatte diese Kopie mit Verweis auf den Datenschutz verweigert. Daraufhin leitete die Firma seine Mietanfrage wegen fehlender Unterlagen nicht weiter, sodass kein Mietvertrag zustande kam. Weiterhin vermutete der Beschwerdeführer, dass das Serviceunternehmen die hohen Anforderungen zur Speicherung und Aufbewahrung von sensiblen personenbezogenen Daten gar nicht erfüllen kann.
Daher wollte der Beschwerdeführer vom TLfDI wissen, wer die korrekte Aufbewahrung von personenbezogenen Daten kontrolliert, ob Firmen eine Kopie des Personalausweises von Kunden verlangen dürfen und ob nicht-öffentliche Stellen personenbezogene Daten von Kunden überhaupt erheben dürfen? Falls Firmen dies nicht dürften, wollte der Beschwerdeführer wissen, wer den Firmen wirksam untersagt, personenbezogene Daten von Kunden zu erheben.
Der TLfDI bat das Unternehmen für Gebäudeservice um eine Stellungnahme zum vorgetragenen Sachverhalt. Dabei wies der TLfDI das Unternehmen darauf hin, dass nach § 14 Nr. 2 Personalausweisgesetz (PAuswG) personenbezogene Daten aus dem Ausweis oder mithilfe des Ausweises durch öffentliche und nicht-öffentliche Stellen ausschließlich nach Maßgabe der §§ 18 bis 20 PAuswG erhoben oder verwendet werden dürfen. In der Gesetzesbegründung zu § 14 PAuswG heißt es: „§ 14 stellt klar, dass die Erhebung und Verwendung personenbezogener Daten aus oder mithilfe des Ausweises künftig nur über die vorgesehenen Wege erfolgen darf. (…)Weitere Verfahren z. B. über die opto-elektronische Erfassung („scannen“) von Ausweisdaten oder den maschinenlesbaren Bereich sollen ausdrücklich ausgeschlossen werden.“ (Drucksache des Bundesrats Nr. 550/08, S. 69 f.)

Daraus ergibt sich, dass zu Identifikationszwecken grundsätzlich nur die Stammdaten überprüft werden dürfen wie Name, Anschrift und ggf. Geburtsdatum. Daten, die nicht zur Identifizierung benötigt werden, dürfen nicht erhoben werden. Dies gilt insbesondere für die auf dem Ausweis aufgedruckte Zugangs- und Seriennummer. Kopien dürfen also nicht angefertigt werden. Lediglich die Vorlage und das anschließende Abschreiben des Namens und der Anschrift sind gesetzlich zulässig. Anschließend ist der Personalausweis dem Besitzer zurückzugeben.
Das Unternehmen teilte dem TLfDI daraufhin mit, dass aufgrund der dargelegten gesetzlichen Vorschriften in Zukunft keinerlei Kopien von Ausweisdokumenten mehr abverlangt oder weitere Angaben außerhalb der Stammdaten erhoben werden. Außerdem bestätigte das Unternehmen, seit November 2016 keine Mieterselbstauskunft von möglichen Mietinteressenten mehr abzuverlangen. Nach einer Besichtigung des Mietobjekts vermittelt die Firma nur noch den Kontakt zwischen dem Vermieter und dem Mietinteressenten. Abschließend teilte die Firma dem TLfDI im Januar 2017 mit, dass die bisher gefertigten Kopien von Ausweisdokumenten datenschutzgerecht vernichtet wurden.
Der TLfDI informierte den Beschwerdeführer über die vorgetragenen Änderungen des Serviceunternehmens und über die künftige datenschutzkonforme Mietvermittlung.

Zum damaligen Zeitpunkt war das Kopieren von Ausweisen in der Regel unzulässig. Ausnahmen galten nur für Unternehmen, die eine besondere, ausdrücklich gesetzlich geregelte „Kopiererlaubnis“ haben (beispielsweise Banken aus dem Geldwäschegesetz). Im Rahmen einer Selbstauskunft zur Anmietung von Wohnungen oder Pkw-Stellplätzen war das vermittelnde Unternehmen nicht berechtigt, Kopien von Ausweisdokumenten anzufertigen oder einzufordern.
Inzwischen hat der Gesetzgeber das Personalausweisgesetz geändert. Der Ausweis kann nunmehr seit 18. Juli 2017 nach Maßgabe des § 20 Abs. 2 PAuswG abgelichtet werden. Allerdings stellt die Norm keinen generellen Erlaubnistatbestand i. S. d. § 4 Abs. 1 BDSG dar. Die Vorschriften des Datenschutzrechts über die Erhebung und Verwendung personenbezogener Daten bleiben gemäß § 20 Abs. 2 PAuswG unberührt.
Das bedeutet, er darf nur vom Ausweisinhaber oder von anderen Personen mit dessen/deren Zustimmung abgelichtet werden und die

Ablichtung muss eindeutig als Kopie gekennzeichnet werden. Ebenfalls dürfen nur die Daten erhoben werden, mit denen der Ausweisinhaber einverstanden ist. Auch dürfen derart erstellte Kopien nicht an Dritte weitergegeben werden.
Aufgrund der Tatsache, dass die gesamte Datenverarbeitung einwilligungsbasiert ist, müssen die Kopien und die damit erhobenen Daten allerdings vernichtet werden, sobald die Einwilligung vom Ausweisinhaber widerrufen wird.

3.13 Bestattungskosten: Datenschutz kein Kostenschutz

Im Berichtszeitraum beschwerte sich ein Bürger beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) über ein Bestattungsunternehmen. Das Unternehmen hatte dem Beschwerdeführer eine Rechnung zugestellt. Daraufhin bat der Beschwerdeführer das Bestattungsunternehmen um Mitteilung, woher seine Anschrift und seine Familienbeziehung zum Verstorbenen bekannt seien. Jedoch habe das Unternehmen seine Anfrage nicht beantwortet. Daher bat der Beschwerdeführer für sein Auskunftsersuchen den TLfDI um entsprechende Unterstützung.
Gemäß § 34 Abs. 1 Bundesdatenschutzgesetz (BDSG) ist das Bestattungsunternehmen verpflichtet, die vom Beschwerdeführer erbetenen Auskünfte zu erteilen. Dementsprechend bat der TLfDI das Bestattungsunternehmen um eine Stellungnahme zur nicht erteilten Auskunft.
Zwischenzeitlich hatte das Unternehmen den Beschwerdeführer jedoch schriftlich über die Herkunft seiner genutzten Daten informiert. Das Bestattungsunternehmen hatte die Daten von der Schwester des Beschwerdeführers erhalten und sicherte zu, die Daten nur zum Zwecke der Rechnungslegung verwendet und an keine andere Stelle weitergeleitet zu haben. Weiterhin bestätigte das Unternehmen schriftlich, dass die Daten nicht gespeichert würden.
Die schriftlich erteilte Auskunft des Bestattungsunternehmens genügte vollständig den Anforderungen des § 34 Abs. 1 BDSG und war somit vom TLfDI datenschutzrechtlich nicht zu beanstanden. Dies teilte der TLfDI abschließend auch dem Beschwerdeführer mit.
„Nicht-öffentliche Stellen sind natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts, soweit sie nicht unter die Absätze 1 bis 3 fallen.“ (§ 2 Abs. 4 S. 1 BDSG).

Wenn solche Stellen für sich personenbezogene Daten erheben, verarbeiten oder nutzen, sind sie „verantwortliche Stellen“ im Sinne des § 3 Abs. 7 BDSG.
Diese verantwortlichen Stellen haben dem Betroffenen auf Verlangen Auskunft zu erteilen über

- die zu seiner Person gespeicherten Daten, auch soweit sie sich auf die Herkunft dieser Daten beziehen,
- den Empfänger oder die Kategorien von Empfängern, an die die Daten weitergegeben werden, und
- den Zweck der Speicherung. (§ 34 Abs. 1 BDSG)

Die Pflicht zur Auskunftserteilung besteht insofern für jedes Unternehmen, wenn es eine entsprechende Anfrage erhält.

3.14 Unzulässige Kopie des Personalausweises – keine Bombenidee

Im Berichtszeitraum beschwerte sich ein Bürger über ein Unternehmen, welches Zubehör für Schwimmbäder und Saunas vertrieb. Das Unternehmen fertigte Ausweiskopien aller Kunden, die einen bestimmten Artikel kauften. Mündlich wurde dem Kunden mitgeteilt, dass dies geschehe, da der Artikel Bestandteile enthält, welche zum Bombenbauen geeignet seien. Der Bitte des Kunden, die Kopie des Personalausweises zurückzubekommen und eine schriftliche Berechtigung zur Fertigung einer solchen Kopie vorzuzeigen, kam das Unternehmen nicht nach. Des Weiteren teilte der Bürger mit, dass die Rechnungen in einem Ordner auf dem Verkaufstresen – scheinbar für jedermann zugänglich – aufbewahrt werden würden.
Der TLfDI hakte deshalb nach und bat das Unternehmen um Stellungnahme. Insbesondere wollte der TLfDI wissen, aufgrund welcher Rechtsvorschrift und in welchen Fällen die Anfertigung von Kopien des Personalausweises der Kunden erfolgt, zu welchem Zweck die Kopien erhoben werden, auf welchem Medium diese Dokumente gespeichert werden, welcher Personenkreis Zugriff auf diese Dokumente hat, wo und wie lange die Personalausweiskopien aufbewahrt werden sowie die Erläuterung zum Löschvorgang dieser Dokumente. Das Unternehmen bestätigte die Fertigung der Ausweiskopien. Diese Pflicht – so das Unternehmen dem Käufer gegenüber – ergebe sich aus den Vorgaben der Lieferanten. Denn diese fordern für dieses Produkt ein entsprechendes Chemieabgabebuch mit ge-

nauer Dokumentation. Das bedeutet, von jedem Kunden, der flüssige Produkte zur Pooldesinfektion kaufte, welche auf Aktivsauerstoffbasis mit einer Konzentration von mehr als 12 Prozent Wasserstoffperoxid versehen waren, wurde eine Kopie des Ausweises gefertigt. Grund hierfür war ein verhinderter Anschlag mit Bomben. Das Unternehmen berichtete, dass aus dem Produkt zur Pooldesinfektion das Wasserstoffperoxid gewonnen worden war, um daraus Bomben zu bauen.
Da es dem Unternehmen im Tagesgeschäft zeitlich nicht möglich war, die Daten handschriftlich zu erfassen, wurden diese Kopien gefertigt und der jeweiligen Rechnungskopie beigefügt. Somit hatte das Unternehmen einen Nachweis. Gerade auch im Hinblick auf mögliche Anschläge könnte somit – so das Unternehmen – ein gewisser Personenkreis anhand dieser Daten ermittelt werden. Kurz darauf teilte das Unternehmen mit, dass im Zuge einer Schulung festgestellt wurde, dass die Ausweiskopien nicht rechtskonform seien.
Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist nur zulässig, soweit das Bundesdatenschutzgesetz (BDSG) oder eine andere Rechtsnorm dies erlaubt oder der Betroffene eingewilligt hat, § 4 Abs. 1 BDSG.
Nach § 28 Abs. 1 Nr. 2 BDSG ist das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt. Eine solche Erforderlichkeit zum Kopieren des Ausweises ist bei den üblichen Bargeschäften in der Regel nicht gegeben.
Die Feststellung der Identität wird nach § 3 Abs. 1 Satz 4 der Chemikalien-Verbotsverordnung (ChemVerbotsV) in diesem Fall angeordnet. Danach hatte der Verkäufer ein Abgabebuch zu führen, welches den Namen und die Anschrift des Erwerbers beinhalten musste. Allerdings war das Kopieren des Personalausweises dennoch unzulässig. Das Abgabebuch war vom Verkäufer mindestens fünf Jahre nach der letzten Eintragung aufzubewahren. Nach § 14 Nr. 2 Personalausweisgesetz (PAuswG) durfte die Erhebung und Verwendung personenbezogener Daten aus dem Ausweis oder mithilfe des Ausweises ausschließlich nach Maßgabe der §§ 18 bis 20 PAuswG er-

folgen. Nach § 20 Abs. 2 PAuswG durfte dieser jenseits des elektronischen Identitätsnachweises weder zum automatisierten Abruf personenbezogener Daten noch zur automatisierten Speicherung personenbezogener Daten verwendet werden. Hierunter zählte auch das Kopierverfahren.
(Nach Abschluss des Verfahrens haben sich die Regelungen im PAuswG geändert. Nunmehr sind Kopien von Personalausweisen zulässig, soweit der Inhaber in die Kopie einwilligt. Allerdings darf der Inhaber selbst bestimmen, welche Daten kopiert werden dürfen und die Kopie darf nicht an Dritte weitergegeben werden.)
Der Verkäufer stellte auf Forderung des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) die Anfertigung der Personalausweiskopien ein. Vielmehr wurden jetzt nur noch der Name und die Anschrift des Endkunden nach Vorlage des Personalausweises erhoben. Das zu führende Abgabebuch über das streitgegenständliche Produkt wurde in einem Stahlschrank des zusätzlich mit Alarmanlage und Sicherheitsdienst bewachten Gebäudes eingeschlossen, sodass sich niemand Zugang zu diesen sensiblen Daten verschaffen konnte.
Auch wenn eine gesetzliche Grundlage gegeben ist, personenbezogene Daten der Kunden zu erheben und zu verarbeiten, muss sich der Unternehmer auf das gesetzlich vorgegebene Maß beschränken. Zu Identifikationszwecken dürfen nach § 20 Abs. 2 PAuswG nur die hierfür erforderlichen Daten erhoben und mit dem Personalausweis abgeglichen werden.
Das Unternehmen zeigte sich sehr einsichtig im Hinblick auf datenschutzrechtliche Aspekte. Es informierte darüber, dass die Angaben, die zur Identifikation einer Person benötigt werden (Name und Anschrift), nach Vorlage des Personalausweises händisch auf der Rechnung zu dem speziellen Produkt erfasst werden können. Diese Rechnungen werden nunmehr in einem abgeschlossenen Aktenschrank aufbewahrt. Dieser ist vor unbefugtem Zugriff geschützt. Auch das Programm, mit dem die Rechnungen für die oben beschriebenen Produkte erstellt werden, ist nur nach Passworteingabe für einen bestimmten Personenkreis einsehbar. Außerdem ist das gesamte Gebäude außerhalb der Öffnungszeiten durch Alarmanlagen und Wachschutz gesichert.
Das Unternehmen hat auf Forderung des TLfDI die Arbeitsprozesse datenschutzgerecht ausgestaltet.

Zu Identifikationszwecken dürfen nach § 20 Abs. 2 PAuswG nur die hierfür erforderlichen Daten erhoben und mit dem Personalausweis abgeglichen werden. Kopien des Personalausweises sind ohne ausdrückliche Befugnis unzulässig.

3.15 Ver(un)sicherung

Dass in dem Wort „Versicherung“ zwar das Wort „sicher“ enthalten ist, seine Daten aber alles andere als das bei dieser Versicherung gewesen sind, musste ein thüringischer Bürger feststellen, als er unaufgefordert ein personalisiertes und mit seinen Daten versehenes Angebot für eine Kfz-Police von einer ihm bis dahin unbekannten Versicherung erhalten hat. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) nahm sich der Beschwerde an und forderte die Versicherung auf, dem Beschwerdeführer eine Auskunft gemäß § 34 Bundesdatenschutzgesetz (BDSG) zu erteilen, welche Daten über ihn gespeichert wurden, woher diese Daten stammen und an wen die Daten weitergegeben worden sind. Daraufhin wurde seitens des Versicherungsunternehmens, welches sich aus dem Briefkopf des Angebots ergeben hat, mitgeteilt, dass keine Daten über den Beschwerdeführer dort hinterlegt seien und der für dieses Unternehmen vor Ort zuständige Versicherungsvertreter die Daten wohl aus seiner Erinnerung heraus in das Angebot eingefügt hätte. Nach Vorhalt des TLfDI, dass es wohl nicht der Lebenserfahrung entspreche, dass ein Versicherungsvertreter spezifische Daten wie das Erstzulassungsdatum, das Kfz-Kennzeichen, die gefahrenen Kilometer, den genauen Fahrzeugtyp usw. einfach aus der Erinnerung heraus replizieren könne, wurde weiter erklärt, dass die selbstständigen Versicherungsvertreter vor Ort die Kundendaten für sich erheben und dort möglicherweise weiter nachzufragen sei. Daraufhin wandte sich der TLfDI an den aus dem Angebot ersichtlichen Versicherungsvertreter persönlich. Dieser gab an, dass er die personenbezogenen Daten des Beschwerdeführers aufgrund seiner vorherigen Tätigkeit für eine andere Versicherung noch in seinen Unterlagen gefunden und dann für die Erstellung des Angebotes verwendet hatte.

Das Erheben, Verarbeiten und Nutzen von personenbezogenen Daten ist nach § 4 Abs. 1 BDSG grundsätzlich unzulässig, es sei denn, es gibt eine Erlaubnisnorm in oder außerhalb des BDSG oder der Betroffene hat eingewilligt (sog. Verbot mit Erlaubnisvorbehalt). Eine

Einwilligung des Beschwerdeführers zur Erhebung seiner Daten lag hier nicht vor, im Gegenteil, der Beschwerdeführer hatte der Verwendung der Daten auch zu Werbezwecken ausdrücklich widersprochen. Auch eine gesetzliche Erlaubnisnorm ist hier nicht gegeben. Der Versicherungsvertreter war nach § 28 Abs. 1 Nr. 1 BDSG weder dazu ermächtigt, die Kundendaten der vorherigen Versicherung zu erheben noch diese zu verarbeiten. Er hatte in diesem Fall die Kundendaten des Beschwerdeführers bei dessen Versicherung nicht für den Zweck der Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen Schuldverhältnisses dieses Versicherungsunternehmens erhoben, sondern für eine andere Verwendung, nämlich um diese später für Zwecke der Werbung für ein anderes Versicherungsunternehmen zu verarbeiten. Eine Erhebung dieser Daten war nach § 28 Abs. 1 Nr. 1 BDSG schon gar nicht erforderlich, da es sich nicht um eine Erhebung für eigene Geschäftszwecke gehandelt hat und eine Verwendung der erhobenen Daten zu einem anderen Zweck nach § 28 Abs. 2 Nr. 1 BDSG hier ebenfalls nicht in Betracht kam, da die Daten auch nicht allgemein zugänglich gewesen sind oder zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich waren. Mindestens überwog jedoch das schutzwürdige Interesse der betroffenen Versicherten am Ausschluss der Verarbeitung, da es dem Betroffenen obliegt, sich seine Geschäftspartner selbst auszusuchen und darüber zu bestimmen, welcher Versicherung er sein Vertrauen schenkt. Auch eine Verarbeitung und Nutzung dieser Daten zum Zwecke der Werbung nach § 28 Abs. 3 BDSG ist unzulässig, da es hier, wie oben bereits festgestellt, an einer Einwilligung des Betroffenen offensichtlich gefehlt hat.
Der selbstständige Versicherungsvertreter wurde daher durch den TLfDI aufgefordert die unzulässig erhobenen und verwendeten Kundendaten gem. § 3 Abs. 4 Nr. 5 BDSG zu löschen. Dieser Forderung kam er dann auch nach, sodass ein anordnender Bescheid in der Sache nicht mehr ergehen musste.

Wie vorliegend geschildert, gibt es immer wieder Fälle, in denen personenbezogene Daten oder ganze Datensätze, wie hier aus Versicherungsverträgen, auf unzulässige Art und Weise erhoben und zweckentfremdet werden. Diese Verwendung darf jedoch nur dann geschehen, wenn der Betroffene eingewilligt hat oder aber ein Gesetz oder eine Rechtsvorschrift dies erlaubt.

3.16 Einmal hin, einmal her – Versicherungsvermittlung ist manchmal schwer

Wie bereits im Beitrag Nummer 8.11 des 2. Tätigkeitsberichts zum Datenschutz: nicht-öffentlicher Bereich 2014/2015 berichtet, erreichte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) die Beschwerde eines Versicherungskunden. Er meldete, dass sein ehemaliger Versicherungsmakler seine Kundendaten missbräuchlich verwendet hätte. Der Versicherungsmakler hatte seine Tätigkeit beim Vermittlungsbüro A aufgegeben und alle von ihm betreuten Kunden angeschrieben, um sie über seinen Wechsel zu Vermittlungsbüro B zu informieren. Im gleichen Schritt hatte er für eine Weiterführung seiner Betreuung mit dem neuen Vermittlungsbüro geworben und hierfür um eine Unterschrift auf der beigelegten Einverständniserklärung gebeten, die ihn dazu berechtigte, alle Versicherungspolicen auf das neue Vermittlungsbüro B umzustellen.
Der Beschwerdeführer unterschrieb solch eine zunächst, widerrief die Einwilligung aber wieder nach sechs Tagen.
Nach § 4 Bundesdatenschutzgesetz (BDSG) ist das Erheben, Verarbeiten und Nutzen von personenbezogenen Daten nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.
Die Umstellung der Versicherungspolicen erfolgte zunächst aufgrund der Einwilligung durch den Beschwerdeführer. Mit Einlegen des Widerrufs erlosch diese jedoch. Daraufhin stoppte der Versicherungsmakler die bereits vorgenommenen Schritte in der Umstellung. Das Versicherungsunternehmen wurde benachrichtigt, die Policen wieder auf das Vermittlungsbüro A zu übertragen. Somit wäre der Vorgang eigentlich erledigt gewesen.
Allerdings meldete sich der Beschwerdeführer nach einiger Zeit erneut beim TLfDI. Ihm wurde vom Versicherungsunternehmen abermals mitgeteilt, dass seine Versicherungspolicen, entgegen seinem Widerruf, über das Vermittlungsbüro B laufen. Der TLfDI wandte sich dann mit einem Auskunftsverlangen nach § 38 Abs. 3 BDSG an den Versicherungsmakler und das Versicherungsunternehmen, für das er tätig gewesen ist. Dabei stellte sich jedoch heraus, dass dem Versicherungsunternehmen bei der Verarbeitung ein Fehler unterlaufen war. Die notwendigen Änderungen im Vertrag haben sich ungünstig überschnitten, sodass die ursprünglich gewollte

Rückabwicklung nicht veranlasst wurde. Nachdem dieser Fehler aufgrund der Rückfrage des TLfDI aufgedeckt worden war, wurden die Versicherungspolicen so wie anfänglich veranlasst wieder zum Vermittlungsbüro A rückabgewickelt.

Gem. § 4 BDSG ist das Erheben, Verarbeiten und Nutzen von personenbezogenen Daten nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Sobald eine Einwilligung widerrufen wird, ist für die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten, die nur aufgrund einer Einwilligung des Betroffenen vonstattengehen, keine Ermächtigung mehr vorhanden. Die weitere Verwendung der personenbezogenen Daten muss sofort eingestellt werden. Außerdem sind die Daten, falls keine Aufbewahrungsfristen dagegen sprechen, unwiderruflich zu löschen.

3.17 Seminararbeit im Netz: nur ohne Personenbezug

Aufgrund einer Beschwerde wurde dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) bekannt, dass auf der Website eines Unternehmens eine Seminararbeit ohne Einwilligung der in der Seminararbeit erwähnten Personen veröffentlicht wurde. Darin waren auch personenbezogene Daten des Beschwerdeführers, der die Seminararbeit unterstützte, enthalten. Personenbezogene Daten sind nach § 3 Abs. 1 BDSG Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person (Betroffener). Es reicht also aus, wenn die Person noch bestimmbar ist. Nur durch Weglassen des Namens in einem Datensatz oder Dokument fehlt es nicht an der Bestimmbarkeit, wenn die äußeren Umstände eine Identifizierung zulassen. Im Fall der Seminararbeit traf dies zu, da diese über eine bestimmte Stelle berichtete und aufgrund der dortigen beruflichen Tätigkeit des Beschwerdeführers ein Bezug zum Beschwerdeführer unschwer hergestellt werden konnte. Mittels Auskunftsersuchen wurde das verantwortliche Unternehmen angeschrieben. Die Website mit der veröffentlichten Seminararbeit wurde daraufhin offline gestellt und das Dokument stillgelegt.
Das Verarbeiten von personenbezogenen Daten ist gem. § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG) zulässig, wenn dies durch das BDSG oder eine andere Rechtsvorschrift erlaubt ist oder angeordnet

wird oder der Betroffene in die Verarbeitung eingewilligt hat. Unter den Begriff der personenbezogenen Daten fallen auch solche Informationen, die einer Person mittelbar zugeordnet werden können und damit auch die vorliegende Seminararbeit.
Aufgrund der Veröffentlichung der personenbezogenen Daten auf der Website des Unternehmens wurden diese einer unbestimmten Anzahl von Dritten zur Verfügung gestellt und somit verarbeitet. Unter Verarbeiten fällt gemäß § 3 Abs. 4 BDSG das Übermitteln personenbezogener Daten. Übermitteln bedeutet nach § 3 Abs. 4 Nr. 3a) BDSG wiederum das Bekanntgeben von Daten an einen Dritten in der Weise, dass die Daten an den Dritten weitergegeben werden. Eine Rechtsvorschrift im BDSG oder anderen Gesetzen, die die Veröffentlichung der Daten erlaubt oder anordnet, war vorliegend nicht gegeben. In diesem Fall wäre eine Einwilligung der Betroffenen zur Veröffentlichung der Seminararbeit erforderlich gewesen, welche aber nicht erteilt wurde. Die Datenverarbeitung war daher unzulässig. Aufgrund des Tätigwerdens des TLfDI konnten durch das Offlinestellen der Website mit deren sämtlichen Inhalten datenschutzkonforme Zustände wiederhergestellt werden, sodass der Beschwerdeführer in seinem Recht auf informationelle Selbstbestimmung nicht mehr verletzt war.

Personenbezogene Daten sind nach § 3 Abs. 1 BDSG Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person (Betroffener). Es reicht also aus, wenn die Person noch bestimmbar ist. Im vorliegenden Fall erfolgte zwar keine namentliche Nennung, jedoch konnte durch die Informationen, die in der Arbeit enthalten waren, die betreffende Person ohne großen Aufwand identifiziert werden.

3.18 Welche Mitgliederdaten darf ein Verein erheben und an seinen Dachverband weitergeben?

Im November 2016 bat der Thüringer Landesverband eines Vereins den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) um die Information, ob seine Satzung hinsichtlich der datenschutzrechtlichen Bestimmungen angepasst werden muss. Hierbei ging es insbesondere darum, welche Mitgliederdaten der Landesverband erheben, verarbeiten und an seine Dachverbände weitergeben darf und welche datenschutzrechtlichen

Informationen auf den Mitgliedsanträgen des Verbands aufgeführt werden müssen. Weiterhin wollte der Landesverband wissen, ob Datenschutzerklärungen für Amtsträger und hauptamtliche Mitarbeiter im Kreis-, Landes-, Bundes- und Europaverband notwendig sind.
Der TLfDI legte dar, dass er nicht die zuständige Aufsichtsbehörde für den Bundes- und den Europaverband des Vereins ist. Zuständige Aufsichtsbehörde für den Bundesverband mit Sitz in Berlin sei der Berliner Datenschutzbeauftragte und für den Europaverband die Commission de la protection de la vie privée in Brüssel. Dementsprechend bot der TLfDI an, die Anfrage des Landesverbandes an die zuständigen Stellen weiterzuleiten.
In Bezug auf den Landesverband Thüringen beantwortete der TLfDI die Fragen des Verbandes folgendermaßen: Vereine, die personenbezogene Daten erheben und verarbeiten, sind gemäß § 2 Abs. 4 Satz 1 Bundesdatenschutzgesetz (BDSG) nicht-öffentliche Stellen, auf die das BDSG Anwendung findet (§ 1 Abs. 2 Nr. 3 BDSG).
Nach § 4 Abs. 1 BDSG dürfen personenbezogene Daten nur erhoben, verarbeitet oder genutzt werden, soweit das BDSG oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder die betroffene Person eingewilligt hat. Eine Vereinssatzung kann jedoch, ebenso wenig wie die Satzung eines Dachverbands, als Rechtsvorschrift im Sinne von § 4 Abs. 1 BDSG das Schutzniveau des BDSG unterschreiten. Daher bedarf es einer anderen Rechtsnorm. Nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG ist das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten – im vorliegenden Falle Mitgliederdaten – oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses erforderlich ist. Einem Schuldverhältnis immanent sind gegenseitige Rechte und Pflichten.
Die Mitgliedschaft in einem Verein bzw. dessen Landesverband ist als ein Schuldverhältnis im Sinne des § 28 Abs. 1 Satz 1 Nr. 1 BDSG anzusehen. Denn hier bestehen Rechte und Pflichten der Mitglieder untereinander und zum Verein. Diese Rechte und Pflichten ergeben sich überwiegend aus dem Inhalt der Vereinssatzung. Der durch die Satzung verfolgte Vereinszweck ist gem. § 28 Abs. 1 Nr. 1 BDSG maßgebend für die Zulässigkeit der Datenverarbeitung. Daher darf der Landesverband Thüringen nur die Daten seiner Mitglieder erheben, die er zur Erfüllung seiner satzungsgemäßen Aufgaben und zur Gestaltung der Mitgliedschaft unbedingt benötigt. Daher ist für den

Umgang mit den Mitgliedsdaten regelmäßig § 28 Abs. 1 Satz 1 Nr. 1 BDSG maßgebende Rechtsgrundlage. Somit darf der Landesverband auf seinen Mitglieds- bzw. Aufnahmeanträgen beim Beitritt eines Mitglieds gemäß § 28 Abs. 1 Satz 1 Nr. 1 BDSG nur die personenbezogenen Daten erheben, die für die Begründung und Durchführung des Mitgliedsverhältnisses benötigt werden. Die dafür erforderlichen Daten müssen im Mitgliedsantrag festgelegt und entsprechend gekennzeichnet werden.
Um seinen Vereinszweck erfüllen zu können, benötigt der Thüringer Landesverband in jedem Falle die „Korrespondenzdaten“ (Name und Anschrift) seiner Mitglieder. Sofern weitere Daten für die Vereinsarbeit erforderlich sind, dürfen auch diese erhoben werden (Beispiel: Kontodaten für den Lastschrifteinzug des Mitgliedsbeitrags). Letztlich muss aber immer gewährleistet sein, dass die Vereinsmitglieder hierüber informiert werden. Nach § 4 Abs. 3 BDSG ist der Betroffene über folgende Umstände in Kenntnis zu setzen:

1. die Identität der verantwortlichen Stelle (der Landesverband Thüringen),
2. die Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung der Daten,
3. die Empfänger der Daten, soweit die Daten weitergeleitet werden und der Betroffene nicht mit einer Übermittlung zu rechnen hatte.

Für nicht erforderliche Daten zur Begründung und Durchführung des Vereinsverhältnisses muss es dem jeweiligen Mitglied selbst überlassen bleiben, ob es Angaben dazu machen möchte oder nicht. Nach der Satzung des Landesverbandes können natürliche Personen, die das 35. Lebensjahr noch nicht vollendet haben, ordentliche Mitglieder werden. Somit ist auch die Angabe des Geburtsdatums für die Mitgliedschaft wichtig. Die Pflichtangabe der E-Mail-Adresse der Mitglieder in der Satzung des Landesverbandes ist nicht zulässig, weil es jedem Mitglied selbst überlassen bleiben muss, ob es diesen Weg der Kommunikation zulassen möchte oder nicht.
Bei der Frage, welche Mitgliederdaten erforderlich sind, muss immer der Grundsatz der Datenvermeidung und Datensparsamkeit nach § 3a Satz 1 BDSG beachtet werden. In diesem Sinne sollte auch die Angabe der Telefonnummer dem Mitglied freigestellt werden, da dies zur Verfolgung der Vereinsziele sowie für die Betreuung und Verwaltung der Mitglieder nicht erforderlich erscheint. Insofern

sollte diese Angabe ausdrücklich als „Freiwillige Angabe“ im Aufnahmeantrag aufgeführt werden.
Nach Ansicht des TLfDI ist es empfehlenswert, von jedem Mitglied schon beim Eintritt in den Verein eine Einwilligungserklärung nach BDSG einzuholen. Diese Einwilligung sollte sich optisch vom Beitrittsformular unterscheiden und mit einer gesonderten Unterschrift bestätigt werden. Im Mitgliedsantrag wird die Einwilligung nach BDSG zusammen mit den anderen Erklärungen zur Mitgliedschaft schriftlich erteilt. Insofern schlug der TLfDI vor, dies im Sinne von § 4a Abs. 1 BDSG drucktechnisch besonders (z. B. farbig) kenntlich zu machen.
Soweit der Landesverband Thüringen seine Mitgliederdaten an die Dachverbände (Bundes- und Europaverband) weitergibt, handelt es sich um eine Datenübermittlung an Dritte im Sinne des § 3 Abs. 4 Nr. 3 BDSG, da gemäß § 3 Abs. 8 Satz 2 BDSG ein Bundes- oder Europaverband im Verhältnis zum Landesverband ein sogenannter Dritter ist. Somit benötigt der Landesverband, wenn er seine Mitgliedsdaten an den Bundes- oder Europaverband übermitteln will, eine Rechtsgrundlage oder die ausdrückliche Einwilligung der betroffenen Mitglieder. Dies ist nur dann unproblematisch, wenn es lediglich um die Übermittlung von anonymisierten Daten zu statistischen Zwecken geht, beispielsweise die Anzahl der Mitglieder, da dann überhaupt keine personenbezogenen Daten verarbeitet werden.
Nach Kenntnis des TLfDI und aufgrund seiner Satzung ist der Landesverband Thüringen jedoch dazu verpflichtet, die in der Satzung benannten konkreten personenbezogenen Daten seiner Mitglieder (Name, Geschlecht, Geburtsdatum, Anschrift, Telefonnummer und E-Mail-Adresse) an den Bundesverband weiterzugeben. Dort werden diese Daten im Rahmen der Mitgliedschaft für interne Vereinszwecke verarbeitet und genutzt, insbesondere für die Mitgliederverwaltung, -information und -betreuung. Für die Weitergabe der Daten an die Dachverbände empfahl der TLfDI dem Landesverband Thüringen, entsprechende klare Regelungen bereits beim Eintritt in den Landesverband festzuschreiben und eindeutig im Mitgliedsantrag zu formulieren. Diese Satzungsklauseln sind verbindlich für alle Vereinsmitglieder, da sie den Regelungen durch ihre Mitgliedschaft und die damit verbundene Anerkennung der Satzung zustimmen und insofern zur genannten Verwendung der Daten eine persönliche Einwilligung erteilen.

Die Frage des Landesverbandes, ob Datenschutzerklärungen für Amtsträger und hauptamtliche Mitarbeiter im Kreis-, Landes-, Bundes- und Europaverband notwendig sind, beantwortete der TLfDI folgendermaßen: Personen, die mit der Verarbeitung von personenbezogenen Daten betraut sind, müssen gemäß § 5 BDSG auf das Datengeheimnis verpflichtet werden. Dies gilt auch für ehrenamtlich im Verein tätige Personen, wenn sie mit der Datenverarbeitung befasst sind. Dazu sollte der Landesverband ein Merkblatt vorbereiten und per Unterschrift von den betreffenden Personen bestätigen lassen. Der TLfDI verwies hierzu auf die Mustervorlage zur Verpflichtung auf das Datenschutzgeheimnis auf seiner Internetseite unter https://www.tlfdi.de/tlfdi/themen/unternehmen/. Diese Vorlage müsste der Thüringer Landesverband ggf. an seine Bedürfnisse anpassen.

Vereine, die personenbezogene Daten erheben und verarbeiten sind gemäß § 2 Abs. 4 Satz 1 Bundesdatenschutzgesetz (BDSG) nichtöffentliche Stellen, auf die das BDSG anzuwenden ist (§ 1 Abs. 2 Nr. 3 BDSG). Nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG ist das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses erforderlich ist. Ein Schuldverhältnis ist eine Rechtsbeziehung mit gegenseitigen Rechten und Pflichten. Im Rahmen der Vereins- oder Verbandsmitgliedschaft bestehen Rechte und Pflichten der Mitglieder untereinander und zum Verein.
Bei der Frage, welche Mitgliederdaten erforderlich sind, muss immer der Grundsatz der Datenvermeidung und Datensparsamkeit nach § 3a Satz 1 BDSG beachtet werden. Die E-Mail-Adresse und die Telefonnummer zählen nicht zu den zwingend erforderlichen (Korrespondenz-)Daten zur Erfüllung der Vereinszwecke. Dies sind vorrangig Name und Anschrift des Vereinsmitglieds und – sofern die Vereinssatzung eine Altersgrenze für die Mitgliedschaft vorschreibt – das Geburtsjahr.
Für die Weitergabe seiner Mitgliederdaten an einen übergeordneten oder Dachverband benötigt der Verein eine Rechtsgrundlage oder die

ausdrückliche Einwilligung der betroffenen Mitglieder. Der TLfDI empfiehlt, von jedem Mitglied schon beim Eintritt in den Verein eine Einwilligungserklärung nach BDSG einzuholen

3.19 Zahlartensteuerung – nein, danke!

Der Onlinehandel ist für den Kunden eine bequeme und schnelle Art des Einkaufens. Er hat eine nahezu unendlich große Auswahl an Produkten und entscheidet sich dann für das attraktivste Angebot. Dass dies aber leider nicht für die Abwicklung des Kaufes und die Auswahl der bevorzugten Zahlart zutrifft, musste ein Betroffener feststellen, als er in einem Thüringer Online-Versandhandel seinen Warenkorb füllte und dann per Kreditkarte zahlen wollte. Der Betroffene hatte seine persönlichen Daten, wie Name, Adresse, Geburtsdatum usw., eingegeben und wurde dann zur Zahlartenauswahl weitergeleitet, wo ihm dann aber nur der Kauf per Vorauskasse oder Sofortüberweisung angeboten wurde, obwohl das Unternehmen auch andere Zahlarten, wie Kauf auf Rechnung, Kreditkarte, Lastschrift oder PayPal, anbietet. Verwundert über diese doch sehr geringe Auswahlmöglichkeit in seinem Fall, wandte sich der Betroffene an das Unternehmen und erhielt dort die Auskunft, dass im Vorfeld der Zahlartenauswahl, eine Bonitätsabfrage bei einer Wirtschaftsauskunftei veranlasst wird und entsprechend dem Ergebnis dieser Abfrage für ihn nur begrenzte Zahlarten zur Verfügung stehen. Der Betroffene sah darin einen Verstoß gegen datenschutzrechtliche Vorgaben und wandte sich mit der Bitte um Prüfung dieses Vorgehens bei der Bestellung an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) als zuständige Datenschutzaufsicht für in Thüringen ansässige Unternehmen.
Der TLfDI forderte daher das Unternehmen zur Auskunft darüber auf, inwieweit das vom Betroffenen geschilderte Prozedere zutrifft und wann genau die Abfrage bei der Wirtschaftsauskunftei erfolgt. Der TLfDI vertrat dabei die Auffassung, dass die Abfrage bei der Wirtschaftskanzlei noch vor Eingabe der Zahlart ein unzulässiges Vorgehen darstellt. Dabei ist ausschlaggebend, dass die Zulässigkeit der Datenverarbeitung sich aufgrund des Bundesdatenschutzgesetzes (BDSG) oder einer anderen Rechtsvorschrift ergeben muss. Das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke ist zulässig, soweit es zur Wahrung berechtigter Inte-

ressen der verantwortlichen Stelle dient und erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen am Ausschluss der Verarbeitung oder Nutzung überwiegt (§ 28 Abs. 1 Nr. 2 BDSG).
Ein berechtigtes Interesse des Unternehmens daran, das kreditorische Risiko bei unsicheren Zahlarten gering zu halten, ist durchaus als gegeben anzunehmen. Eine Zahlartensteuerung ist aber zur Wahrung dieses Interesses keinesfalls erforderlich. Es reicht nicht aus, dass aus der Sicht des Unternehmens die Verwendung geeignet oder zweckmäßig erscheint. Im Bestellprozess des Unternehmens wurde noch vor der Entscheidung des Kunden für eine bestimmte, möglicherweise ein kreditorisches Risiko auslösende Zahlart eine Bonitätsprüfung bei einer Auskunftei veranlasst. Die Bonitätsabfrage wurde damit auf einen Zeitpunkt vorverlagert, zu dem sie noch überhaupt nicht für die Wahrung des berechtigten Interesses des Unternehmens erforderlich war.
Es ist dem Onlinehändler ohne weiteres möglich, eine Auswahl der vom Kunden beabsichtigten Zahlart abzuwarten und erst bei Entscheidung für eine unsichere Zahlmethode eine Bonitätsauskunft bei einer Auskunftei einzuholen. Die Auswahlmöglichkeit des Kunden muss sich auf alle angebotenen Zahlarten beziehen. Die für den Betreiber unsicheren Zahlmethoden (Rechnung und Lastschrift) sind zudem mit dem Hinweis zu versehen, dass bei Auswahl ggf. eine Bonitätsprüfung vorbehalten bleibt. Insoweit wird auch dem Transparenzgebot Rechnung getragen und der Kunde vorab darüber informiert, mit welchen Konsequenzen er bei Auswahl einer bestimmten Zahlart rechnen muss.

Die Abfrage bei einer Auskunftei darf erst dann erfolgen, wenn der Kunde sich im Rahmen des Bestellvorgangs für eine bestimmte Zahlart entschieden hat. Für den Fall der Entscheidung für eine sog. risikolose Zahlart (Vorkasse, Kreditkarte, paypal u. ä.), also solche, bei denen für ein Unternehmen kein kreditorisches Risiko entsteht, ist eine Abfrage bei einer Auskunftei keinesfalls erforderlich und verstößt damit gegen die Regelungen des BDSG. In jedem Fall aber sind die hier beschriebenen Zahlartensteuerungen unzulässig.

3.20 Der TLfDI macht viel – aber nicht alles

Besorgte Bürger wandten sich auch im aktuellen Berichtszeitraum an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) mit gut 100 Anfragen und Beschwerden, die nicht in die Zuständigkeit des TLfDI fielen. Denn der TLfDI kontrolliert gemäß § 37 Thüringer Datenschutzgesetz (ThürDSG) bei allen öffentlichen Stellen die Einhaltung der Bestimmungen über den Datenschutz und ist gemäß § 42 ThürDSG i. V. m. § 38 Abs. 6 Bundesdatenschutzgesetz (BDSG) Aufsichtsbehörde für die nicht-öffentlichen Stellen im Freistaat Thüringen. Die örtliche Zuständigkeit richtet sich grundsätzlich nach dem Sitz der für die Datenverarbeitung verantwortlichen Stelle bzw. nach dem Ort einer Betriebsstätte. Gingen die Beschwerden der Bürger per E-Mail ein, so wurde den Beschwerdeführern die Adresse der zuständigen Aufsichtsbehörde genannt. Gingen die Beschwerden per Briefpost beim TLfDI ein, wurde über die Nichtzuständigkeit des TLfDI informiert und angefragt, ob die Anfrage an die zuständige Stelle gesandt werden soll. Bei Einverständnis des Beschwerdeführers wurde das Schreiben weitergeleitet.

Beispiele für die Unzuständigkeit des TLfDI

Nicht zuständig ist der TLfDI z. B. für die Bereiche Telekommunikation, Rundfunk (Radio und Fernsehen), kirchliche Stellen und Jobcenter (sofern es sich nicht um Optionskommunen handelt). Welche Stellen hierfür jeweils zuständig sind, wurde bereits im 2. Tätigkeitsbericht unter 2.35 näher erläutert.
Ebenfalls nicht zuständig ist der TLfDI für die Datenschutzkontrolle von Postdienstunternehmen. Für die Kontrolle dieser Unternehmen ist die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit mit Sitz in 53117 Bonn, Husarenstraße 30, E-Mail: poststelle@bfdi.bund.de zuständig, unabhängig davon, wo der Sitz des Unternehmens ist.
Für die Kontrolle der Verarbeitung von personenbezogenen Daten bei den Krankenkassen ist das jeweilige Bundesland, in welchem der Hauptsitz ist, zuständig, auch wenn es in Thüringen eine entsprechende Niederlassung gibt.

Die Beschwerden über die Schufa müssen an den Hessischen Datenschutzbeauftragten, Gustav-Stresemann-Ring 1 in 65189 Wiesbaden gerichtet werden, da der Sitz der SCHUFA in Wiesbaden ist.



Bei Beschwerden über Unternehmen, die ihre Hauptniederlassung im Ausland haben, ist die jeweilige Datenschutzaufsichtsbehörde des Landes zuständig. Die entsprechenden Adressen und Ansprechpartner findet man im Virtuellen Datenschutzbüro unter https://www.datenschutz.de.

Die Zuständigkeit der Kontrolle des TLfDI richtet sich nach dem Sitz der Daten verarbeitenden Stelle bzw. nach dem Hauptsitz der Betriebsstätte. Denn der TLfDI kontrolliert gemäß § 37 ThürDSG bei allen öffentlichen Stellen die Einhaltung der Bestimmungen über den Datenschutz und ist gemäß § 42 ThürDSG i. V. m. § 38 Abs. 6 BDSG Aufsichtsbehörde für die nicht-öffentlichen Stellen im Freistaat Thüringen.

3.21 Pressefreiheit versus Datenschutz?

Ein Bürger wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und beschwerte sich darüber, dass die Presse personenbezogene Daten veröffentlichte. Der Bürger hatte sich mit Missständen innerhalb seiner Kommune an die Presse gewandt. Diese veröffentlichte hierzu auch einen Artikel, jedoch nicht nur das. Während der Bürger die Veröffentlichung begrüßte, da er damit ja auch etwas bewirken wollte, rechnete er jedoch nicht mit der Veröffentlichung seines vollständigen Namens. Er war der Überzeugung, dass dies eine erhebliche Verletzung des Datenschutzes sei und bat um diesbezügliche Klärung. Des Weiteren wollte er wissen, ob und welche rechtlichen Schritte er gegen die Zeitung einleiten kann.
Leider kann der TLfDI nur den Dingen nachgehen, die im Rahmen seiner Zuständigkeiten liegen. Dies ist im Pressebereich in der Regel nicht der Fall. So regelt § 41 BDSG das sogenannte Presseprivileg. Darin wird geregelt, dass der Landesgesetzgeber in bestimmten Bereichen Regelungen für die Presse erlassen muss. Dort regelt der Landesgesetzgeber in § 11a Thüringer Pressegesetz:

Soweit Unternehmen oder Hilfsunternehmen der Presse personenbezogene Daten ausschließlich zu eigenen journalistisch-redaktionellen oder literarischen Zwecken erheben, verarbeiten oder nutzen, gelten von den Bestimmungen des Bundesdatenschutzgesetzes (BDSG) nur die §§ 5, 9 und 38a sowie § 7 mit der Maßgabe, dass nur für Schäden gehaftet wird, die durch eine Verletzung des Datengeheimnisses nach § 5 BDSG oder durch unzureichende technische oder organisatorische Maßnahmen im Sinne des § 9 BDSG eintreten.
Da damit die Anwendung von § 38 BDSG bei rein redaktionellen oder journalistischen Tätigkeiten ausgeschlossen ist, sich die Zuständigkeit des TLfDI aber aus § 38 Abs. 6 BDSG (i. V. m. § 42 Abs. 1 Thüringer Datenschutzgesetz) ergibt, folgt daraus die Unzuständigkeit des TLfDI in solchen rein redaktionellen oder journalistischen Tätigkeiten.
Anwendbar bleibt das BDSG jedoch, wenn es sich nicht um eine reine redaktionelle oder journalistische Tätigkeit handelt, § 41 Abs. 1 BDSG.
Im hier vorliegenden Fall handelte es sich jedoch ganz klar um eine rein journalistische Angelegenheit, weswegen der TLfDI dem Bürger gegenüber seine Unzuständigkeit erklärt hätte.
Noch bevor der TLfDI im Fall irgendetwas unternehmen konnte, meldete sich der betroffene Bürger jedoch nochmals und teilte mit, er wünsche doch keine Verfolgung, da sich die Redaktion entschuldigt habe.
Dem Bürger wurde dennoch mitgeteilt, dass der TLfDI für die hiesige Beschwerde über den mutmaßlichen Datenschutzverstoß ohnehin nicht die zuständige Behörde sei, da es sich um eine rein journalistische Angelegenheit handelt und der TLfDI insoweit nicht Aufsichtsbehörde sei. Sollte der Bürger trotzdem eine Prüfung wünschen, müsse er sich an den Deutschen Presserat wenden.

Zwar ist der TLfDI bei rein redaktionellen oder journalistischen Tätigkeiten nicht die zuständige Aufsichtsbehörde, jedoch müssen diese Voraussetzungen auch greifen. Handelt es sich nicht um eine ausschließlich journalistische oder ausschließlich redaktionelle Tätigkeit, sondern werden die personenbezogenen Daten auch anderweitig verwendet, ist der TLfDI zuständig.

3.22 Wie oft muss man der Hausbank den Personalausweis vorlegen?

Ein Bankkunde wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), weil er im Jahr 2016 ohne Angabe der Rechtsgrundlage von seiner Bankfiliale in Thüringen aufgefordert worden war, seinen Personalausweis zum Zweck der Aktualisierung der Ausweisdaten im System der Bank zur Filiale mitzubringen. Bereits drei Jahre zuvor war der Kunde nämlich auch schon zur Vorlage seines Personalausweises aufgefordert worden, wobei sich bei der damaligen Prüfung durch den Datenschutzbeauftragten der Bank ergab, dass hierfür keine Rechtsgrundlage bestand bzw. die angegebene Rechtsgrundlage (§ 154 Abgabenordnung) keine Vorlage des Ausweises begründete und der Bank ein Fehler unterlaufen war.
Die Datenschutzabteilung der Bank erklärte dem TLfDI auf seine Nachfrage, dass die Bank nach den §§ 3 und 4 des Gesetzes über das Aufspüren von Gewinnen aus schweren Straftaten (Geldwäschegesetz – GwG) im Rahmen ihrer Sorgfaltspflicht zur Identifizierung und kontinuierlichen Überwachung ihrer Vertragspartner verpflichtet sei. Gemäß § 3 Abs. 1 Nr. 4 GwG müsse daher sichergestellt werden, dass die jeweiligen Dokumente, Daten oder Informationen in angemessenem zeitlichen Abstand aktualisiert werden. Eine erneute Legitimation des Bankkunden durch Vorlage des Ausweises sei eigentlich nur dann erforderlich, wenn zum Beispiel bei der Kontoeröffnung die Dokumente nicht vollständig oder nur in Kopie vorgelegt werden konnten. Dies sei im vorliegenden Fall aber nicht gegeben gewesen, vielmehr sei aufgrund eines Versehens die erneute Legitimation erbeten worden. Dafür habe man sich beim Beschwerdeführer bereits entschuldigt.
Auch wenn der Beschwerdeführer bereits zum zweiten Mal zur Vorlage von Identifikationspapieren zur Aktualisierung aufgefordert wurde, ohne dass die konkrete Rechtsgrundlage angegeben worden war, hat der TLfDI das jeweilige Versehen zwar als unverständlich angesehen, weitere Nachforschungen waren jedoch nicht angezeigt, denn eine unzulässige Erhebung und Verarbeitung nicht erforderlicher Daten erfolgte letztendlich nicht.

Banken sind nach dem Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten (Geldwäschegesetz – GwG) im Rahmen

ihrer Sorgfaltspflicht zur Identifizierung und kontinuierlichen Überwachung ihrer Vertragspartner verpflichtet. Sie müssen sicherstellen, dass die jeweiligen Dokumente, Daten oder Informationen in angemessenem zeitlichem Abstand aktualisiert werden. Jede Aufforderung, die Ausweispapiere vorzulegen, bedarf einer Rechtsgrundlage, die gegenüber dem Betroffenen angegeben werden muss.

3.23 Wenn die Hausbank keine Auskunft erteilt

Ein Rechtsanwalt wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und beschwerte sich im Namen seines Mandanten darüber, dass von einer Bankfiliale in Thüringen seine Fragen nicht beantwortet wurden. Das Auskunftsbegehren nach § 34 Abs. 1 Bundesdatenschutzgesetz (BDSG) bezog sich auf die zur Person des Mandanten gespeicherten Daten, deren Herkunft sowie der Empfänger oder Kategorien von Empfängern, an die die Daten weitergegeben wurden. Hintergrund war, dass offenbar Gerüchte und Informationen über die Firma des Mandanten kursierten, deren Ursprung der Mandant in der Bank vermutete. Schließlich sah er dadurch seine Firma in Misskredit gezogen.
Der TLfDI wandte sich mit einem Auskunftsbegehren nach § 38 Abs. 1 Satz 1 BDSG an die Bankfiliale. Postwendend teilte die für Datenschutz zuständige Abteilung am Hauptsitz der überregionalen Bank mit, der TLfDI habe offensichtlich übersehen, dass sich der Sitz der nicht-öffentlichen Stelle nicht in Thüringen befinde und solle sich mit der zuständigen Datenschutzaufsichtsbehörde in Verbindung setzen. Der TLfDI wies darauf hin, dass die Zuständigkeit der Datenschutzaufsicht in Thüringen nicht als grundsätzlich ausgeschlossen angesehen werden könne. § 3 Abs. 1 Nummer 2 Thüringer Verwaltungsverfahrensgesetz bestimmt nämlich die örtliche Zuständigkeit für Betriebsstätten in Thüringen, die dann beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit liegt, wenn eine Angelegenheit von der Betriebsstätte selbst vorgenommen oder geregelt wird. Die Abteilung Datenschutz der Bank am Hauptsitz legte daraufhin dar, dass eine Auskunftserteilung im Rahmen des § 34 BDSG ausschließlich durch den betrieblichen Datenschutzbeauftragten am Hauptsitz der Bank erfolge. Die Filialen (Betriebsstätten) lieferten hierzu gegebenenfalls Informationen, eine eigenständige Auskunftserteilung durch die Filiale erfolge jedoch

nicht. Im Übrigen habe man die Anfrage des TLfDI bereits zum Anlass genommen, dem Kunden die gewünschte Auskunft zu erteilen. Der Anwalt des Kunden sah jedoch durch die offenbar erteilte Auskunft noch keine Erledigung der Sache und bat den TLfDI um Abgabe an die für den Hauptsitz zuständige Datenschutzaufsicht. Dem kam der TLfDI selbstverständlich nach.

Der TLfDI ist nach § 3 Abs. 1 Nummer 2 Thüringer Verwaltungsverfahrensgesetz zuständige Datenschutzaufsicht für Betriebsstätten in Thüringen. Handelt es sich dabei um Niederlassungen eines überregionalen Unternehmens mit Hauptsitz in einem anderen Bundesland, ist zu prüfen, ob die Betriebsstätte oder Filiale in Thüringen eigene Handlungsspielräume oder Regelungskompetenzen hat. Wird dies verneint, ist der Vorgang an die für den Sitz des Hauptunternehmens zuständige Datenschutzaufsicht abzugeben.

3.24 Frage eines Software-Entwicklers: Veröffentlichung von Vertretungsplänen sowie Stundenplänen innerhalb einer App für Schulen

„Ist nun morgen Deutsch statt Astro in der Ersten?“ „Haben wir nachher Sport bei Herrn Freistoß oder vertritt Frau Sprint?“ – Ganz normale Fragen im Schulalltag. Die Antworten darauf ändern sich oft schneller wie der Vertretungsplan, der vor dem Lehrerzimmer hängt. Da wär’ doch eine Info auf dem Smartphone ganz sinnvoll, oder?
Die Verwendung moderner Kommunikationskanäle hat auch in vielen Schulen Einzug gehalten. Oft nutzen sie ihre Internetseiten, um Informationen an Schüler, Lehrer und Eltern schnell und papierlos zu verteilen. Dabei stellt sich oft die Frage, ob die Verteilung personenbezogener Informationen, die ja regelmäßig in solchen Nachrichten stecken, datenschutzrechtlich immer o. k. ist oder nicht.
Diese Frage sollte auch Softwarefirmen beschäftigen, die einen Bedarf an Applikationen für die Zielgruppe Schule sehen und decken wollen. Erfreulich ist es, wenn diese Sensibilität besteht. Datenschutzfreundliche Programme sind durchaus nicht die Regel, wie viele Beispiele beweisen. Dass es anders geht, beweist eine Anfrage eines Softwareherstellers an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Er bat um Klärung, ob Vertretungspläne in einem passwortgeschützten Bereich

zulässig wären, auf den nur Schüler der jeweiligen Schule und ggf. auch nur der betroffenen Klasse Zugriff haben. Der TLfDI antwortete, dass dies grundsätzlich möglich sei. Auch gegen die Veröffentlichung der Namen der vertretenden Lehrkräfte spräche dann nichts, wenn die Schule dies aus bestimmten Gründen für erforderlich hält. Klargestellt wurde aber auch, dass eine Veröffentlichung im jedermann zugänglichen Bereich der Schulhomepage, ggf. unter Bekanntgabe der Lehrernamen, nicht zulässig wäre, weil dies zur Aufgabenerfüllung der Schule nicht erforderlich ist. Insgesamt ist es wichtig, die Datenflüsse entsprechend den Anforderungen des Datenschutzrechts zu gestalten. Sobald der Softwarefirma etwa für die Anmeldung personenbezogene Daten übermittelt werden, ist ein Vertrag über die Auftragsdatenverarbeitung zu schließen. Im Hinblick auf die grundsätzlichen Probleme der Nutzung von Apps an Schulen wird auf den Beitrag unter Punkt 12.29 im 12. Tätigkeitsbericht des TLfDI im öffentlichen Teil verwiesen.

Den TLfDI erreichte eine Anfrage, ob Vertretungspläne von Schulen inkl. Lehrernamen in passwortgeschützten Bereichen von Apps erlaubt seien. Der TLfDI bestätigte das grundsätzlich, wies jedoch darauf hin, dass im Gegensatz dazu eine Veröffentlichung in für jedermann zugänglichen Bereichen von Schulhomepages o. ä. für die Aufgabenerfüllung der Schule grundsätzlich nicht erforderlich und damit unzulässig ist.

3.25 Mitgliedsbeiträge am schwarzen Brett?

Der Betriebsrat der Beschäftigten eines gemeinnützigen Vereins wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und bat um Einschätzung, ob die Geschäftsleitung befugt sei, Listen für alle Mitarbeiter einsehbar auszuhängen, aus denen ersichtlich ist, welche Mitgliedsbeiträge die einzelnen Beschäftigten bezahlen. Dabei war in der Satzung des gemeinnützigen Vereins kein Mindestbeitrag festgelegt worden, jedoch hatte man seitens der Geschäftsleitung Vorstellungen, welche Beträge entrichtet werden sollten. Auch wollte man Anreize schaffen, dass diejenigen Mitarbeiter, die noch nicht Mitglied in dem gemeinnützigen Verein waren, beitreten und ebenfalls Beiträge entrichten. Durch diese Vorgehensweise fühlten sich die Mitarbeiter unter Druck gesetzt.

Beratend führte der TLfDI aus, der Aushang der Liste stelle eine Verarbeitung von Beschäftigtendaten verschiedener Betroffener in der Form der Übermittlung an andere Mitarbeiter dar, die nur dann zulässig sei, wenn eine Rechtsgrundlage hierfür existiert. Eine solche sei jedoch nicht erkennbar. § 32 Bundesdatenschutzgesetz (BGSG) als maßgebliche Vorschrift für die Verarbeitung von Beschäftigtendaten könne hierfür nicht herangezogen werden. Selbst wenn die Vereinsmitgliedschaft im Falle eines sogenannten Tendenzbetriebs Voraussetzung für die Beschäftigten sein sollte und daher unter Umständen vom Arbeitgeber erhoben und verarbeitet werden dürfte, rechtfertigte dies noch keine Übermittlung an andere Mitarbeiter.
Auch eine Einwilligung nach § 4a Abs. 1 Satz 3 BGSG konnte keine Rechtsgrundlage für die eingangs geschilderte Vorgehensweise bilden. Maßgeblich für eine wirksame Einwilligung ist, dass sie auf Freiwilligkeit beruht, wovon im Beschäftigtenverhältnis regelmäßig nicht ausgegangen werden kann, weil der Beschäftigte möglicherweise im Falle einer Verweigerung der Einwilligung mit Nachteilen rechnet.
Im Ergebnis war die Veröffentlichung der Namen und der Mitgliedsbeiträge von Vereinen weder mit noch ohne Zustimmung der Betroffenen zulässig.
Für den Betriebsrat war die Auskunft offenbar hilfreich.

Ein gemeinnütziger Verein ist nicht befugt, die Mitgliedschaft und die entrichteten Mitgliedsbeiträge der bei ihm Beschäftigten zu veröffentlichen. Weder § 32 BDSG noch die Einwilligung der Betroffenen können eine Rechtsgrundlage hierfür bilden.

3.26 Der Übergang von Kundendaten bei Unternehmensverkäufen

Im Rahmen verschiedener Anfragen von Unternehmen und auch von mit der Abwicklung von Unternehmensinsolvenzen betrauten Insolvenzverwaltern wurde an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit folgendes Problem herangetragen und um eine datenschutzrechtliche Lösung nachgesucht: Wie ist mit Kundendaten im Rahmen von Unternehmensverkäufen umzugehen?
Kundendaten haben einen erheblichen wirtschaftlichen Wert und stellen daher im Rahmen von Unternehmensverkäufen nicht selten

den hauptsächlichen Wert des Unternehmens dar. Auch im Hinblick auf die Veräußerung von Betriebsteilen oder werthaltigen Wirtschaftsgütern (sog. Assets) im Rahmen einer Insolvenz stellt sich diese Frage, weil auch hier der Wert in den vorhandenen Kundendatensätzen liegt.
In diesem Zusammenhang ist es jedoch notwendig, die datenschutzrechtlichen Grundsätze nicht außer Acht zu lassen, da Kundendaten keine „Ware“ sind, sondern dafür eigene gesetzliche Regelungen greifen.
Regelmäßig geht es dem Erwerber beim Unternehmenskauf darum, die Altkunden mittels Werbung ansprechen zu können. Die Datenübermittlung zu Werbezwecken ist in § 28 Abs. 3 Bundesdatenschutzgesetz (BDSG) abschließend geregelt. Die Verarbeitung oder Nutzung personenbezogener Daten für Zwecke der Werbung ist zulässig, soweit der Betroffene eingewilligt hat. Sofern eine solche Einwilligung aber nicht vorliegt, ist darüber hinaus die Verarbeitung oder Nutzung personenbezogener Daten zulässig, soweit es sich um listenmäßig zusammengefasste Daten handelt. Der Umfang der Kundendaten, die der Erwerber aufgrund dieser Vorschrift erhalten darf, ist daher auf die sog. Listendaten beschränkt. Bei den Listendaten handelt es sich um Name, Titel, akademischer Grad, Berufs-, Branchen- oder Geschäftsbezeichnung, Anschrift und Geburtsjahr, soweit sich diese Daten auf die Zugehörigkeit zu einer bestimmten Personengruppe beziehen. Auf dieser Grundlage dürfen aber nur die „Listendaten“ übergeben werden. Zusätzliche Daten wie Telefonnummern, E-Mail-Adressen oder Bankverbindungsdaten sind davon nicht umfasst.
In der Regel ist eine saubere, den Vorschriften des BDSG entsprechende Übermittlung von über die Listendaten hinausgehenden Kundendaten im Zuge eines Unternehmensverkaufs nur im Wege einer Einwilligung möglich, die den Voraussetzungen des § 4a BDSG entspricht. Die vom TLfDI vertretene Auffassung berücksichtigt dabei, dass bei dem alternativen Lösungsvorschlag, also einer Widerspruchslösung, nach hiesiger Auffassung nicht mit der notwendigen Wahrscheinlichkeit davon ausgegangen werden kann, dass schutzwürdige Belange der Betroffenen nicht überwiegen. Denn eine Widerspruchslösung bedeutet, dass der Betroffene dem Übergang seiner Daten widersprechen muss, um einen solchen zu verhindern und setzt daher ein Handeln des Betroffenen voraus. Handelt dieser jedoch nicht, sei es durch Änderung der Adressdaten, sei es durch

vorübergehende Abwesenheit, wird sein Schweigen „zu seinen Lasten“ gewertet, was bei einem so hohen Schutzgut wie dem informationellen Selbstbestimmungsrecht aus Art. 2 Abs. 1 Grundgesetz (GG) i. V. m. Art. 1 Abs. 1 GG als nicht vertretbar erscheint. Denn das Schweigen ist keine Erklärung und ein Dulden ist auch keine Handlung.

Ein besonderes Problem bei der Übernahme von Unternehmen stellen Arztpraxen und Rechtsanwaltskanzleien dar, da hier zum einen besondere Arten von personenbezogenen Daten in Form von Gesundheitsdaten im Raum stehen und zum anderen auf die Besonderheiten von Berufsgeheimnisträgern Rücksicht zu nehmen ist, dass in solchen Fällen eine Strafbarkeit nach § 203 Strafgesetzbuch (StGB) im Raum steht.

Der BGH hat für die Übergabe einer Patientenkartei im Rahmen des Verkaufs einer Arztpraxis entschieden, dass die Weitergabe personenbezogener Daten in ärztlichen Behandlungsunterlagen, die grundsätzlich über intime Einzelheiten Aufschluss geben, zur Anwendung von § 203 Nr. 1 StGB führt (vgl. BGH in BGHZ 116, 268). Grundlage der Entscheidung BGHZ 116, 268 war die Bedeutung des Rechts des Einzelnen auf informationelle Selbstbestimmung und die daraus herzuleitende besondere Schutzbedürftigkeit personenbezogener Daten. Dies folgt sowohl – in Bezug auf Angehörige der Heilberufe sowie Rechtsanwälte – aus § 203 Nr. 1 StGB sowie ansonsten aus § 28 Abs. 2 BDSG. Unter Heranziehung dieser Wertungen des BGH in dem vergleichbar gelagerten Fall überwiegt das schutzwürdige Interesse der Betroffenen an dem Ausschluss der Nutzung – hier also der Ausschluss der Weitergabe ohne Einwilligung – das Interesse des Datenverwenders. Bereits eine Rechtfertigung der Weitergabe der Daten mit dem objektiven Eigeninteresse der betroffenen Patienten an einer guten Fortführung ihrer Behandlung durch den neuen Arzt vermag nicht eine freie Entscheidung des Patienten zur Datenweitergabe zu ersetzen.

Beim Praxisverkauf oder bei der Praxisübernahme ist daher zu beachten, dass der übernehmende Arzt nicht automatisch ein Zugriffsrecht auf die Patientendaten hat. Der Verkauf einer Praxis oder die Insolvenz stellt dabei keine Befugnis dar, die anvertrauten Geheimnisse einem anderen Arzt zu offenbaren. Für die Übernahme der Patientenakten muss es eine Einwilligungserklärung gem. § 4a BDSG aller Patienten geben. In der Praxis wird hier auf die sog. Zwei-Schränke-Methode zurückgegriffen. In einem Schrank werden

die Patientenakten des bisherigen Praxisinhabers aufbewahrt. Wenn der Patient nach der Praxisübernahme wieder zur Behandlung erscheint, wird er darüber aufgeklärt und er wird gefragt, ob er die Behandlung beim Praxiserwerber weiterführen möchte und dieser dazu in seine Patientenakte Einsicht nehmen darf. Wenn der Patient eine solche Einwilligung erteilt, dann wird die Akte im anderen Schrank, in dem des Erwerbers, abgelegt. Alle so gewanderten Akten stehen dann dem Erwerber als Patientenakten für seinen Praxisbetrieb zur Verfügung. Alle im ersten Schrank verbliebenen Akten bleiben dort und sind von dem Arzt, der die Praxis aufgibt, bis zum Ablauf der Aufbewahrungsfrist unter Verschluss zu halten.

Im Rahmen von Unternehmensveräußerungen oder Teilveräußerungen ist neben den wirtschaftlichen Aspekten auch stets auf die datenschutzkonforme Umsetzung dieser Veräußerungen zu achten. Auch im Hinblick auf eine wirtschaftliche und zeitnahe Lösung für die Unternehmen kann es im Hinblick auf die datenschutzrechtlichen Vorgaben nur eine Lösung geben: Die Übertragung von Kundendaten beim Unternehmenskauf ist grundsätzlich nur mittels einer Einwilligung gem. § 4a BDSG datenschutzkonform zu bewerkstelligen.

3.27 Datenschutz für Pseudonym?

Aufgrund der Beschwerde einer Mieterin erlangte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) Kenntnis über einen möglichen Datenschutzverstoß seitens der in dem Mehrfamilienhaus tätigen Hausverwaltung. Die Beschwerdeführerin teilte dem TLfDI mit, dass die Hausverwaltung statt des von ihr aus diversen Gründen verwendeten Pseudonyms ihren richtigen Namen auf der für alle Mieter zugänglichen Haus- und Putzordnung vermerkt sowie die Nebenkostenabrechnung ebenfalls unter ihrem richtigen Namen versendet hatte. Darüber hinaus gab es in dem Mietshaus einen außen liegenden Gemeinschaftsbriefkasten, zu dem jeder Mieter einen Schlüssel hatte. Die Post wurde seitens der Mieter in die im Hausflur befindlichen Briefkästen umverteilt. Dabei kamen diverse Briefe und Post bei der Beschwerdeführerin gar nicht oder geöffnet an. Der TLfDI ermittelte durch ein Auskunftsersuchen an die Hausverwaltung den Sachverhalt abschließend. Die Beschwerdeführerin teilte daraufhin mit, dass die Hausverwaltung zwischenzeitlich ihr Pseudonym nunmehr akzeptiert

habe und in der erforderlichen Weise verwenden würde. Die Beschwerde dahingehend hatte sich damit erledigt. Grundsätzlich gibt es keinen datenschutzrechtlichen Anspruch darauf, dass ein Vertragspartner statt des bürgerlichen Namens das von der betroffenen Person in der Öffentlichkeit benutzte Pseudonym verwendet. Eine solche Vereinbarung ist zivilrechtlich zwischen den Vertragspartnern zu vereinbaren, was im vorliegenden Fall nicht geschehen ist. Auch hinsichtlich der Problematik des Briefkastens und der geöffneten Briefe konnte kein datenschutzrechtlicher, sondern lediglich ein strafrechtlicher Verstoß gegen § 202 Strafgesetzbuch festgestellt werden, sodass das Verwaltungsverfahren gegen die Hausverwaltung beim TLfDI insgesamt abgeschlossen werden konnte.

Pseudonyme sind ebenfalls personenbezogene Daten i. S. d. § 3 Abs. 1 Bundesdatenschutzgesetz (BDSG). Hierüber ist eine Identifikation der betreffenden Person möglich. Diese sind daher auch vom Schutz des BDSG umfasst, welches nach § 1 Abs. 1 BDSG den einzelnen davor schützt, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird. Es gibt jedoch keinen datenschutzrechtlichen Anspruch des Betroffenen auf Verwendung dieses Pseudonyms. Hierfür ist eine zivilrechtliche Vereinbarung der einzelnen Vertragspartner erforderlich. Sofern bei der Verwendung dieses Pseudonyms Verstöße festgestellt werden, kann eine datenschutzrechtliche Überprüfung erfolgen.

3.28 Bürgerinitiative ratlos – der TLfDI kann helfen

Im Berichtszeitraum wandte sich eine Bürgerinitiative (BI) an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Sie bat um datenschutzrechtliche Unterstützung bezüglich einer Unterschriftensammlung für die Errichtung eines Bestattungswaldes. Das Vorhaben konnte nicht realisiert werden, da die zuständige Thüringen Forst – Anstalt öffentlichen Rechts (AöR) das dafür notwendige Areal nicht zur Verfügung gestellt hatte. Die Unterschriftensammlung sollte an das Aufsichtführende Ministerium übergeben werden. Ziel dieses Bürgervotums sei es, das Anliegen der Bürgerinitiative (BI) für die Errichtung eines solchen Friedhofes mit überregionaler Bedeutung zu stützen. Die BI sah sich in Bezug auf die Erhebung und Nutzung von personenbezogenen

Daten im Rahmen der Unterschriftensammlung als verantwortliche Stelle im Sinne des § 2 Abs. 4 Bundesdatenschutzgesetz (BDSG). Da dieses Vorhaben für die BI von großer Bedeutung war und es nicht gefährdet werden sollte, wurde der TLfDI um datenschutzrechtliche Überprüfung gebeten.
Der TLfDI erklärte, dass sie als BI und damit Zusammenschluss mehrerer Personen mit einem gemeinsamen Zweck als Gesellschaft bürgerlichen Rechts einzuordnen ist. Als (teil-)rechtsfähige Personengesellschaft unterfällt diese damit auch den Regelungen des BDSG, soweit sie mit personenbezogenen Daten umgehe.
Der TLfDI gab zwei Möglichkeiten für eine datenschutzkonforme Unterschriftensammlung und die anschließende Übermittlung an das zuständige Ministerium vor:
Zum einen gibt es den sogenannten Erlaubnistatbestand. Demnach ist die angestrebte Unterschriftenliste von § 28 Abs. 1 Satz 1 Nr. 2 BDSG erfasst. Danach ist die Datenerhebung und -übermittlung zulässig, soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zur Annahme besteht, dass schutzwürdige Interessen des Betroffenen an dem Ausschluss der Verarbeitung überwiegen.
Das Sammeln der Unterschriften ist für diese BI erforderlich. Ein Überwiegen der Interessen der Unterschreibenden an einem Ausschluss der Verarbeitung, insbesondere der Übermittlung an das zuständige Ministerium, ist nicht ersichtlich, wenn auf diese beabsichtigte Folge hingewiesen wird, § 4 Abs. 3 BDSG. Einen solchen Hinweis enthielt das Schreiben der BI. Nicht gedeckt von § 28 Abs. 1 Satz 1 Nr. 2 BDSG ist das Bekanntgeben (Übermitteln) von personenbezogenen Daten (andere Unterschriften) an einzelne, folgende Unterschreiber. Dies betrifft insbesondere die Information, wer noch auf der Liste unterschrieben hat. Daher ist die Liste auf geeignete Art und Weise abzudecken um eine (unbefugte) Übermittlung dieser Daten zu vermeiden. Der BI wurde geraten in ihrem Hinweis zu ergänzen, dass die Datenweitergabe ausschließlich an das zuständige Ministerium erfolgt.
Als zweite Möglichkeit wurde die Einwilligung erklärt. Nach § 4 Abs. 1 BDSG ist das Erheben, Verarbeiten oder Nutzen von personenbezogenen Daten verboten, es sei denn, eine Norm im BDSG oder eine andere Rechtsvorschrift erlaubt dies, ordnet dies an oder der/die Betroffene willigt in den Umgang mit seinen personenbezogenen Daten ein. Dies gilt auch, wenn private Stellen, zum Beispiel

Vereine, Unterschriften sammeln. Nach § 4a BDSG muss die Einwilligung auf der freien Entscheidung des Betroffenen beruhen. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Sollte eine Einwilligung zusammen mit anderen Einwilligungen schriftlich erteilt werden, ist sie besonders hervorzuheben. Wegen der speziellen, im Gesetz eindeutig geregelten Voraussetzungen einer wirksamen Einwilligung ist hier jedoch pro unterschreibender Person ein Blatt zu nutzen. Dies liegt darin begründet, dass die Einwilligungen nicht auf dem Umfrageblatt erfolgen können und so ausgeschlossen ist, dass der Unterschreibende Kenntnis von anderen Einwilligenden nehmen kann. Zunächst hat die Person dann die Einwilligung auf diesem Blatt zu unterschreiben. Die Einwilligung hat sich vom übrigen Text auf geeignete Weise abzugrenzen, wie etwa mittels eines umlaufenden Kastens. Die Unterschrift muss als diesem Textstück zugehörig geleistet werden.

Nach § 4 Abs. 1 BDSG ist das Erheben, Verarbeiten oder Nutzen von personenbezogenen Daten verboten, es sei denn, eine Norm im BDSG oder eine andere Rechtsvorschrift erlaubt dies, ordnet dies an oder der/die Betroffene willigt in den Umgang mit seinen personenbezogenen Daten ein. Dies gilt auch, wenn private Stellen, zum Beispiel Vereine, Unterschriften sammeln. Da die Unterschriften in einer Liste erfasst werden, sind die bisherigen Unterschriften abzudecken, wenn eine neue Person unterschreibt. Somit kann der Folgeunterschreiber keine Kenntnis der bisherigen Unterschreiber erlangen.

3.29 Aktenlager überall

Im Berichtszeitraum erreichte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) ein Hinweis über eine unsichere Aktenlagerung in einer Halle. Daraufhin wandte der TLfDI sich an das dortige Ordnungsamt mit der Bitte um Kontrolle des Gebäudes im Wege der Amtshilfe.
Gemäß § 9 Bundesdatenschutzgesetz (BDSG) hat die öffentliche oder nicht-öffentliche Stelle, die selbst oder im Auftrag personenbezogene Daten erhebt, verarbeitet oder nutzt, die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die

in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Zu den organisatorischen Maßnahmen zählt unter anderem, dass sichergestellt wird, dass nur die Zugriffsberechtigten Einsicht in die Akten haben.
Die während der Kontrolle aufgenommenen Fotos zeigten, dass sich mehrere Gitterboxen voll mit Akten in der Halle befanden. Das Gebäude selbst war nicht begehbar; alle Türen und Tore waren verschlossen sowie die Fensterscheiben intakt. Somit hatte kein Dritter Zugang zu den Altakten.
Zu ermitteln war nun, wem die Akten gehörten, wem die Halle gehörte und ob die Akten überhaupt noch aufbewahrt werden müssen (Aufbewahrungsfristen). Die Ermittlung der verantwortlichen Stelle, also des Besitzers der Akten gestaltete sich schwierig. Firmenübernahmen und Verkäufe der Halle verlangsamten den Prozess. Nach einem erneuten Verkauf der Halle wurde dem TLfDI mitgeteilt, dass die Akten vernichtet worden seien. Erneut wurde das Ordnungsamt um eine Kontrolle gebeten. Bei dieser stellte sich heraus, dass tatsächlich alle Akten ausgeräumt waren.

Bei Verlassen eines Firmengebäudes wegen Verkaufs, Geschäftsaufgabe, etc. dürfen keine Akten zurückgelassen werden. Die Akten müssen archiviert und bei Ablauf der Aufbewahrungsfrist datenschutzgerecht vernichtet werden. Hierbei sind die Anforderungen an die Sicherheitsstufen der Schredder im Hinblick auf die Schutzklasse der Akten nach der DIN 66399 zu beachten.

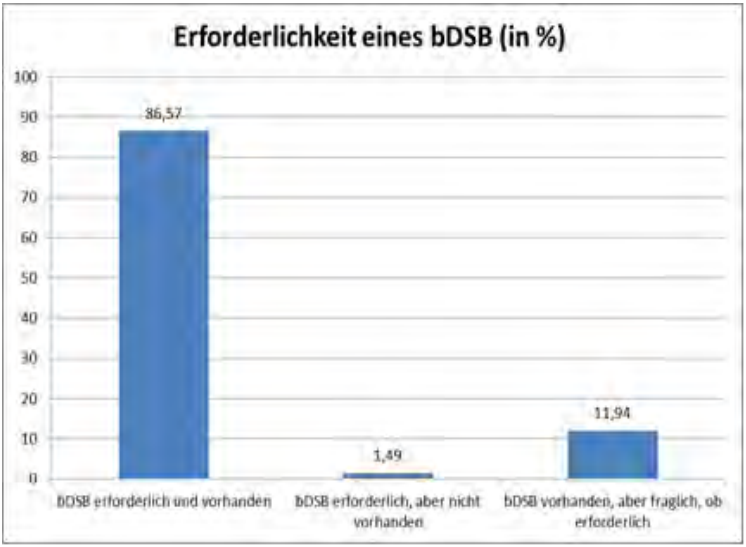
3.30 Umfrage des TLfDI – Thüringer Unternehmen zeigen sich hinsichtlich Datenschutzanforderungen höchst vorbildlich

Im Jahr 2016 führte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) eine Umfrage zum Thema „behördlicher Datenschutzbeauftragter“ i. V. m. „Datenübermittlung ins außereuropäische Ausland“ durch.
Hierbei wurden alle Thüringer Unternehmen mit mehr als 50 Beschäftigten angeschrieben. Mit der Umfrage hat sich der TLfDI einen Überblick über die Thüringer Datenschutzlandschaft in den abgefragten Bereichen verschafft.
Positiv hervorzuheben ist, dass 83 Prozent der Unternehmen sehr vorbildlich waren und ihrer Verpflichtung zur Antwort fristgemäß

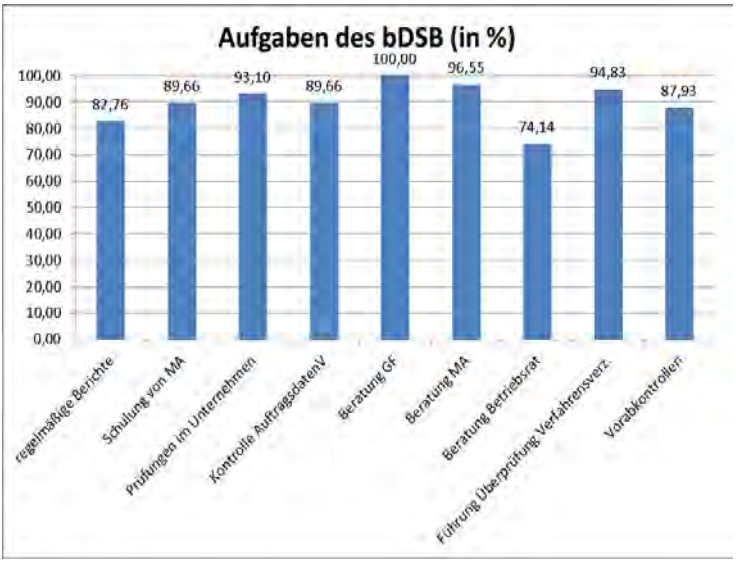
nachgekommen sind. Alle übrigen Unternehmen kamen der Aufforderung nach der ersten Erinnerung nach.



Der erste Teil des Fragebogens bezog sich auf die behördlichen Datenschutzbeauftragten (bDSB) und auf die Art und Weise, wie mit der Verarbeitung von personenbezogenen Daten umgegangen und verfahren wird. Nach dem Willen des Gesetzgebers haben bestimmte Unternehmen unter bestimmten Voraussetzungen einen solchen bDSB zu bestellen. Dieser muss wiederum bestimmten Kriterien entsprechen. Der TLfDI ist der Auffassung, dass der bDSB ein wichtiges Instrument für die Gewährleistung eines ausreichenden Datenschutzniveaus in Unternehmen ist, weswegen es auch besonders wichtig ist, dass die gesetzlichen Bestimmungen insoweit eingehalten werden. Die Umfrage hat ergeben, dass bei einer sehr deutlichen Mehrheit der Unternehmen ein bDSB erforderlich und vorhanden ist.



Positiv anzumerken ist hierbei, dass es bei 86 Prozent der Angeschriebenen nichts im Hinblick auf die Bestellpflicht eines bDSB zu bemängeln gibt. Auch in Bezug auf die Vereinbarkeit des bDSB mit dessen hauptberuflicher Tätigkeit im Unternehmen ist bei 97 Prozent der Unternehmen alles im grünen Bereich. Wer als bDSB bestellt ist und daneben noch andere Tätigkeiten im Unternehmen ausübt, darf nämlich keine Aufgaben wahrnehmen, die zu Interessenskonflikten bei der Tätigkeit als bDSB führen. Klassisches (Negativ-)Beispiel hierfür ist die Bestellung des IT-Leiters oder gar des Geschäftsführers als bDSB.

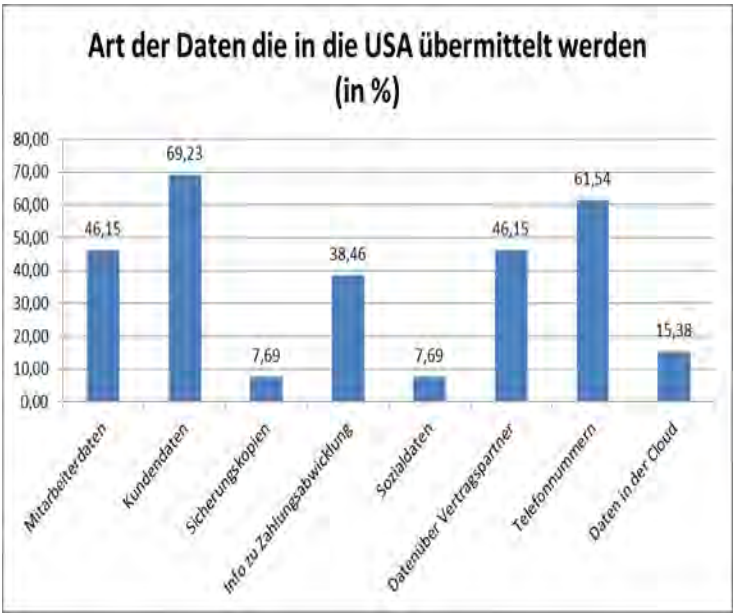


In der Grafik ist gut erkennbar, welche Aufgaben die behördlichen Datenschutzbeauftragten im Rahmen ihrer Tätigkeit erledigen.

Auch im Hinblick auf die Weiterbildung der bDSB in den Unternehmen gibt es seitens des TLfDI fast nichts zu meckern. Denn 86 Prozent der bDSB gehen regelmäßig zu Fortbildungen. Dies ist gerade zu dem jetzigen Zeitpunkt, also dem Ausklingen des Bundesdatenschutzgesetzes (BDSG) bis zum Mai 2018 und ab dann dem Gelten der DS-GVO, unverzichtbar.
Bis auf wenige Einzelfälle hat die Umfrage also ein positives Bild auf Thüringens größere Unternehmen geworfen. Sie sind in Sachen bDSB gut aufgestellt und wissen in der Regel auch, was ihre Pflichten sind.

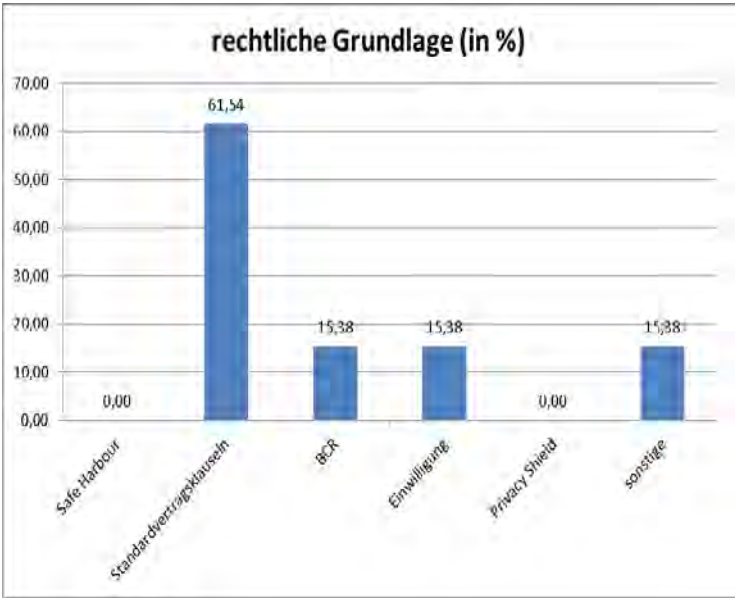
Der andere Bereich, den die Umfrage abprüfen sollte, war die Übermittlung von personenbezogenen Daten insbesondere in die USA. Hier ist nach Auswertung der Umfrage festzustellen, dass 2/3 der befragten Unternehmen nach eigenen Angaben überhaupt keine personenbezogenen Daten in die USA übermitteln. Etwa drei Prozent der Unternehmen machten hierzu keine Angaben, hier wird der TLfDI in Einzelfällen nochmals nachhaken. Das bedeutet

im Umkehrschluss, dass etwa 19 Prozent der Unternehmen diese sensiblen Daten in die USA übermitteln.
Übermittelt werden übrigens, wie sich der folgenden Grafik entnehmen lässt, vornehmlich Mitarbeiterdaten und Kundendaten.

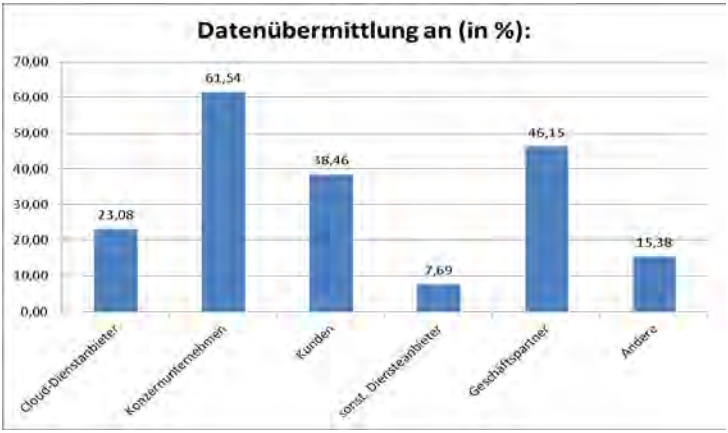


Anhand der Grafik lässt sich die Art der Daten gut erkennen. Nicht überraschend ist, dass Kundendaten, Daten über Vertragspartner und Mitarbeiterdaten weit vorne liegen.

Doch auf welcher rechtlichen Grundlage erfolgt dies? 61 Prozent rechtfertigen dies mit dem Hinweis auf Standardvertragsklauseln. Jeweils 15 Prozent berufen sich auf Einwilligungen, Binding Coporate Rules (BCR). Unter „Sonstige“ gaben die Unternehmen Vertragsklauseln und § 4c Abs. 1 BDSG an. Die Prüfungen hierzu hat der TLfDI noch nicht abgeschlossen.



Übermittelt werden die Daten übrigens an verschiedene Empfänger. In der folgenden Grafik ist das Ziel der Datenübermittlung gut erkennbar. Unter „Andere“ wurden US-Steuerbehörden, SWIFT und sonstige Diensteanbieter seitens der Unternehmen benannt.



Zusammenfassend für den Bereich „Datenübermittlung ins außereuropäische Ausland“ kann man sagen, dass es eher bei einem kleinen Kreis der Thüringer Unternehmen eine Rolle spielt. Es ist davon auszugehen, dass in kleineren Unternehmen noch weniger Daten in die USA übermittelt werden.

Inwieweit die Übermittlungen durch die einzelnen, befragten Unternehmen rechtmäßig sind, wird vom TLfDI geprüft werden.

Diese Umfrage war das erste Mal, dass der TLfDI sich dieses Instruments bedient hat, um sich einen breiten Überblick zu verschaffen, wie die Datenschutzlandschaft in Thüringen in bestimmten Bereichen ausgestaltet ist. Das Ergebnis war nach derzeitigem Kenntnisstand erfreulich. Den wenigen Einzelfällen, in denen die Antworten Fragen oder Stirnrunzeln bei den Prüfern hervorgerufen haben, wird in naher Zukunft nachgegangen werden. Es ist auch nicht auszuschließen, dass dieses Instrument erneut genutzt wird, um einzelne Sparten gezielt zu prüfen.

3.31 Weitergabe von Kundenverbrauchsdaten durch Versorgungsunternehmen

Im Berichtzeitraum wandte sich ein Versorgungsunternehmen an den Thüringischen Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Es erhielt von einer thüringischen Stadtverwaltung die Anfrage, Verbrauchsdaten von Kunden herauszugeben wegen des Verdachts auf dauerhaft illegale Wohnungsnutzungen. Dies geschah außerhalb eines offiziellen Ermittlungsverfahrens. Das Versorgungsunternehmen lehnte die Bitte um Auskunft ab und erbat sich vom TLfDI eine Bestätigung der Rechtsauffassung bzw. um eine Stellungnahme, falls diese abweichen sollte.
Messdaten, die mit Zählern ermittelt werden, sind auch personenbezogene Daten i. S. d. § 3 Abs. 1 Bundesdatenschutzgesetz (BDSG). Gemäß § 4 Abs. 1 BDSG ist die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.
Ursprünglich wurden die Messdaten für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen Schuldverhältnis-

ses mit dem Betroffenen erhoben und verarbeitet (§ 28 Abs. 1 Satz 1 Nr. 1 BDSG).
Für die Übermittlung der personenbezogenen Daten an die Stadtverwaltung käme sodann als Erlaubnisnorm § 28 Abs. 2 Nr. 2 BDSG infrage. Demnach ist eine Übermittlung von personenbezogenen Daten für einen anderen Zweck nur zulässig, soweit es zur Wahrung berechtigter Interessen eines Dritten (Buchstabe a) oder zur Abwehr von Gefahren für die staatliche oder öffentliche Sicherheit oder zur Verfolgung von Straftaten erforderlich ist (Buchstabe b) und kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung oder Nutzung hat. Das Versorgungsunternehmen rechtfertigte die Ablehnung mit folgenden Gründen:
Das illegale Bauen oder Nutzen von baulichen Anlagen stellt nach der Thüringer Bauordnung eine Ordnungswidrigkeit und keine Straftat dar. Der Gesetzgeber hat ausdrücklich davon abgesehen, Ordnungswidrigkeiten in den Katalog der zulässigen Zweckänderungen mit aufzunehmen. Somit ist § 28 Abs. 2 Nr. 2 Buchstabe b BDSG nicht einschlägig.
Zweifelsfrei ist die Ermittlung von illegalem Wohnungsbau und illegaler Wohnungsnutzung ein berechtigtes Interesse der Stadtverwaltung (Buchstabe a). Allerdings besteht durchaus ein Grund zur Annahme, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung oder Nutzung seiner Daten hat. Solch ein Interesse ist immer dann anzunehmen, wenn Daten übermittelt werden sollen, die sich auf strafbare Handlungen, Ordnungswidrigkeiten oder arbeitsrechtliche Verhältnisse beziehen.
Der TLfDI stimmt der Rechtsauffassung zu und führt ergänzend aus, dass eine Beurteilung, ob der Betroffene ein schutzwürdiges Interesse an dem Ausschuss der Übermittlung hat, immer am Einzelfall zu erfolgen hat. Die Angaben der Stadtverwaltung „um gegen illegale, dauerhafte Wohnnutzungen vorzugehen“ ist viel zu abstrakt, um eine Einzelfallprüfung vornehmen zu können. Ebenso wird von der Stadtverwaltung nicht konkret angegeben, welche Rechtsverstöße genau vorliegen.
Folglich wäre die Situation anders zu bewerten, wenn die Stadtverwaltung ein offizielles Verwaltungsverfahren einleitet und eindeutig darlegen kann, welche Rechtsverstöße gegeben sind und damit eine konkrete Gefahr für die öffentliche Sicherheit bestünde. Bei Gefahr für die öffentliche Sicherheit wird es nahezu unmöglich, die Verar-

beitung von Daten aufgrund von Interessen der Betroffenen abzulehnen.
Aber auch dann hat die Stadtverwaltung ihrerseits eine Ermächtigungsnorm zu nennen, die sie zur Erhebung der Daten berechtigt.

Die Datenerhebung und nachfolgende Verarbeitung hat immer zweckgebunden zu erfolgen (§ 28 Abs. 1 S. 2 BDSG). Eine zweckfremde Übermittlung oder Nutzung ohne Einverständnis des Betroffenen ist nur in engen Grenzen und nur soweit das Gesetz dies ausdrücklich regelt zulässig (siehe § 28 Abs. 2 BDSG).

3.32 Schrott sammeln = Daten sammeln? Fortsetzung II

Seit sechs Jahren beschäftigt sich der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) mit einem Fall der Anfertigung von Personalausweiskopien bei einem Metall-Recycling-Unternehmen.
Im 2. Tätigkeitsbericht des TLfDI zum Datenschutz: Nicht-öffentlicher Bereich endete der Beitrag damit, dass das Unternehmen Rechtsmittel einlegte (s. a. 2. TB TLfDI: Nicht-öffentlicher Bereich [2.27]).
Die fortwährende Diskussion drehte sich erneut um die Frage, in welchem Umfang das Schrottunternehmen Daten erheben darf. Nachdem das Erstellen von Personalausweiskopien nach Anordnung eingestellt wurde, ging das Unternehmen dazu über, ein Formblatt von den Lieferanten ausfüllen zu lassen. Hierin wurden folgende Daten abgefragt: Name, Vorname, Straße, PLZ/Ort, Geburtsdatum, Geburtsort, Staatsangehörigkeit, Personalausweisnummer, Gültigkeit des Personalausweises.
Gemäß § 4 BDSG ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.
Das Unternehmen trug vor, dass es, um seiner Benennungspflicht nach § 160 Abgabenordnung (AO) nachzukommen, notwendig sei, diese Daten zu erheben. Gemäß § 160 AO sind Schulden und andere Lasten, Betriebsausgaben, Werbungskosten und andere Ausgaben steuerlich regelmäßig nicht zu berücksichtigen, wenn der Steuerpflichtige dem Verlangen der Finanzbehörde nicht nachkommt, die Gläubiger oder die Empfänger genau zu benennen. Allerdings zählt

§ 143 AO abschließend auf, welche Daten von Unternehmen bei Wareneingängen aufgezeichnet werden müssen. Gefordert sind lediglich der Name oder die Firma und die Anschrift des Lieferers (§ 143 Abs. 3 Nr. 2 AO) sowie weitere Daten zur Lieferung an sich.
Daraufhin erwiderte das Unternehmen, dass während Betriebsprüfungen mehrfach von Finanzbehörden Kopien von Personalausweisen gefordert wurden. Jedoch besagt die ständige Rechtsprechung der Finanzgerichte und des Bundesfinanzgerichtshofs eindeutig, dass nach § 160 AO der Name und die Anschrift vollkommen ausreichend sind. Die Unternehmen sollen nicht aus Angst vor steuerrechtlichen Nachteilen durch Betriebsausgabenabzug vorbeugende Ermittlungsaufgaben für das Finanzamt wahrnehmen.
Auf die steuerrechtlichen Normen lässt sich eine Erhebung und Speicherung von Daten über den Namen oder die Firma und die Anschrift des Lieferers folglich nicht stützen.
Da sich das Unternehmen nicht überzeugen ließ, ordnete der TLfDI an, dass nur noch die Daten erhoben werden sollen, die der Gesetzgeber in der Abgabenordnung vorschreibt. Gegen diesen Anordnungsbescheid erhob das Unternehmen Klage beim zuständigen Verwaltungsgericht.
In der mündlichen Verhandlung wurden die Punkte nochmals problematisiert. Das Verwaltungsgericht wies die Klage des Unternehmens ab und bestätigte die Rechtsauffassung des TLfDI.

Unternehmen sind in bestimmten Fällen verpflichtet, gewisse Daten über ihre Kunden zu erheben, um Betriebsausgaben steuerrechtlich geltend zu machen. Dabei hat der Gesetzgeber vorgegeben, welche Daten dies sind. Darüber hinaus dürfen Unternehmen keine Daten erheben, da es hierfür keine Erlaubnisnorm gibt.

3.33 Handy als Navigator im Einkaufzentrum – beim TLfDI läuten die Alarmglocken

Im Berichtszeitraum erlangte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) aus der Presse Kenntnis darüber, dass an einem Pilotprojekt gearbeitet wird. In einem Einkaufszentrum solle das Handy den Kunden durch das Zentrum führen. Das Smartphone solle zudem – jeweils vor dem entsprechenden Schaufenster – auf besondere Aktionen hinweisen. In diesem Presseartikel wurde erklärt, dass man um die neuen Tech-

nologien wüsste und man im Handel nicht auf der Stelle treten dürfe, wenn man vorne mit dabei sein wolle. Man wolle die richtige Information zum richtigen Zeitpunkt „an den Mann“ bringen. Mit entsprechenden Minisendern im gesamten Einkaufszentrum soll es möglich werden, den Standort der Kunden zu „ermitteln“ und somit eine mögliche Navigation zu ermöglichen. Die Kunden könnten durch eine entsprechende App selbst entscheiden, ob sie diesen Service nutzen möchten und sich somit durch das Center leiten lassen. Aber damit nicht genug. Weiterhin soll auch das Umfeld mit eingebunden werden. Von der Parkplatzsuche bis zum Nahverkehr.
Beim Datenschutz klingelten daraufhin alle Alarmglocken. Also wandte man sich an das Management des Centers. Man wollte im Vorfeld die datenschutzrechtlichen Auswirkungen des geplanten Systems mit dem Management besprechen. Im Zuge dessen wurden alle technischen Details – sofern schon bekannt – zum künftigen System erfragt.
Das Management erklärte daraufhin, dass derzeit eine App entwickelt wird, die die Kunden über Neuigkeiten und Ereignisse im Einkaufszentrum informieren soll. Zudem bietet die App eine Reihe von ortsbasierten Diensten an. Hierzu zählen die Positionsbestimmung des Kunden im Einkaufszentrum und die Navigation zu einem gewünschten Ziel. Damit wird dem Kunden des Centers eine bessere Orientierung ermöglicht. Um die Funktion der App zu optimieren, muss der Nutzer sein Geschlecht und sein Alter angeben. Bezüglich der Einwilligung zur Nutzung der Daten gemäß § 4a Bundesdatenschutzgesetz muss jeder Nutzer beim Installieren der App die Datenschutzbestimmungen akzeptieren.
Der TLfDI wandte sich erneut an das Management des Centers, um noch mehr Details zur technischen Ausstattung der App in Erfahrung zu bringen.
Der Fall befindet sich derzeit noch in Bearbeitung. Ob diese App und die damit verbundene Verwendung im Sinne des Datenschutzes sind, bleibt abzuwarten. Der TLfDI bleibt jedenfalls dran.

Die Zuständigkeit des TLfDI beschränkt sich nicht nur auf bereits stattfindende Datenverarbeitung. Vielmehr kann er bereits im Vorfeld beratend tätig sein oder bei sich abzeichnenden schweren Verstößen gegen das Datenschutzrecht auch schon dann tätig werden, wenn es noch nicht zu einer Rechtsverletzung gekommen ist.

3.34 Öffentlich zugänglich aufgestellte Container mit Akten eines Steuerbüros in Gera

Im Berichtszeitraum wurde dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) von einer Thüringer Landespolizeiinspektion (LPI) mitgeteilt, dass zwei Datentonnen mit der Beschriftung „Datenträger zu vernichten“ frei zugänglich im öffentlichen Raum stehen würden. Dies wurde der Polizei durch einen aufmerksamen Bürger mitgeteilt. Die eingeleiteten Ermittlungen der Polizei bestätigten diesen Zustand. Bei einem Container war es ohne Umstände möglich, an entsprechende Akten zu gelangen. Die Polizeibeamten stellten fest, dass zumindest einer der beiden Behälter möglicherweise bauliche Mängel aufweist, welche eine Entnahme von Dokumenten aus dem Behälter ermöglichen würde. Die Container konnten einem Steuerbüro zugeordnet werden. Die Verantwortlichen wurden hinzugezogen und das sichere Verwahren der Akten wurde überwacht.
Der Bürger teilte wenige Stunden später der Polizei erneut mit, dass nun Teile des Inhaltes der besagten Tonnen für jedermann zugänglich im öffentlichen Raum aufgefunden worden sein sollen. Wie und wann diese Unterlagen aus den Behältern in die Öffentlichkeit gelangen konnten, konnte durch die Beamten vor Ort nicht festgestellt werden. Die an die Polizeibeamten übergebenen Dokumente wurden sichergestellt. Die Polizei bat den TLfDI um datenschutzrechtliche Prüfung.
Der TLfDI wandte sich daraufhin an das Unternehmen und forderte die Übersendung der Unterlagen zu allen technischen und organisatorischen Maßnahmen, die zur Gewährleistung der Regelungen des Bundesdatenschutzes (BDSG) in diesem Unternehmen getroffen wurden. Insbesondere wollte der TLfDI wissen, wie der Umgang mit zu vernichtenden Unterlagen geregelt wurde.
Das Unternehmen teilte dem TLfDI mit, dass die sensiblen Daten von einem beauftragten Unternehmen vernichtet werden sollten. Es wurden dafür vorgesehene Container bestellt. Die Behälter wurden mit Dokumenten gefüllt, ordnungsgemäß verschlossen und zur vereinbarten Abholung bereitgestellt. Das Entsorgungsunternehmen hatte die Container jedoch nicht wie vereinbart abgeholt. Über die Presse erfuhr dann das Unternehmen, dass aus den verschlossenen Containern Dokumente entwendet wurden.

Das Unternehmen konnte keinen Verstoß gegen die Anforderungen des Datenschutzes nach Bundesdatenschutzgesetz erkennen. Vielmehr träfe die Verantwortung wohl das Unternehmen, das mit der Vernichtung der Unterlagen beauftragt war und diese nicht abgeholt hatte.
Der TLfDI teilte dem Unternehmen mit, dass es selbst verantwortliche Stelle nach § 3 Abs. 7 BDSG bleibt, auch wenn es personenbezogene Daten durch andere im Auftrag verarbeiten lässt. Dies gilt auch für den Fall von Datenvernichtung. Von einer solchen verantwortlichen nicht-öffentliche Stelle sind technische und organisatorische Maßnahmen vorzunehmen, die erforderlich sind, um die Ausführung der Vorschriften des Bundesdatenschutzgesetzes zu gewährleisten. Hierzu zählt ausdrücklich die Gewährleistung nach Ziffer 3 zweiter Halbsatz der Anlage zu § 9 Satz 1 BDSG, dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle). Durch die Lagerung von personenbezogenen Daten in den Datensicherheitsbehältern im öffentlichen Raum kam es zur Kenntnisnahme dieser personenbezogenen Daten durch Dritte und letztendlich zur Beschlagnahme durch die Polizeibehörde. Im Ergebnis waren die getroffenen technisch organisatorischen Maßnahmen daher nicht ausreichend.
Ein Steuerberater unterliegt nach § 203 Absatz 1 Strafgesetzbuch (StGB) einem besonderen Berufsgeheimnis. Das bedeutet, wer unbefugt das Privatgeheimnis verletzt, wie beispielsweise durch die Offenbarung eines fremden Geheimnisses, eines namentlich zum persönlichen Lebensbereich gehörenden Geheimnisses oder eines Betriebsgeheimnisses seiner Mandanten, kann mit einer Freiheitsstrafe bis zu einem Jahr oder einer Geldstrafe bestraft werden. Eine solche Verletzung würde dann vorliegen, sobald ein Dritter – in diesem Fall der mit der Vernichtung der Akten beauftragte Mitarbeiter des Vernichtungsunternehmens – Kenntnis vom Inhalt der Akten erlangen würde. Dies wäre zweifelsfrei beim Herausnehmen der Akten aus den Behältern der Fall.
Die Vernichtung oder sonstige Verarbeitung von personenbezogenen Daten, die einem besonderen Berufsgeheimnis unterfallen, kann rechtlich einwandfrei nur dann durch Beauftragung eines Drittunternehmens realisiert werden, wenn eine Kenntnisnahme des Akteninhalts durch das Drittunternehmen zu 100 Prozent ausgeschlossen ist. Dies liegt darin begründet, dass mit der Übergabe der Daten an ein

Drittunternehmen regelmäßig der objektive Straftatbestand des § 203 StGB erfüllt ist. Damit ist der in solchen Fällen zur Auftragsdatenverarbeitung zu schließende und zwingend vorausgesetzte Vertrag über die Auftragsdatenverarbeitung gemäß § 11 BDSG nach § 134 Bürgerliches Gesetzbuch wegen eines bestehenden gesetzlichen Verbotes nichtig. Ohne einen solchen Vertrag über die Auftragsdatenverarbeitung ist eine Vernichtung der betreffenden Daten aber rechtlich nicht in zulässiger Art und Weise realisierbar.
Nach Kenntnis des TLfDI ist derzeit ein Gesetzgebungsverfahren im Gange, dass auf eine Änderung des § 203 StGB abzielt. Damit sollen auch Berufsgeheimnisträger in die Lage versetzt werden, Dritte als Auftragsdatenverarbeiter einzusetzen.
Das Steuerbüro teilte dem TLfDI daraufhin mit, dass es nunmehr alle zu vernichtenden Unterlagen vor Ort mittels eines Büroschredders vernichten würde. Dieser entspricht der Sicherheitsstufe 4 nach DIN 32757-1. Das geschredderte Material weist demnach eine Materialteilchenfläche kleiner/gleich 30 Quadratmillimeter auf.
Da damit sichergestellt wurde, dass eine Kenntnisnahme durch Dritte ausgeschlossen ist, war eine weitere Tätigkeit des TLfDI nicht erforderlich.

Ein Steuerberater unterliegt nach § 203 Absatz 1 Strafgesetzbuch einem besonderen Berufsgeheimnis. Die Vernichtung oder sonstige Verarbeitung von personenbezogenen Daten ist besonders zu beachten. Der Steuerberater ist bis zur letztlichen Unkenntlichmachung seiner zur Vernichtung abgegebenen Akten verantwortlich. Er hat dafür Sorge zu tragen, dass niemand Kenntnis vom Inhalt der Akten erhält. Dies ist beim Abgeben der Akten in den Datencontainern schwer zu kontrollieren. Der entsprechende Mitarbeiter des Aktenvernichtungsunternehmens könnte Kenntnis vom Inhalt der Akten erlangen. Dies kann verhindert werden, indem die Akten vor Entsorgung geschreddert werden.

3.35 Onlineshops: Kreditkartendaten frei Haus?

Der Bayerische Landesbeauftragte für den Datenschutz und die Informationsfreiheit (BayLfDI) informierte seine Länderkollegen, darunter auch den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), über eine Medienmeldung, wonach zahlreiche Onlineshops (Internethandel) mit Kredit-

karten-Skimmern „verseucht“ sind. Sicherheitslücken bei Onlineshop-Betreibern würden ausgenutzt, um Skimming-Wanzen zu implementieren und damit Kreditkartendaten abzugreifen. Dem BayLfDI lag eine Liste vor, wieviele und welche Onlineshops in den Bundesländern von den Angriffen betroffen waren.
Der TLfDI bat den BayLfDI um Information, ob und welche Onlineshops in Thüringen betroffen sind. Die vom BayLfDI übersandten Informationen ergaben, dass in Thüringen lediglich ein Onlineshop von den Hackerangriffen und der Ausspähung von Kreditkartendaten betroffen war.
Nach § 42 Abs. 1 i. V. m. § 38 Abs. 6 Bundesdatenschutzgesetz (BDSG) ist der TLfDI datenschutzrechtlich die zuständige Aufsichtsbehörde i. S. d. § 38 Abs. 1 BDSG für Unternehmen. Im Rahmen seiner Aufsicht überwacht der TLfDI die Einhaltung des BDSG und anderer datenschutzrechtlicher Vorschriften bei nicht-öffentlichen Stellen in Thüringen und somit auch Privatunternehmen. Daher wandte sich der TLfDI schriftlich an den Betreiber des betroffenen Thüringer Onlineshops und informierte ihn darüber, dass in einem Artikel des Online-Magazins heise.de (https://www.heise.de/newsticker/meldung/Ueber-1000-deutsche-Online-Shops-infiziert-und-angezapft-3592281.html) vom 10. Januar 2017 von potenziellenen Sicherheitslücken bei Online-Shops berichtet wird, die von Cyber-Kriminellen ausgenutzt werden könnten. Diesbezüglich verwies der TLfDI auf die veröffentlichte Liste der betroffenen Shops (https://gitlab.com/gwillem/public-snippets/snippets/28813/raw), die auch die betriebenen Domains des Thüringer Internethandels enthielt.

Der TLfDI wies den Unternehmer darauf hin, dass auf seinen betriebenen Domains eine Shop-Software in einer nicht-ausreichend gesicherten Version eingesetzt wird und die vorhandenen Sicherheitslücken von Cyberkriminellen bereits ausgenutzt werden. Eine Prüfung durch den TLfDI hatte ergeben, dass auch sein Internethandel mit Schadsoftware infiziert war, die Kreditkartendaten an Kriminelle übermittelt. Details, welches Skript diese Übermittlung ausführt, waren jedoch nicht bekannt.



Der TLfDI empfahl dem Betreiber des Onlineshops, sofort die Shop-Software im aktuellen Status zu sichern, um Beweise gegenüber Dritten zwecks Schadensersatz zu bewahren. Der TLfDI wies den Unternehmer auf eine Internetseite hin, die eine detaillierte Anleitung zur Lösung des Problems enthielt, https://support.hypernode.com/knowledgebase/how-to-fix-credit-card-hijack/ und auf die Seite https://www.magereport.com.
Auf dieser Seite konnte der Unternehmer den aktuellen Sicherheitsstatus seines Shops nachprüfen.
Abschließend forderte der TLfDI den Onlineshop-Betreiber auf, den Schadcode zu entziffern und zu entfernen, sofern dies nicht möglich sein sollte, müsste die Shop-Software neu installiert werden. Im Hinblick darauf bat der TLfDI den Shop-Betreiber um eine Mitteilung, welche Maßnahmen er getroffen hatte und um die Übersendung einer gepackten Sicherheitskopie der Shop-Software (nur die PHP-Skripte, HTML-Code und Javaskripte – ohne Datenbanken und Zugangsdaten).



Der Betreiber des Internethandels teilte dem TLfDI daraufhin schriftlich mit, dass in seinem Onlineshop keine Kreditkartendaten erhoben werden und erhoben wurden; als einzige Zahlungsart biete er Vorkasse mit Überweisung an. Somit hatte der Betreiber nach eigener Darlegung nie Zahlungsdaten von Kunden erhoben oder gespeichert, die hätten ausgespäht werden können. Dem Kunden wurden lediglich die Bankdaten des Betreibers mitgeteilt. Somit fand die Zahlung an seine Bank durch den Kunden außerhalb des Shop-Systems statt.
Weiterhin informierte der Unternehmer den TLfDI darüber, dass er sich aufgrund der Hacker-Angriffe dennoch entschieden hatte, zukünftig ein alternatives Shop-System zu verwenden und dies bereits angelegt hatte.
Mit der Umstellung auf ein anderes Shop-System erklärte der TLfDI gegenüber dem Onlineshop-Betreiber die datenschutzrechtliche Erledigung des Vorgangs.

Nach § 42 Abs. 1 i. V. m. § 38 Abs. 6 Bundesdatenschutzgesetz (BDSG) ist der TLfDI datenschutzrechtlich die zuständige Aufsichtsbehörde i. S. d. § 38 Abs. 1 BDSG für nicht-öffentliche Stellen und somit auch Privatunternehmen. Der TLfDI kann gegenüber Privatunternehmen technische Maßnahmen anordnen, um die Einhaltung datenschutzrechtlicher Bestimmungen zu gewährleisten.

3.36 Datenschutz auch beim Schornsteinfeger

Im Berichtszeitraum erreichte den Thüringer Beauftragten für den Datenschutz und die Informationsfreiheit die Beschwerde eines Schornsteinfegermeisters. Er meldete, dass der Geselle des ehemaligen für den Kehrbezirk zuständigen Schornsteinfegers, der sich mittlerweile zur Ruhe gesetzt hatte, ein Rundschreiben zur Kundengewinnung an ehemalige Kunden verschickte. Diesem Anschreiben war ein Flyer beigelegt, der die Serviceleistungen des Unternehmens des Gesellen beschreibt sowie eine vorbereitete personalisierte Vertragsausfertigung für die Kunden zur sofortigen Unterschrift und zur Beauftragung mit den Schornsteinfegerarbeiten an deren Liegenschaften.
Der Beschwerdeführer äußerte den Verdacht, dass der Geselle die Daten aus dem Bestand des Schornsteinfegers, für den er tätig gewesen ist, übernommen hätte.
Nach § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG) ist die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Der TLfDI wandte sich mit einem Auskunftsersuchen an den Gesellen und bat um Stellungnahme. Dieser antwortete, dass er durch seine jahrelange Tätigkeit, als Geselle im Betrieb des Schornsteinfegermeisters Kenntnis von den Daten erlangt hatte. Zudem hatte er handschriftliche Karteikarteien geführt, auf denen die Kundendaten notiert wurden: die Anschrift, die Termine, die Art der Feuerstätten und die erledigten Aufgaben. Mithilfe dieser Karteikarten, war es ihm möglich, die Anschreiben an die Kunden zu fertigen und die Werbung für sein Unternehmen zu versenden. Von den Kunden wurden vorab allerdings keine schriftlichen Einwilligungserklärungen zur werblichen Nutzung ihrer Daten eingeholt.

Der TLfDI prüft derzeit, inwieweit eine Rechtsgrundlage zur Nutzung der Daten bestanden haben könnte. Über den Ausgang der Prüfung wird der TLfDI im nächsten Tätigkeitsbericht informieren.

Nach § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG) ist die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.

3.37 Datenübermittlung von Makler zu Makler – Der TLfDI bezieht Stellung!

Im Berichtszeitraum erreichte ein Schreiben eines Versicherungsunternehmens einige Datenschutzbeauftragte des Bundes und der Länder. Das Versicherungsunternehmen bat um Information darüber, wie eine Bestandsübertragung eines Versicherungsmaklers bei z. B. Tod, Insolvenz, Geschäftsaufgabe oder Verkauf an einen anderen Versicherungsmakler im Einklang mit dem Bundesdatenschutzgesetz (BDSG) erfolgen kann.
Der TLfDI vertritt hierzu folgende Auffassung:
Beim Übergang eines Maklergeschäfts von der gekauften Gesellschaft auf die übernehmende Gesellschaft und bei der damit verbundenen Übertragung der Kundendaten ist zunächst die Art der Daten, die übertragen werden sollen, von Bedeutung und ob diese Daten ggf. als ganzer Datensatz oder auch als Teile von Kundendatensätzen übertragen werden können.
Für die Übertragung der Datensätze ist § 28 Abs. 2 Nr. 1 Bundesdatenschutzgesetz (BDSG) i. V. m. § 28 Abs. 1 S. 1 Nr. 2 BDSG für das abgebende Unternehmen und § 28 Abs. 1 S. 1 Nr. 2 BDSG für das übernehmende Unternehmen als einschlägige Rechtsgrundlage anzusehen, soweit keine Gesundheitsdaten betroffen sind.
In die Interessenabwägung zwischen dem berechtigten Interesse der verantwortlichen Stelle, also dem Versicherungsunternehmen, und dem schutzwürdigen Interesse der Betroffenen ist allerdings nach Auffassung des TLfDI folgendes mit einzubeziehen: Die Betroffenen dürfen keinem Kontrahierungszwang ausgesetzt werden. Die Beauftragung eines Versicherungsmaklers liegt im Ermessen des Betroffenen. Auch steht es ihm gewöhnlich frei, sich diesen auszusuchen. Der Betroffene ist nicht gehalten, mit einem bestimmten Makler eine vertragliche Beziehung einzugehen. Der Betroffene kann auch jeder-

zeit ohne Makler mit dem Versicherungsunternehmen seiner Wahl einen Versicherungsvertrag abschließen. Der Weg über den Makler mag zwar für den Kunden bequemer sein, ist aber nicht notwendig. Es liegt daher nicht ohne weiteres auch im Interesse des Betroffenen, dass er die Daten, die er einem Makler anvertraut hat, einem anderen, für ihn unbekannten Makler zur Verfügung stellen will. Das schutzwürdige Interesse des Betroffenen geht zweifelsfrei dahin, dass seine wirtschaftlichen, sozialen und beruflichen Daten nicht unnötig offen gelegt werden. Insoweit wird es als notwendig angesehen, dieser Interessenlage im Besonderen gerecht zu werden. Daher müssen die schutzwürdigen Interessen der Betroffenen durch die Einräumung eines Widerspruchsrechts und einer angemessenen Widerspruchsfrist, die auch längere Urlaube berücksichtigt, gewahrt werden.

Das Widerspruchsrecht muss allerdings auch bestimmten Anforderungen genügen. Es ist ähnlich wie bei der Einwilligung notwendig, dass dem Betroffenen mitgeteilt wird, an wen, wann und zu welchem Zweck welche Daten übertragen werden sollen. Es ist ihm gleichwohl mitzuteilen, dass sein Vertrag auch ohne die Inanspruchnahme eines neuen Maklers weiterbesteht, da nur so dem Eindruck von Zwang entgegengesteuert werden kann. Erst nach dem Fristablauf können dann ggf. die Übertragungen der Daten, gestützt auf § 28 Abs. 2 Nr. 1 BDSG, vorgenommen werden.

Als Problem bei dieser Art der Wegbereitung für die Anwendung von § 28 Abs. 2 Nr. 1 BDSG für die Übermittlung von Kundendaten wird allerdings im Bereich der Versicherungen gesehen, dass es eine Vielzahl von Betroffenen gibt, die sich lediglich für den Vertragsabschluss eines Maklers bedient haben, diesen aber sonst nie wieder bemüht haben. Insoweit ist fraglich, ob ein Schreiben mit der Aufforderung zum Widerspruch z. B. mangels aktueller Zustelladresse die schutzwürdigen Interessen des Betroffenen in ausreichendem Maße wahren kann, da hier die Einräumung des Widerspruchsrechts wohl ins Leere geht.

Für den Bereich der Übermittlung von Gesundheitsdaten ist auf jeden Fall eine explizite Einwilligung der Betroffenen erforderlich. Diese Einwilligung ist an die Voraussetzungen des § 4a BDSG geknüpft. Hierin heißt es, dass eine Einwilligung nur dann wirksam ist, wenn diese auf einer freien Entscheidung des Betroffenen beruht. Diese Einwilligung bedarf der Schriftform. Der Betroffene ist auf eventuelle Folgen bei einer nicht erfolgten Einwilligung hinzuwei-

sen. Sollte es sich gemäß § 4a Absatz 3 BDSG i. V. m. § 3 Absatz 9 BDSG um eine besondere Art der personenbezogenen Daten handeln, wie beispielsweise Gesundheitsdaten, muss sich die Einwilligung darüber hinaus ausdrücklich auf diese Daten beziehen.

Oftmals werden Kundendaten bei Unternehmensverkäufen freigiebig mitverkauft oder stillschweigend im Unternehmen belassen. Dieses Vorgehen ist datenschutzrechtlich oftmals mit schwerwiegenden datenschutzrechtlichen Verstößen verbunden, die auch vom TLfDI in Thüringen verfolgt und geahndet werden. Es lohnt daher vorher ein Blick ins Gesetz, um die notwendigen Voraussetzungen für die Weitergabe der Daten zu schaffen. Oder ein Anruf beim TLfDI ☺

3.38 Digitale Unterschriften versus Datenschutz

Im Berichtzeitraum erreichte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) die Presseanfrage eines Onlineportals. Der TLfDI wurde gebeten, eine Stellungnahme zur Rechtmäßigkeit von digitalen Unterschriften in Versicherungsverträgen abzugeben. Anbei wurde ein Fragenkatalog zur Beantwortung geschickt. Es stellte sich heraus, dass mehrere Landesaufsichtsbehörden diese Anfrage erhielten. Daraufhin einigte man sich auf eine gemeinsame, abgestimmte Positionierung im Rahmen der ständigen Arbeitsgruppe für Versicherungswirtschaft.
Grundsätzlich ist die Wirksamkeit von Verträgen eine zivilrechtliche Fragestellung. Erst bei Verträgen, die auch die Verarbeitung von personenbezogenen Daten regeln, gilt es die Normen des Bundesdatenschutzgesetzes (BDSG) zu beachten. Eine Einwilligung zur Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten muss gem. § 4a BDSG in Schriftform erfolgen, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Die hier genannte Schriftform entspricht den Vorgaben des § 126 Bürgerliches Gesetzbuch.
Eine digitale Unterschrift, die auf einem Unterschriften-Pad mittels Touch-Eingabe gezeichnet wird, ist keine schriftliche Erklärung in dem Sinne. Es fehlt dem Touch-Display an der Fähigkeit, Schriftzeichen dauerhaft festzuhalten. Zu beachten ist auch, dass ein besonderer Umstand i. S. d. § 4a Abs. 1 BDSG nicht schon vorliegt, weil es bequemer ist, eine Unterschrift digital zu verwalten oder beide Parteien im Einvernehmen auf die zivilrechtliche Schriftform verzich-

ten. Ebenso stellt die Unterschrift auf dem Unterschriften-Pad keine qualifizierte elektronische Signatur im Sinne des Signaturgesetzes dar. Die qualifizierte elektronische Signatur ist ein algorithmisches Verfahren, das einen Buchstaben- und Zahlencode mit dem zu signierenden Dokument verbindet. Nur dieses Verfahren kann eine eigenhändige Unterschrift ersetzen.
Außerdem müssen Versicherer den Vorschriften des Versicherungsvertragsgesetzes nachkommen. Auch hier wird an zahlreichen Stellen eine schriftliche Erklärung verlangt.
Jedenfalls ist datenschutzrechtlich immer darauf zu achten, dass bei jeder Datenverarbeitung ein legitimer Zweck verfolgt wird. Für diesen Zweck muss eine Rechtsgrundlage oder die Einwilligung des Betroffenen vorliegen. Auch müssen die personenbezogenen Daten der Versicherten in technischer sowie organisatorischer Hinsicht vor dem Zugriff durch Unbefugte (z. B. andere Sachbearbeiter der Organisation) geschützt werden. Hierbei sind die Vorgaben des § 9 BDSG, welcher die Festlegung von technischen und organisatorischen Maßnahmen regelt, einschließlich der Anlage 1 zu § 9 BDSG zu beachten.

Die Gültigkeit eines Vertrages und die Bindungswirkung der verschiedenen Formvorgaben ist eine zivilrechtliche Fragestellung. Erst wenn Verträge auch die Verarbeitung von personenbezogenen Daten regeln, sind die datenschutzrechtlichen Vorgaben zu beachten (§§ 4, 4a BDSG). Für die Erhebung, die weitere Verarbeitung und Nutzung der personenbezogenen Daten hat die verantwortliche Stelle die erforderlichen technischen und organisatorischen Maßnahmen zu treffen, um die Daten vor dem Zugriff von Dritten zu schützen (siehe § 9 BDSG samt Anlage).

3.39 Schreddern? – Aber richtig?

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichte eine Anfrage eines Thüringer Vereins hinsichtlich der gesetzlichen Vorgaben für die Aufbewahrung und Vernichtung von Akten mit personenbezogenen Daten und besonderen Arten von personenbezogenen Daten, z. B. Daten zur ethnischen Herkunft, zu politischen Meinungen, zu religiösen Überzeugungen, zur Gewerkschaftszugehörigkeit und zu Gesundheitsdaten. Zunächst unterliegt auch die Vernichtung der Akten dem Bun-

desdatenschutzgesetz (BDSG), da die Vernichtung eine Form der Datenverarbeitung ist, nämlich eine Datenlöschung, § 3 Abs. 4 Nr. 5 BDSG.
Dem Verein wurde auf seine Anfrage hin mitgeteilt, dass die Aufbewahrung von derart sensiblen Daten in Aktenform oder in Form von elektronisch gesicherten Daten auf einem Speichermedium grundsätzlich in einem verschließbaren Behälter stattfinden muss. Hierzu ist grundsätzlich auch ein Tresor geeignet. Zu diesem dürfen dann aber auch nur solche Personen Zugang haben, die die Berechtigung zum Umgang mit den Akten haben. Andere Personen sind vom Zugriff auszuschließen.
In Sachen Aktenvernichtung wurde dem Verein mitgeteilt, dass es im Rahmen der Vernichtung von Datenträgern wichtig ist, dass die DIN 66399-1 „Büro- und Datentechnik – Vernichtung von Datenträgern“ Berücksichtigung findet. Sie beschreibt die Anforderungen an Maschinen und Einrichtungen zur Vernichtung von Informationsträgern. Je nach dem Grad der Schutzbedürftigkeit der auf dem Datenträger oder in der Akte gespeicherten Informationen werden fünf Sicherheitsstufen definiert. Die Stufe P-3 ist dabei nur als eine Mindestanforderung für die datenschutzgerechte Vernichtung anzusehen. Für sensible personenbezogene Daten ist aber aus Sicht des TLfDI (und weiterer zehn deutscher Datenschutzbehörden) mindestens die Sicherheitsstufe P-5 erforderlich. Der Schredder, der dieser Sicherheitsstufe entspricht, zerteilt das Material in eine Teilchengröße kleiner/gleich 30 qmm. Bei dieser Sicherheitsstufe ist von einer datenschutzkonformen Vernichtung durch die verantwortliche Stelle auszugehen.
Soll die Vernichtung nicht durch die verantwortliche Stelle selbst, sondern durch einen externen Dienstleister erfolgen, muss im Rahmen der Beauftragung zur Vernichtung der Akten an den Abschluss eines Auftragsdatenverarbeitungs-Vertrages (ADV-Vertrages) gemäß § 11 Abs. 2 BDSG gedacht werden, da dieser zwingend notwendig ist. Die Vernichtung der Akten stellt eine Verarbeitung im Auftrag durch andere dar. Dieser Vertrag ist schriftlich abzufassen und muss die notwendigen Angaben enthalten, welche sich aus § 11 Abs. 2 Nr. 1-10 BDSG ergeben.
Zu beachten ist allerdings, dass gem. § 1 Abs. 3 S. 2 BDSG die Verpflichtung zur Wahrung gesetzlich vorgesehener Geheimhaltungspflichten oder von besonderen Berufs- und Amtsgeheimnissen bestehen bleibt. Diese Pflichten, die insbesondere in § 203 Strafgesetz-

buch ausdrückliche Erwähnung finden, bestehen neben den Vorschriften des BDSG. Die Auslagerung der Datenvernichtung an einen externen Dienstleister mittels eines ADV-Vertrages, kann daher eine unzulässige Offenbarung von Geheimnissen darstellen, selbst wenn die Voraussetzungen für eine Auftragsverarbeitung vorliegen.

Auch für die Vernichtung von Akten gelten die Vorschriften des BDSG, da die Vernichtung eine Form der Verarbeitung, nämlich der Löschung darstellt. Es gelten daher auch für die Vernichtung von Akten die Pflichten der verantwortlichen Stelle. Die verantwortliche Stelle hat daher die erforderlichen technischen und organisatorischen Maßnahmen zu ergreifen, die für die Umsetzung des BDSG erforderlich sind. Bei Aktenvernichtungen, die besondere Arten personenbezogener Daten beinhalten, ist darauf zu achten, dass diese auch nach dem Schreddern nur eine Materialteilchengröße von kleiner/gleich 30 qmm aufweisen und damit den Anforderungen an die Sicherheitsstufe P-5 der DIN 66399-1 genügen.

3.40 Hilferuf eines Vereins aus dem datenschutzrechtlichen Dickicht

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichte eine breit gefächerte Anfrage eines Thüringer Vereins hinsichtlich verschiedener datenschutzrechtlicher Problemstellungen, angefangen bei den besonderen Anforderungen an eine Einwilligung zur Datennutzung, die Formulierung einer Datenschutzerklärung, der Versendung von Newslettern an seine Vereinsmitglieder sowie die zulässige Nutzung von Fotos für die Website des Vereins.
Die datenschutzrechtliche Einwilligungserklärung und die Hinweise zum Datenschutz sind dabei sachlich verschiedene Dinge, die nicht miteinander vermischt werden dürfen. Es ist daher zwischen einem reinen Datenschutzhinweis und zwischen einer datenschutzrechtlichen Einwilligungserklärung zu trennen. Ein entsprechendes Formblatt, welches an die Mitglieder ausgegeben werden soll, muss dies auch redaktionell berücksichtigen. Der Betroffene muss in dem Formblatt zur Einwilligung klar und verständlich über die zu verarbeitenden Daten und den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung der Daten durch die verantwortliche Stelle

informiert werden. Ebenfalls ist auf die Folgen einer eventuellen Verweigerung der Einwilligung hinzuweisen (§ 4a Abs. 1 Satz 2 Bundesdatenschutzgesetz [BDSG]). Wenn im Rahmen der Verarbeitung auch Datenübermittlungen an Dritte in Betracht kommen, sind die Datenübermittlungen mit deren Zweckbestimmung und die Empfänger der Daten transparent in der Einwilligungserklärung zu erläutern. Weiterhin ist zu beachten, dass eine wirksame Einwilligung gem. § 4a BDSG auch nur dann vorliegt, wenn diese freiwillig abgegeben wurde und jederzeit widerrufen werden kann. Auf diese Möglichkeit ist ebenfalls explizit hinzuweisen. Schlussendlich sollte auch die Erklärung selbst eindeutig und aus sich heraus verständlich sein. Es ist eine Formulierung zu wählen, die dem Betroffenen bewusst macht, dass er eine zusätzliche Erklärung abgibt. Es sollte auch möglichst eine Einwilligungserklärung erstellt werden, die alle Zwecke der möglichen Verwendung beinhaltet. Für jeden einzelnen Zweck, also für werbliche Ansprache, Newsletter, für Veröffentlichung von Daten im Internet, für das Lastschriftverfahren usw., wird eine gesonderte Erklärung abgefragt und jeweils auf die Widerruflichkeit hingewiesen. Jede einzelne Erklärung kann dann entweder vom Betroffenen unterschrieben und damit die Einwilligung erteilt werden, oder eben nicht. Eine Vielzahl von einzelnen Einwilligungserklärungen trägt nicht zur Transparenz bei und birgt die Gefahr, dass die Einholung einzelner Erklärungen auch vergessen werden kann.
Bei der Datenschutzerklärung hingegen handelt es sich um die reinen Informationen über Datenverarbeitung auf der Grundlage von Gesetz bzw. Vertrag.
Der Verein wollte seine Mitglieder zukünftig auch gerne in einem Newsletter über alles rund um den Verein informieren. Dieser Newsletter sollte aber gleichermaßen an die bestehenden und die neuen Mitglieder versandt werden. Die Voraussetzungen dafür sind jedoch unterschiedlich. Zunächst ist bei den bestehenden Mitgliedschaften von einer rechtmäßigen Erhebung der Adressdaten der E-Mail-Adresse ausdrücklich für Vereinszwecke, d. h. für die Übersendung von Informationen über alle Belange des Vereins, auszugehen. Diese Informationsübermittlung kann dann auch mithilfe des Newsletters geschehen. Beachtet werden muss jedoch, dass dieser Newsletter dann keine „Werbung“ darstellt und ausschließlich vereinsinterne Mitteilungen enthält, die vom Vereinszweck gedeckt sind und damit durch die Versendung eigene Geschäftszwecke des Vereins gemäß § 28 Abs. 1 Nr. 1 BDSG erfüllt werden.

Enthält der Newsletter Werbung, so ist eine Nutzung der E-Mail-Adresse nur unter den Voraussetzungen des § 28 Abs. 3 ff. BDSG möglich. Da es sich bei der E-Mail-Adresse nicht um listenmäßig zusammengefasste Daten über Angehörige einer bestimmten Personengruppe, die sich auf die Zugehörigkeit des Betroffenen zu dieser Personengruppe, seine Berufsbezeichnung, seinen Namen, Titel, akademischen Grad, seine Anschrift und sein Geburtsjahr beschränken (privilegiertes Listendatum) handelt, wird daher dann zwingend die Einwilligung der jeweiligen Person, § 28 Abs. 3 Satz 1 BDSG, benötigt. Auch muss in den Fällen der Datenerhebung nach § 28 Abs. 1 Satz 1 BDSG und bei jeder Ansprache des einzelnen Mitglieds zum Zwecke der Werbung über das Widerspruchsrecht belehrt werden, § 28 Abs. 4 Satz 2 BDSG. Diese Belehrung ist dann an die „Bestandsmitglieder“ bereits vor der ersten werblichen Ansprache zu erteilen, da bereits hierfür und dann ohne vorherige Belehrung die E-Mail zum Zwecke der Werbung genutzt werden würde. Bei den neuen Mitgliedern würde man diese Einwilligung zur werblichen Ansprache natürlich vorab, schon bei Beantragung der Mitgliedschaft, einholen. Dem Verein wurde daher angeraten, dass Einwilligungsformular entsprechend anzupassen.

Eine weitere Frage betraf die Verwendung von Fotos, welche im Rahmen von Veranstaltungen wie Messen oder anderen öffentlichen Anlässen gemacht werden. Diese Fotos sollen dem Verein für seine Vereinschronik zur Verfügung stehen. Hierbei wurden von den Personen, die jeweils fotografiert worden sind, mündliche Zustimmungen eingeholt. Fraglich war seitens des Vereins, ob dies ausreichend ist und was passiert, wenn ein Betroffener auf einem Foto nicht zustimmt. Da der Verein im Zweifel die rechtmäßige Verwendung der Fotos nachzuweisen hat, ist es auf jeden Fall notwendig, dass die Einwilligung zur Nutzung und/oder Veröffentlichung der Fotos schriftlich niedergelegt wird. Daraus lässt sich auch zweifelsfrei der jeweilige Umfang der Nutzungsberechtigung ersehen. Ein grundsätzliches Löschen des gesamten Fotos, wenn eine Einwilligung nicht gegeben wurde, ist nicht notwendig. Es genügt dann, wenn der Einzelne stark verpixelt dargestellt oder anderweitig unkenntlich gemacht wird (Balken).

Der Verein hat zusammen mit dem TLfDI seine Formulare und Erklärungsblätter überarbeitet und seinen Mitgliedern daraufhin überarbeitet zur Verfügung gestellt.

Die datenschutzrechtliche Einwilligungserklärung und die Hinweise zum Datenschutz sind sachlich verschiedene Dinge, die nicht miteinander vermischt werden dürfen. In der Einwilligungserklärung muss klar und verständlich über die zu verarbeitenden Daten und den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung der Daten durch die verantwortliche Stelle informiert werden. Ebenfalls ist auf die Folgen einer eventuellen Verweigerung der Einwilligung hinzuweisen. Für jeden einzelnen Zweck, also für werbliche Ansprache, Newsletter, für Veröffentlichung von Daten im Internet, für das Lastschriftverfahren usw., wird eine gesonderte Erklärung abgefragt und jeweils auf die Widerruflichkeit hingewiesen.

3.41 Vereinsberatunng

Im Berichtszeitraum wandte sich ein beratender Verein an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Er erbat eine Beratung zu seinem Umgang mit Datenflüssen sowie die Klärung von Fragen zu datenschutzrechtlichen Bestimmungen, um seine Arbeit zu optimieren.
Gemäß § 38 Abs. 1 S. 2 Bundesdatenschutzgesetz (BDSG) berät und unterstützt die Aufsichtsbehörde die Beauftragten für den Datenschutz und die verantwortlichen Stellen mit Rücksicht auf deren typische Bedürfnisse.
Um den Umgang mit personenbezogenen Daten datenschutzrechtlich bewerten zu können, mussten zunächst die genauen Datenflüsse und Beratungssachverhalte geklärt werden. Hierfür traf sich der TLfDI mit Vertretern der Beratungsstelle. Zu klärende Fragen waren unter anderem: Auf welche Ermächtigungsnormen stützen sich die Erhebung, Verarbeitung und Übermittlung von personenbezogenen Daten und besonderer Arten von personenbezogenen Daten (siehe § 3 Abs. 9 BDSG).
Werden schriftliche Einwilligungserklärungen der Betroffenen eingeholt?
Außerdem wurde die Beratungsstelle gebeten darzulegen, wie und welche Daten erhoben werden, warum diese erforderlich sind, wie diese Daten dann weiterverarbeitet werden und, falls eine Übermittlung der Daten stattfindet, an wen diese Übermittlung erfolgt. Zudem sollte erklärt werden, welche technischen und organisatorischen Maßnahmen getroffen wurden, um das Bundesdatenschutzgesetz umzusetzen (gem. § 9 BDSG i. V. m. der Anlage). Des Weiteren

sollte die Beratungsstelle ausführen, welchen Aufbewahrungsfristen die erhobenen Daten unterliegen und auf welche Art und Weise die Löschung vorgenommen wird. Die Beratungsstelle kam dem nach und reichte hierfür verschiedene Unterlagen ein. Diese Unterlagen werden nun vom TLfDI auf ihre Vereinbarkeit mit dem BDSG hin geprüft. Nach der Feststellung eines möglichen Änderungsbedarfs wird der TLfDI eine abschließende datenschutzrechtliche Beurteilung treffen. Über den Ausgang wird der TLfDI im nächsten Tätigkeitsbericht informieren.

Nach § 38 Abs. 1 S. 2 Bundesdatenschutzgesetz (BDSG) berät und unterstützt die Aufsichtsbehörde die Beauftragten für den Datenschutz und die verantwortlichen Stellen mit Rücksicht auf deren typische Bedürfnisse. Verantwortliche Stellen, also Unternehmen und Personen, die personenbezogene Daten erheben, verarbeiten und übermitteln, können sich bei Unsicherheiten im Umgang mit Daten mit ihren Fragen immer an den TLfDI wenden.

3.42 Herrenlose Akten eines Bauunternehmers

Der behördliche Datenschutzbeauftragte (bDSB) eines Thüringer Landratsamtes (LRA) wandte sich im Namen des Bauordnungsamtes des LRA an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Bei der Begehung einer Abbruchimmobilie hatte das Bauordnungsamt zwei Schränke mit diversen Aktenordnern gefunden. Aufgrund des sehr maroden Gebäudezustands und der Gefahr für die öffentliche Sicherheit und Ordnung beabsichtigte das Bauordnungsamt einen kurzfristigen Rückbau. Als Eigentümer der Immobilie war im Grundbuch eine GmbH eingetragen, deren Prokurist verstorben war und deren Geschäftsführer sich im Ausland befand. Das Bauordnungsamt hatte jedoch keine Zustelladresse herausfinden können.
Im Hinblick auf den Datenschutz und den unbekannten Inhalt der Aktenordner im Gebäude bat der bDSB den TLfDI um Auskunft darüber, ob der Landkreis die Akten sicherstellen müsse (beispielsweise im Archiv) und wer Akteneinsicht erhalten dürfe. Zur Erläuterung übersandte der bDSB dem TLfDI Fotos der Aktenschränke im Gebäude.
Der TLfDI führte im Rahmen der Amtshilfe zunächst eine gemeinsame Begehung der Immobile mit dem Bauordnungsamt des LRA

durch. Dabei wurden ca. 50 Aktenordner festgestellt, die einem Bauunternehmen und dessen Komplementärin (persönlich haftender Gesellschafter einer Kommanditgesellschaft) zugeordnet werden konnte. Der TLfDI bat die zuständigen Gewerbeämter um nähere Auskunft zum Status der Unternehmen. Das Gewerbeamt informierte den TLfDI darüber, dass beide angefragten Firmen abgemeldet seien und teilte dem TLfDI die genauen Adressen der früheren Firmensitze mit. Die zu diesem Zeitpunkt bestehende Adresse der Geschäftsführerin war auch bekannt. Beide Gesellschaften waren bereits aus dem Handelsregister gelöscht worden, wodurch auch die eingetragenen Liquidatoren seit diesem Zeitpunkt nicht mehr bestellt waren.
Aufgrund dieser Informationen wandte sich der TLfDI an das Einwohnermeldeamt und bat um Mitteilung, ob die Adresse der letzten Geschäftsführerin noch aktuell ist. Das Einwohnermeldeamt teilte dem TLfDI die aktuelle Adresse der letzten eingetragenen Geschäftsführerin mit.
Aufgrund der ihm nunmehr vorliegenden Informationen teilte der TLfDI dem Bauordnungsamt des Landkreises mit, dass die Geschäftsführerin wegen ihrer nicht vollständig durchgeführten Liquidation und der im Abbruchgebäude verbliebenen Akten u. U. als Störerin im ordnungsrechtlichen Sinne in Betracht komme. Dies müsse durch die hierfür zuständige Behörde geprüft werden. Sofern Tatbestände von Ordnungswidrigkeiten vorliegen, können diese auch verjährt sein.
Nach Auffassung des TLfDI tragen Liquidatoren einer GmbH auch eine Verantwortung im Sinne des Datenschutzrechts, da sie verpflichtet sind, die Geschäfte der Gesellschaft abzuwickeln und somit zumindest die verantwortliche Stelle entsprechend einem Geschäftsführer vertreten. Allerdings kann eine solche Verantwortlichkeit im Sinne des Bundesdatenschutzgesetzes (BDSG) nicht mehr greifen, wenn die zu liquidierende Gesellschaft gelöscht und damit die Liquidatoreneigenschaft ebenfalls erloschen ist.
Zur Abwicklung der Angelegenheit und zu einer möglichen Aufforderung, die Akten aus dem Gebäude zu entfernen, teilte der TLfDI dem Bauordnungsamt des Landkreises die aktuelle Meldeadresse der letzten Geschäftsführerin im Rahmen der Amtshilfe mit. Der TLfDI kündigte an, die frühere Geschäftsführerin über die Abgabe ihrer Meldeadresse gemäß § 21 Abs. 6 Thüringer Datenschutzgesetz (ThürDSG) zu informieren und bat das Bauordnungsamt, ihn über

den Ausgang des Verfahrens in Kenntnis zu setzen. Eine derartige Information hat den TLfDI noch nicht erreicht.

Nach Auffassung des TLfDI tragen Liquidatoren einer GmbH auch eine Verantwortung im Sinne des Datenschutzrechts, da sie verpflichtet sind, die Geschäfte der Gesellschaft abzuwickeln und somit zumindest die verantwortliche Stelle entsprechend einem Geschäftsführer zu vertreten. Allerdings kann eine solche Verantwortlichkeit im Sinne des Bundesdatenschutzgesetzes (BDSG) nicht mehr greifen, wenn die zu liquidierende Gesellschaft gelöscht und damit die Liquidatoreneigenschaft ebenfalls erloschen ist. Sofern nach der Löschung festgestellt wird, dass die Vernichtung bzw. Abwicklung von Unternehmensakten datenschutzrechtlich nicht ordnungsgemäß erfolgte, sind Tatbestände einer Ordnungswidrigkeit zu prüfen.

3.43 Nachhilfe: Bürger erhält Auskunft

Im Berichtszeitraum wandte sich ein Bürger an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und bat um Hilfe. Er hatte sich mit der Bitte um Auskunft nach § 34 Bundesdatenschutzgesetz (BDSG) über die zu seiner Person gespeicherten Daten an eine Firma gewandt. Nach § 34 Abs. 1 BDSG hat jedermann einen Auskunftsanspruch gegen verantwortliche Stellen. Dieser Anspruch beinhaltet die zu einer Person gespeicherten Daten, die Herkunft der Daten, den Empfänger, an den diese Daten weitergegeben werden und den Zweck der Speicherung.
Die Firma beantwortete die vom Beschwerdeführer gestellten Fragen allerdings nicht, weswegen dieser sich hilfesuchend an den TLfDI wandte. Der TLfDI kontaktierte daraufhin mit einem Auskunftsverlangen nach § 38 BDSG das Unternehmen und bat um Auskunft darüber, welche Daten zu dessen Person gespeichert, woher diese Daten bezogen, an wen diese Daten weitergegeben und zu welchem Zweck diese Daten gespeichert wurden. Gleichzeitig wurde das Unternehmen vom TLfDI über den Inhalt der Auskunftspflicht nach § 34 BDSG belehrt.
Das Unternehmen reagierte auf das Auskunftsverlangen rasch und erklärte dem TLfDI die Vorgehensweise bei Anfragen nach § 34 BDSG. Es hätte bereits einigen Kunden solche Auskünfte erteilt, weswegen ihnen das Prozedere nicht unbekannt sei. In der Regel würden solche Anfragen innerhalb einer Woche beantwortet. Des

Weiteren versicherte das Unternehmen, dass es durchaus wüsste, dass es diese Auskünfte zu erteilen habe und auch keinen Grund sähe, dies nicht zu tun. Allerdings teilte das Unternehmen mit, dass es diese Anfrage des Bürgers nicht erhalten habe. Es konnte die Anfrage auch nicht anhand des Namens finden. Der TLfDI übersandte deshalb – mit Zustimmung des Bürgers – das Auskunftsersuchen erneut an das Unternehmen, woraufhin der Bürger seine erwünschten Auskünfte erhielt.
Am Ende bedankte sich der Bürger beim TLfDI für die unkomplizierte und schnelle Hilfe. Damit war das Verfahren abgeschlossen. Die Aussage, man habe das Schreiben des Bürgers nicht erhalten, ließ sich nicht widerlegen, da es per E-Mail versandt wurde. Aus diesem Grund wurden gegenüber dem Unternehmen auch keine weiteren Maßnahmen ergriffen.

Gemäß § 34 Abs. 1 BDSG sind die verantwortlichen Stellen dem Betroffenen gegenüber verpflichtet, auf dessen Verlangen über die zu seiner Person gespeicherten Daten, auch soweit sie sich auf die Herkunft dieser Daten beziehen, sowie über den Empfänger, an den die Daten weiter gegeben werden und über den Zweck der Speicherung Auskunft zu erteilen. Die Auskunft umfasst auch die Mitteilung, dass, sollte dies der Fall sein, über den Betroffenen keine Daten gespeichert sind (sog. Negativauskunft). Der TLfDI rät dazu, solche Auskunftsersuchen immer in einer Art und Weise zu versenden, die den Zugang dokumentiert. Am besten per Einschreiben mit Rückschein. Dabei sollte dem Unternehmen eine angemessene Frist zur Bearbeitung eingeräumt werden. In der Regel ist hierbei ein Zeitraum von zwei Wochen anzusetzen.

3.44 Keine Lastschrift ohne Daten

Im Berichtszeitraum erreichte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) die Beschwerde einer Kundin über das Lastschriftverfahren in einem Einzelhandelsgeschäft.
Zur Klärung des Sachverhalts führte der TLfDI eine unangekündigte Vor-Ort-Kontrolle nach § 38 Abs. 4 Bundesdatenschutzgesetz (BDSG) durch. Während des Gesprächs mit dem Geschäftsführer erklärte sich dieser nach anfänglichen Vorbehalten auch mit der Kontrolle einverstanden. Daraufhin erklärte er den Ablauf eines

Lastschriftverfahrens in seinem Ladengeschäft. Der Kunde wird beim Zahlvorgang mittels Lastschrift nach Name und Anschrift gefragt. Diese Angaben werden vom Verkäufer in die elektronische Kasse (Computerkasse) eingegeben, um dann einen Beleg drucken zu können. Auf dem Lastschriftbeleg werden dann neben der Kontonummer, der Bankleitzahl und dem Betrag auch der Name und die Adresse des Einkaufenden erfasst.
Gemäß § 4 Abs. 1 BDSG ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Eine schriftliche Einwilligung, wie vom Gesetzgeber gefordert, wird vorliegend nicht eingeholt. Als einzige Erlaubnisnorm für die hier vorgenommene Datenerhebung und Speicherung käme § 28 Abs. 1 Satz 1 Nr. 1 BDSG infrage. Gemäß dieser Vorschrift ist das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke nur zulässig, wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist. Allerdings sind Name und Anschrift nicht erforderlich, um das Schuldverhältnis zwischen dem Kunden und dem Einzelhandelsgeschäft zu begründen, durchzuführen oder zu beenden. Auch für den eventuellen Fall der Nichteinlösung einer Lastschrift sind diese zusätzlichen Daten nicht erforderlich. Für die Abwicklung eines Lastschriftverfahrens sind die mittgeteilten Kontodaten ausreichend. Im Falle der Nichteinlösung der Lastschrift wird die Bank des Kunden durch dessen Unterschrift bevollmächtigt, an den Verkäufer die zur Verfolgung des Anspruchs notwendigen personenbezogenen Daten herauszugeben. Das zusätzliche Erfassen von Adresse und Name des Kunden auf dem Lastschriftbeleg ist daher zur Verfolgung des Anspruchs auf Zahlung nicht erforderlich, da der Verkäufer ohne Weiteres von der Bank diese Daten auf Nachfrage erhält. Insoweit stellt daher das Vermerken der zusätzlichen Daten auf dem Beleg einen datenschutzrechtlich unzulässigen Vorgang dar.

Gem. § 28 Abs. 1 Satz 1 Nr. 1 BDSG ist das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke nur zulässig, wenn es für die Begründung, Durchführung oder Beendi-

gung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist. Ein Unternehmen ist daher nur dazu berechtigt, die zur Durchführung einer Kaufhandlung notwendigen Daten zu erheben und zu nutzen.

3.45 Jeder kennt jeden – Hausverwaltung gibt Daten weiter

Im Berichtszeitraum beschwerte sich ein Bürger über seine Hausverwaltung. Er erhielt ein Mieterhöhungsschreiben seiner Hausverwaltung. Hierbei wurden zur Ermittlung der ortsüblichen Miete, drei sogenannte Vergleichsobjekte im selben Gemeindegebiet benannt. Diese Vergleichsobjekte enthielten in ihrer Beschreibung den vollständigen Namen der derzeitigen Mieter, die vollständige Adresse mit Angabe der Etage, die Wohnfläche und den Mietzins pro Quadratmeter. Der Bürger kritisierte zudem, dass man durch die Daten – wie Größe der Wohnung und den monatlichen Mietzins – durchaus Rückschlüsse auf die Einkommensverhältnisse ziehen könnte.
Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) wandte sich mit einem Auskunftsverlangen an die Hausverwaltung. Der TLfDI wollte in Erfahrung bringen, aufgrund welcher Rechtsgrundlage die vollständigen Namen der Mieter der Vergleichsobjekte benannt wurden und bei welchen weiteren Mieterhöhungsschreiben die personenbezogenen Daten des Bürgers wiederum als Referenzobjekt für eine Mieterhöhung angegeben wurden.
Die Hausverwaltung erklärte, dass die rechtliche Grundlage in § 558a Absatz 2 Nummer 4 des Bürgerlichen Gesetzbuchs (BGB) zu finden sei. Danach könne zur Begründung der Mieterhöhung Bezug auf entsprechende Entgelte für einzelne vergleichbare Wohnungen genommen werden, dabei genüge die Nennung von drei Wohnungen. Weiterhin gab die Hausverwaltung an, dass eine Voraussetzung für die Erhöhung nach der Vergleichsmiete sei, dass der Mieter die genannten Wohnungen eindeutig identifizieren kann. Der Mieter müsse nachvollziehen können, dass die geforderte Vergleichsmiete korrekt ist. Insbesondere bei Mehrfamilienhäusern ist es notwendig, auch den Namen des Mieters anzugeben. Hierzu führt der Bundesgerichtshof in seiner Entscheidung vom 20. September 1982 (BGHZ 84, 392) sowie vom 28. März 2012 (BGH WuM 2003, 149) aus, dass der Vermieter hierzu mindestens folgende Angaben machen muss: Anschrift der Vergleichswohnung (Straße, Hausnummer,

Stockwerk, Lagebezeichnung im Stockwerk), Name des Mieters, Angabe des Quadratmeterpreises mit Angabe der Gesamtgröße der Wohnung. Die Hausverwaltung teilte mit, dass die Daten des Bürgers in keinem weiteren Schreiben angegeben wurden.

Der TLfDI entgegnete daraufhin, dass gemäß § 4 Absatz 1 Bundesdatenschutzgesetz (BDSG) die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig ist, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Das Verarbeiten ist gem. § 3 Abs. 4 BDSG auch das Übermitteln personenbezogener Daten in der Weise, dass die Daten an einen Dritten weitergegeben werden. Der § 558a Abs. 2 Nr. 4 BGB ist für sich isoliert keine hinreichende Rechtsgrundlage dahingehend, vollständige Namen von Mietparteien der Vergleichsobjekte oder sonstige Informationen hierzu an andere Mieter übermitteln zu dürfen. *In der Kommentierung zum § 558a BGB nach Palandt, Rn. 11 heißt es dazu, dass die Vergleichswohnungen für den Mieter identifizierbar sein müssen, damit diese zugeordnet werden können, um beurteilen zu können, ob der Vergleich angemessen ist. Die Angabe der Adresse, des Geschosses und bei einem Mehrfamilienhaus die genaue Lage im Geschoss, die Wohnungsnummer oder aber auch den Namen des Mieters sowie die Quadratmeterzahl und -größe genügen an dieser Stelle.*

Dabei ist zu beachten, dass eben auch die sonstigen Informationen, die bei der Angabe einer Vergleichswohnung notwendig sind, personenbeziehbare Informationen sind, die einer natürlichen Person, dem Mieter, zugeordnet werden können. Rechtsgrundlage für eine Weitergabe dieser weiteren Informationen kann jedoch § 28 Abs. 1 Satz 1 Nr. 2 BDSG sein. Das Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke, Begründung einer Mieterhöhung, ist gemäß § 28 Abs. 1 Nr. 2 BDSG nur zulässig, soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle – nämlich die des Vermieters, die Mieterhöhung rechtmäßig durchzusetzen – erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt.

Bei der Abwägung dieser Interessen muss zwischen der Übermittlung des Namens und den sonstigen Identifizierungsmerkmalen der Wohnung unterschieden werden.

Die Weitergabe der Identifizierungsmerkmale der Vergleichswohnungen wie Adresse, Geschoss, Lage im Geschoss bzw. Wohnungsnummer kann gem. § 28 Abs. 1 Satz 1 Nr. 2 BDSG gerechtfertigt sein. Berechtigtes Interesse des Vermieters ist dabei, sein Mieterhöhungsverlangen auf eine Art und Weise zu begründen, mit der es vor Gericht Bestand haben kann. Eine der vom Gesetzgeber eingeräumten Möglichkeiten ist dabei das Vorlegen von drei Vergleichswohnungen. Das Interesse des Vermieters umfasst daher auch, diese so genau zu beschreiben, dass die Begründung wirksam ist.
Eben diese Angaben, die hierfür notwendig sind, nämlich Art, Größe, Preis und Lage der Wohnung, betreffen aber auch die unmittelbare Privatsphäre des jeweiligen Mieters. Es handelt sich dabei, wie oben bereits erwähnt, um personenbeziehbare Daten. Auch der Mieter hat ein schützenswertes Interesse an der Geheimhaltung dieser wirklich sehr privaten Informationen. Im Rahmen der nunmehr notwendigen Interessenabwägung hat man diese widerstreitenden Interessen gegeneinander abzuwägen. Weil die gesetzliche Wertung des § 558a BGB dabei Beachtung finden muss, ist in der Regel davon auszugehen, dass die schutzwürdigen Interessen des jeweiligen Mieters nicht überwiegen. Um dies bewerten zu können, müssen die jeweiligen Mieter der Wohnungen allerdings vorab befragt werden, ob aus deren Sicht irgendwelche schutzwürdigen Interessen bestehen. Anders ist die Nennung des Vor- und Nachnamens des jeweiligen Mieters der Vergleichswohnung zu bewerten. Hier überwiegt das schutzwürdige Interesse des Mieters an dem Ausschluss der Verarbeitung oder Nutzung zumindest hinsichtlich seines Vor- und Nachnamens zum Zwecke der Angabe von Vergleichswohnungen im Rahmen des § 558a Abs. 2 Nr. 4 BGB gegenüber der Wahrung berechtigter Interessen der Hausverwaltung an der Erfüllung der Geschäftszwecke, hier dem Erfordernis aus § 558a Abs. 2 Nr. 4 BGB, der Angabe von Vergleichsobjekten nachzukommen. Der Mieter hat ein schutzwürdiges Interesse daran, dass seine Daten, so hier insbesondere die Angabe seines Namens in Schreiben, welche an andere Mieter gerichtet sind, durch den Vermieter geschützt werden und er anonym bleiben kann. Weil es hier an der im Rahmen des § 28 Abs. 1 Satz 1 Nr. 2 BDSG notwendigen Erforderlichkeit der Übermittlung des Namens fehlt, hätte es einer Einwilligung des betroffenen Mieters bedurft, die den Voraussetzungen des § 4a BDSG entspricht.

Die Hausverwaltung bezog daraufhin Stellung. Der Hausverwaltung sei die Problematik des Schutzes der persönlichen Daten des Mieters auf der einen Seite und der Wahrung der Interessen des Vermieters für die Erhöhung der Miete auf der anderen Seite durchaus bewusst. Allerdings sei die Hausverwaltung bisher davon ausgegangen, dass die Vergleichswohnungen so genau wie möglich beschrieben werden müssen, um den Mieter in die Lage zu versetzen, genau zu prüfen, um welche Vergleichswohnungen es sich handelt und ob das Erhöhungsverlangen des Vermieters gerechtfertigt ist. Die Hausverwaltung bedankte sich für die Klarstellung und versicherte die rechtlichen Hinweise zukünftig zu beachten.

Gemäß § 4 Absatz 1 Bundesdatenschutzgesetz (BDSG) ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Das Verarbeiten ist gem. § 3 Abs. 4 BDSG auch das Übermitteln personenbezogener Daten in der Weise, dass die Daten an einen Dritten weitergegeben werden. Der § 558a Abs. 2 Nr. 4 BGB ist für sich isoliert keine hinreichende Rechtsgrundlage dahingehend, vollständige Namen von Mietparteien der Vergleichsobjekte oder sonstige Informationen hierzu an andere Mieter übermitteln zu dürfen. Dabei ist zu beachten, dass eben auch die sonstigen Informationen, die bei der Angabe einer Vergleichswohnung notwendig sind, personenbeziehbare Informationen sind, die einer natürlichen Person, dem Mieter, zugeordnet werden können.

3.46 Ich bin du, du bist ich?

Im Berichtszeitraum erreichte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) die Beschwerde eines Unternehmens, dass die Identität dieses Unternehmens gestohlen und die Daten bei angeblichen Verkäufen von Waren genutzt worden seien, um an die Gelder der Käufer zu gelangen. Recherchen ergaben, dass die Adresse des Unternehmens von einem anderen Unternehmen mit einem ähnlich klingenden Namen als Rechnungsadresse genutzt sowie auf der Website unter Kontaktinformationen aufgeführt wurde.
Nach § 1 Bundesdatenschutzgesetz (BDSG) ist der Zweck des Bundesdatenschutzgesetzes, den Einzelnen davor zu schützen, dass er

durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird. Personenbezogene Daten sind gemäß § 3 Abs. 1 BDSG Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).
In dem vorliegenden Fall wurden die Daten eines Unternehmens missbräuchlich verwendet. Somit ist das Unternehmen nicht Betroffener in dem Sinne, da es sich bei einem Unternehmen um eine juristische Person und nicht um eine natürliche Person handelt. Daher musste der TLfDI leider mitteilen, dass er in diesem Fall sachlich nicht zuständig ist. Anders wäre der Sachverhalt zu beurteilen, wenn auch die Daten der Unternehmensangehörigen, wie z. B. der Name, im Rahmen des Identitätsbetrugs genutzt worden wären. Bei diesen Daten handelt es sich wiederum um personenbezogene Daten, da die Daten natürliche Personen betreffen.

§ 3 Abs. 1 BDSG definiert personenbezogene Daten als Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Sofern keine Daten, die mit einer natürlichen Person verknüpft werden können (z. B. Namen, Zugehörigkeiten und Funktionen in einem Unternehmen) in einem Identitätsbetrug genutzt werden, sondern es sich lediglich um reine Unternehmensdaten handelt, ist der TLfDI nicht zuständig.

3.47 Geheimnis: Akten einer Steuerberatungskanzlei

Im Berichtszeitraum wurde dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) mitgeteilt, dass in einem derzeit nicht mehr gewerblich genutzten Gebäude Akten einer Steuerkanzlei lagern und dieses Gebäude nunmehr von den Eigentümern verkauft wurde.
Der TLfDI wandte sich daraufhin an die Eigentümer und den zuletzt in diesem Gebäude tätigen Steuerberater als möglichen Verantwortlichen und forderte diesen auf, die Akten im Gebäude zu beräumen bzw. fachgerecht zu entsorgen. Daraufhin teilte der Steuerberater dem TLfDI mit, dass es zwar richtig sei, dass er zuletzt in dem Gebäude mit seiner Steuerkanzlei tätig gewesen sei, die Aktenbestände aber wohl zum großen Teil nicht von ihm stammen, sondern noch von seinem Vorgänger, von dem er die Kanzlei seinerzeit übernommen habe. Daraufhin wurde vom TLfDI eine Vor-Ort-Kontrolle der

lagernden Akten durchgeführt. Diese ergab, dass es sich bei den Akten wirklich um solche handelte, die keinen Aufbewahrungsfristen mehr unterliegen und daher der fachgerechten Entsorgung zuzuführen sind. Die Entsorgung von Altaktenbeständen unterliegt datenschutzrechtlich § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG), da es sich um eine Verarbeitung personenbezogener Daten handelt. Diese ist jedoch nur zulässig, wenn das BDSG oder eine andere Rechtsvorschrift dies erlaubt oder anordnet. Gemäß § 35 Abs. 2 Nr. 3 sind personenbezogene Daten zu löschen, wenn sie für eigene Zwecke verarbeitet werden, sobald ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist.
Aus diesem Grunde wurde auch der Vorinhaber der Kanzlei angeschrieben und aufgefordert, die Altaktenbestände zu entsorgen. Die Beteiligten wurden seitens des TLfDI darauf aufmerksam gemacht, dass bei der datenschutzgerechten Entsorgung der Akten darauf zu achten ist, dass diese nach DIN 66399-2 und der dortigen Sicherheitsstufe P-5 vernichtet werden. Eine Vernichtung unterhalb dieser Sicherheitsstufe würde nicht den datenschutzrechtlichen Vorgaben entsprechen, da es sich vorliegend um Daten handelt, die einem besonderen Schutzbedarf unterfallen. Die dem Steuerberater anvertrauten Geheimnisse unterfallen dem Schutzbereich des § 203 Strafgesetzbuch (StGB). Es ist also darauf zu achten, dass eine Kenntnisnahme durch Dritte deswegen beim Vernichtungsprozess absolut ausgeschlossen ist.
Wird die Vernichtung durch Dritte durchgeführt, ist mit diesem Unternehmen hinsichtlich der Vernichtung ein entsprechender Vertrag über die Auftragsdatenverarbeitung nach § 11 BDSG zu schließen. Nach Aufforderung des TLfDI zur datenschutzgerechten Entsorgung der Altaktenbestände einigten sich die Kanzleiinhaber darüber, die Aktenbestände gemeinschaftlich mithilfe eines zertifizierten Aktenentsorgungsunternehmens zu entsorgen. Die Vorgaben des TLfDI wurden eingehalten und die Entsorgung erfolgreich durchgeführt.

Bei Verlassen eines Firmengebäudes wegen Verkaufs oder Geschäftsaufgabe dürfen keine Aktenbestände zurückgelassen werden. Die Akten müssen archiviert und bei Ablauf der Aufbewahrungsfrist datenschutzgerecht vernichtet werden. Die Entsorgung von Altaktenbeständen unterliegt datenschutzrechtlich § 4 Abs. 1 BDSG, da es sich um eine Verarbeitung personenbezogener Daten handelt. Diese ist jedoch nur zulässig, wenn das BDSG oder eine andere

Rechtsvorschrift dies erlaubt oder anordnet. Gemäß § 35 Abs. 2 Nr. 3 sind personenbezogene Daten zu löschen, wenn sie für eigene Zwecke verarbeitet werden, sobald ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist. Handelt es sich bei dem Aktenmaterial um Geheimnisse i. S. v. § 203 StGB, muss eine Kenntnisnahme durch unbefugte Dritte beim Vernichtungsprozess ausgeschlossen sein.

3.48 TLfDI kontrolliert Weihnachtsmann ;-)

In der Vorweihnachtszeit wollte ein engagierter Bürger wissen, ob der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) das Weihnachtspostamt der Deutschen Post AG geprüft habe. Namentlich war die Adresse „An den Weihnachtsmann in 99706 Himmelsberg“ angegeben. Sollte eine Prüfung nicht erfolgt sein, bat er dies – aufgrund des zu erwartenden hohen Andrangs – nachzuholen.
Das Bundesdatenschutzgesetz (BDSG) ist dem Grunde nach § 1 Abs. 2 Nr. 3 anwendbar, sofern es sich beim Weihnachtsmann um eine Stelle handelt, die nicht in einem anderen Mitgliedsstaat der europäische Union (EU) oder im europäischen Wirtschaftsraum (EWR) ihren Sitz hat, § 1 Abs. 5 Satz 1 BDSG. Der Sitz des Weihnachtsmannes und damit auch Ort der Datenverarbeitung sind strittig. Vertreten werden hauptsächlich die Länder Schweden und Finnland, sowie Grönland und der Nordpol. Jedenfalls hat der Weihnachtsmann keinen Sitz in Deutschland. Dies kann festgestellt werden, da er aufgrund der Art und des Umfangs seiner Tätigkeit als sogenannter Istkaufmann nach § 1 Abs. 1 Handeslgesetzbuch (HGB) im Handelsregister eingetragen sein müsste. Da es an einer solchen Eintragung fehlt und dem Weihnachtsmann grundsätzlich Rechtstreue unterstellt werden kann, ist also davon auszugehen, dass ein Sitz in Deutschland nicht existiert. Je nach tatsächlichem Sitz des Weihnachtsmanns würde eine Zuständigkeit des TLfDI schon aufgrund von § 1 Abs. 5 Satz 1 BDSG ausscheiden. Beim Sitz in Grönland oder gar am Nordpol hingegen könnte der TLfDI nach § 1 Abs. 5 Satz 1 BDSG zuständig sein, da dann eine Stelle, die ihren Sitz nicht innerhalb der EU oder des EWR hat, die Datenerhebung und -verarbeitung im (u. a.) Thüringer Inland durchführt.
Die Frage des tatsächlichen Sitzes des Weihnachtsmannes kann aber dahinstehen. Beim Weihnachtsmann handelt es sich, ebenso wie

beim Konkurrenzunternehmen Christkind, höchstwahrscheinlich um eine Angelegenheit der Religionsausübung, bzw. um das Innehaben und Ausüben einer religionsspezifischen Funktion, jedenfalls aber um eine andere vergleichbare organisationsinterne Angelegenheit der Religionsgesellschaft. Damit handelt es sich um den Kernbereich der durch Art. 137 Weimarer Reichsverfassung geschützten Autonomie der Religionsgesellschaften, weswegen der TLfDI nicht zuständig ist (vgl. auch Dammann in Simitis, 8. Auflage, § 2,Rn. 113). Zuständig wäre in diesem Fall je nach persönlicher Einstellung der Beauftragte für den Datenschutz der Evangelischen Kirche in Deutschland, Böttcherstraße 7, 30419 Hannover oder der Diözesandatenschutzbeauftragte, Chausseestraße 1, 39218 Schönebeck.
Für sein unterstützendes Organ, nämlich das Weihnachtspostamt unter der Adresse „An den Weihnachtsmann, 99706 Himmelsberg“, betrieben durch die Deutsche Post AG, besteht leider beim TLfDI ebenfalls keine Zuständigkeit. Nach § 42 Abs. 3 Postgesetz ist hierfür die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) zuständig.
Bedauerlicherweise war es dem TLfDI nicht möglich, weder den Weihnachtsmann selbst, noch das benannte Postamt zu kontrollieren.

In Angelegenheiten der Religionsausübung der beiden christlichen Kirchen bzw. bei organisationsinternen Angelegenheiten der Religionsgesellschaften ist der Beauftragte für den Datenschutz der Evangelischen Kirche in Deutschland oder der Diözesandatenschutzbeauftragte zuständig. Hinsichtlich des unterstützenden Organs des Weihnachtsmannes, nämlich das Weihnachtspostamt, betrieben durch die Deutsche Post AG, besteht beim TLfDI leider keine Zuständigkeit. Hierfür ist nach § 42 Abs. 3 Postgesetz die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) zuständig.



© Spencer – 3D Man Office / Fotolia.com

4 Datenschutzkonformität von unternehmensinternen Unterlagen

4.1 Datenschutz auch bei Korruptionsbekämpfung

In einem Thüringer Unternehmen wurde eine neue Dienstanweisung mit dem Thema Korruptionsprävention und -bekämpfung herausgegeben. Der Betriebsratsvorsitzende des Unternehmens wandte sich mit der Bitte um Beratung an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). In der Dienstanweisung war eine Regelung enthalten, nach der die Mitarbeiter des Unternehmens mitteilen sollten, welche Firmen, mit denen das Unternehmen in Geschäftsverbindung stand, diese auch privat beauftragen wollen. Dies sollten sie ihrem direkten Vorgesetzten

oder der Geschäftsführung anzeigen. Der Betriebsratsvorsitzende war der Auffassung, dass es völlige Privatsache sei, von wem ein Mitarbeiter bzw. dessen Familie Ware und Dienstleistungen bestellt, bezieht oder kauft.
Der TLfDI erfragte bei dem Unternehmen die Rechtsgrundlage dieser Regelung in der neuen Dienstanweisung. Das Unternehmen teilte mit, dass das vorgesehene Vorgehen dem Schutz der Betroffenen diene. Es solle vermieden werden, dass Sonderkonditionen, die mit bestimmten Unternehmen vereinbart werden, auch bei Vertragsbeziehungen mit der Privatperson zum Einsatz kommen bzw., dass eventuell ein Verdacht in dieser Hinsicht entsteht.
Da es sich um ein Unternehmen in 100 prozentiger kommunaler Trägerschaft handelte, war zunächst zu klären, ob das Thüringer Datenschutzgesetz (ThürDSG) oder das Bundesdatenschutzgesetz (BDSG) gilt. Das Unternehmen legte auf Nachfrage des TLfDI dar, dass es als juristische Person am Wettbewerb teilnehme. Damit ist nach § 26 ThürDSG nur der Fünfte Abschnitt des ThürDSG, ausgenommen § 34 Abs. 2 ThürDSG, und ansonsten das BDSG mit Ausnahme des 2. Abschnitts und des § 38 BDSG anwendbar. Das bedeutet, dass grundsätzlich alle Bestimmungen des BDSG auf dieses kommunale Wettbewerbsunternehmen anwendbar sind, mit Ausnahme der Bestimmungen, die die Datenschutzaufsicht betreffen. Diese richtet sich nach den für öffentliche Stellen geltenden Vorschriften des ThürDSG.
Zur Regelung in der Dienstvereinbarung merkte der TLfDI Folgendes an:
Nach der Definition des § 3 Abs. 1 BDSG sind personenbezogene Daten Einzelheiten über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener). Daher stellt die Anzeige, dass ein bestimmter Mitarbeiter beabsichtigt, ein bestimmtes Unternehmen im privaten Bereich zu beauftragen, selbstverständlich eine Erhebung personenbezogener Daten dar. Der anzuzeigende Sachverhalt bezieht sich jeweils auf einen bestimmten Mitarbeiter. Für die Erhebung, Verarbeitung und Nutzung der Beschäftigtendaten im Zusammenhang mit Korruptionsbekämpfung oder -verhinderung kommt § 32 Abs. 1 Satz 2 BDSG zur Anwendung. Danach können zur Aufdeckung von Straftaten personenbezogene Daten eines Beschäftigten nur dann erhoben, verarbeitet oder genutzt werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im

Beschäftigungsverhältnis eine Straftat begangen hat, die Erhebung, Verarbeitung oder Nutzung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind. Sollte also ein konkreter Verdacht bestehen, dass besondere Vorteile aus den Geschäftsbeziehungen des Unternehmens mit dem privat zu beauftragenden Unternehmen in Anspruch genommen werden oder werden sollen, ist gegen eine derartige Datenerhebung nichts einzuwenden. Hinsichtlich der Verhältnismäßigkeit ist zu beachten, dass es sich im Regelfall bei privater Beauftragung eines Unternehmens, das auch in Geschäftsbeziehung mit der Beschäftigungsfirma steht, um Geschäfte des täglichen Lebens handelt. Daher wäre nur dann eine mögliche Datenerhebung begründet, wenn es sich um einen nicht unerheblichen Betrag bzw. Auftrag handeln sollte. Bei jeglicher Beauftragung eines Unternehmens bereits zu unterstellen, dass von Beschäftigten Vorteile aus der Geschäftsbeziehung mit dem Arbeitgeber gezogen werden sollen, die im Bereich der Korruption bzw. der persönlichen Vorteilsnahme anzusiedeln wären, geht zu weit.
Der TLfDI sah daher die in Rede stehende Passage der Dienstanweisung als unzulässig an. Nach intensivem Schriftwechsel, in dessen Verlauf dem Unternehmen die Rechtslage dargelegt wurde, passte das Unternehmen die Passage der Dienstvereinbarung den datenschutzrechtlichen Anforderungen des TLfDI an. Von der Meldepflicht wurden nunmehr Geschäfte des täglichen Lebens ausgenommen, und in anderen Fällen wurden die Mitarbeiter angehalten, auch Angebote anderer Firmen einzuholen, um sicherzustellen, dass keine unverhältnismäßig günstigeren Konditionen vereinbart wurden.

Daten über Beschäftigte dürfen auch zum Zweck der Korruptionsbekämpfung und -verhinderung nur erhoben, verarbeitet oder genutzt werden, wenn § 32 BDSG dies zulässt. Da hier eine Straftat verhindert werden soll, kommt § 32 Abs. 1 und 2 BDSG zur Anwendung, nach dem es zu dokumentierende tatsächliche Anhaltspunkte für den Verdacht geben muss, dass der Betroffene im Bestechungsverhältnis eine Straftat begangen hat. Jedes Unternehmen muss daher prüfen, ob die Verhinderung von Korruption auch durch andere Maßnahmen als die Datenerhebung möglich ist.

4.2 Datenschutz im Sportverein – was dürfen SV, FC und Co.?

Ein Sportverein bat den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) darum, die vereinseigene Datenschutzverordnung hinsichtlich ihrer Vereinbarkeit mit dem Bundesdatenschutzgesetz zu überprüfen.
Beim TLfDI wurde das vereinseigene Regelungswerk näher beleuchtet und zunächst konnte festgestellt werden, dass es erfreulicherweise in seinen Grundzügen bereits den gesetzlichen Anforderungen entsprochen hat.
Grundsätzlich dürfen personenbezogene Daten nur erhoben, verarbeitet oder genutzt werden, soweit eine Vorschrift des Bundesdatenschutzgesetzes (BDSG) oder eine sonstige Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat, § 4 Abs. 1 BDSG. In § 28 Abs. 1 BDSG findet sich die zentrale Rechtsgrundlage für den Umgang mit personenbezogenen Daten in Vereinen. Danach ist das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist (Nr. 1). Die Mitgliedschaft in einem Verein ist als ein solches Schuldverhältnis anzusehen. Nur auf solche Daten, die der Verein zur Erfüllung seiner satzungsgemäßen Aufgaben und zur Gestaltung der Mitgliedschaft unbedingt benötigt, darf der Verein gem. § 28 Abs. 1 Nr. 1 BDSG zugreifen. Der in § 28 BDSG normierte Geschäftszweck ist in Vereinen mit dem Satzungszweck gleichzusetzen. Demnach ist für Vereine nach § 28 Abs. 1 Nr. 1 BDSG das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Satzungszwecke zulässig, wenn es für die Begründung, Durchführung oder Beendigung der Mitgliedschaft im Verein erforderlich ist. Dies schließt zumeist die Erhebung und Speicherung der Daten hinsichtlich Name, Vorname und Anschrift des Vereinsmitglieds ein.
Kommunikationsdaten werden neben der Anschrift für den Verein nicht unbedingt zur Erfüllung seiner satzungsgemäßen Aufgaben und zur Gestaltung der Mitgliedschaft benötigt. Es muss dem jeweiligen Mitglied selbst überlassen bleiben, ob es Angaben dazu machen möchte oder nicht. Es sollte daher klar im Mitgliedsantrag erkennbar sein, dass es sich bei den Kommunikationsdaten, wie E-Mail-

Adresse oder Telefonnummer, nicht um Pflichtangaben, sondern um freiwillige Angaben handelt. Allgemein muss bei der Frage, welche Mitgliederdaten erforderlich sind, immer der Grundsatz der Datenvermeidung und -sparsamkeit nach § 3a Satz 1 BDSG beachtet werden. Wenn der Verein für Funktionsträger auch Angaben zu Lizenzen und deren Gültigkeit erfasst, kann dies ebenfalls im Hinblick auf die jeweiligen satzungsgemäßen Aufgaben erfolgen. Die Erhebung und Verarbeitung der Bankverbindung ist auch nur zulässig, wenn die Satzung eine Zahlung der Vereinsbeiträge per Bankeinzug vorsieht. Ohne eine entsprechende Verpflichtung durch die Satzung ist der Einzug nicht erforderlich zur Gestaltung der Mitgliedschaft.
In Bezug auf eine mögliche Datenweitergabe an Dritte ist festzustellen, dass im Verein zuständige Personen keine Dritten im Sinne des § 3 Abs. 4 Nr. 3 BDSG sind. Danach ist Dritter jede Person oder Stelle außerhalb der verantwortlichen Stelle. Dies können z. B. Dachverbände sein. Hier handelt es sich um eine Datenübermittlung an Dritte im Sinne der vorgenannten Vorschrift. Folglich benötigt ein Verein, der seine Mitgliederdaten an die Dachorganisationen übermitteln will oder soll, eine Rechtsgrundlage oder die ausdrückliche Einwilligung der betroffenen Mitglieder. Es sollte sich für die jeweiligen Mitglieder aus der Satzung ableiten, welche Daten genau zu den notwendigen personen- und vereinsbezogenen Daten zählen.
Wegen der bestehenden Datenschutzverantwortung in einem Verein ist auch hier für einen ordnungsgemäßen Umgang mit den Mitgliederdaten zu sorgen und es sind technische und organisatorische Maßnahmen im Sinne des § 9 BDSG zu ergreifen. Insbesondere müssen die Daten gegen den Zugriff unberechtigter Dritter geschützt werden. Wird bei der Vereinskommunikation in zulässiger Weise mit einem E-Mail-Verteiler gearbeitet, sollte grundsätzlich der bcc-Modus genutzt werden. Es bedarf auch einer Verpflichtung derjenigen Personen auf das Datengeheimnis, die mit der Verarbeitung von personenbezogenen Daten im Verein betraut sind, vgl. § 5 BDSG. Soweit ehrenamtliche Mitarbeiter im Verein mit der Datenverarbeitung befasst sind, sind auch sie auf das Datengeheimnis zu verpflichten. Dazu sollte der Verein ein Merkblatt vorbereiten und dieses gegenzeichnen lassen.

Personenbezogene Daten dürfen nur erhoben, verarbeitet oder genutzt werden, soweit eine Vorschrift des BDSG oder eine sonstige Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene ein-

gewilligt hat, § 4 Abs. 1 BDSG. § 28 Abs. 1 BDSG ist die zentrale Rechtsgrundlage für den Umgang mit personenbezogenen Daten in Vereinen, da das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung nur als Mittel für die Erfüllung eigener Geschäftszwecke zulässig ist, wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen, also für die Mitgliedschaft in einem Verein, erforderlich ist. Dabei darf nur auf solche Daten zugegriffen werden, die der Verein zur Erfüllung seiner satzungsgemäßen Aufgaben und zur Gestaltung der Mitgliedschaft unbedingt benötigt. Ein Blick in die jeweilige Vereinssatzung ist daher unerlässlich.

4.3 Da wird der Hund in der Pfanne verrückt

Dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) wurde von der Landesbeauftragten für den Datenschutz und die Informationsfreiheit Nordrhein-Westfalen eine Eingabe beim Bayerischen Landesamt für Datenschutzaufsicht zugeleitet. Der Eintrag im Vereinsregisterauszug ergab, dass der betroffene Hundeverband e. V. seinen Sitz in Thüringen hat. Der TLfDI wurde als zuständige Stelle um Übernahme des Falles gebeten. Der Verein veröffentlichte regelmäßig bestimmte Vereinsmitglieder samt Adresse in einer Zeitschrift.
Im Rahmen seiner aufsichtsbehördlichen Tätigkeit wandte sich der TLfDI mit einem Auskunftsverlangen nach § 38 Abs. 3 Bundesdatenschutzgesetz (BDSG) an den Vereinsvorsitzenden. In seiner Bitte um Stellungnahme teilte der TLfDI dem Vereinsvorsitzenden mit, dass er darauf aufmerksam geworden ist, dass personenbezogene Daten, u. a. die genaue Adresse einzelner Mitglieder, in einer Verbandszeitschrift veröffentlicht wurden. Die personenbezogenen Daten wurden zuvor von seinem Verband erhoben und an den Verlag der Zeitschrift übermittelt. Bei der betroffenen Verbandszeitschrift handelte es sich um eine monatlich erscheinende, auch über den Handel zu beziehende Zeitschrift. Daher handelte es sich hierbei nicht um eine reine Mitgliederzeitschrift, vielmehr kann die Zeitschrift grundsätzlich von jedermann gekauft werden. Im Mittelteil einer jeden Ausgabe dieser Zeitschrift werden über mehrere Seiten umfangreich Kontaktdaten von o. g. Personen (Namen mit vollständiger Anschrift und Telefonnummer) veröffentlicht. In der betreffen-

den Ausgabe betraf dies ca. 400 Personen auf 8 1/4 Seiten. Soweit dem TLfDI bekannt geworden war, wurde seitens des Verlags / Herausgebers zu keiner Zeit um eine Zustimmung zur Veröffentlichung der Kontaktdaten gebeten.
Nach § 4 Abs. 1 BDSG ist die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten nur zulässig, soweit dieses Gesetz oder einen andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Darüber hinaus ist der Betroffene nach § 4 Abs. 3 BDSG von der verantwortlichen Stelle u. a. über die Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung und die Kategorien von Empfängern zu unterrichten.
Der Vereinsvorsitzende führte in seiner Stellungnahme aus, dass nach der Satzung seines Verbandes eine Bezugspflicht des offiziellen Mitteilungsblattes, wie er es nannte, für die Mitglieder bestand. Aus dieser ergab sich auch, dass die Namen von bestimmten Mitgliedern in dem offiziellen Mitteilungsblatt jeweils zu veröffentlichen waren. Dies sei für den Verein wegen der besonderen Tätigkeit dieser Mitglieder wichtig. Auch wurde die Auffassung vertreten, dass es sich bei der Veröffentlichung um ein Presseerzeugnis handele und der TLfDI damit nicht zuständig sei.
Nach § 41 Abs. 1 BDSG i. V. m. § 11a Thüringer Pressegesetz (TPG) hat das Land Thüringen in seiner Gesetzgebung vorgesehen, dass für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten von Unternehmen und Hilfsunternehmen der Presse ausschließlich zu eigenen journalistisch-redaktionellen oder literarischen Zwecken den Vorschriften der §§ 5, 9 und 38a BDSG entsprechende Regelungen einschließlich einer hierauf bezogenen Haftungsregelung entsprechend § 7 BDSG zur Anwendung kommen. Als Normadressaten gelten daher Unternehmen oder Hilfsunternehmen der Presse. Um die grundrechtlich gewährleistete Pressefreiheit sicherzustellen, ist dabei zunächst von der Begriffsdefinition in Art. 5 Abs. 1 Satz 2 Grundgesetz auszugehen. Daher gilt das BDSG in seinen wesentlichen Teilen nicht, soweit die Datenverarbeitung vom Grundrecht der Pressefreiheit gedeckt ist. Ausgangspunkt ist daher der sogenannte formelle Pressebegriff, wonach die Art und der auf die Verarbeitung gerichtete Zweck, nicht der Inhalt oder die Qualität der Veröffentlichung entscheiden. Danach gehören in diesem formellen Sinn zur Presse alle mittels Buchdruckerpresse oder eines sonstigen zur Massenherstellung geeigneten Vervielfältigungsverfahrens hergestellten und zur Verarbeitung bestimmten Schriften, bespro-

chene Tonträger, bildliche Darstellungen mit und ohne Schrift und Musikalien mit Text oder Erläuterungen (vgl. *Dix* in Simitis, Kommentar zum BDSG, § 41 Rn. 9). Darunter fällt auch dieses offizielle Mitteilungsblatt des Vereins.

Als Unternehmen der Presse einzuordnen sind vor allem Zeitungs-, Zeitschriften und Buchverlage, aber auch selbstständige Journalisten. Dagegen können Presseabteilungen von Wirtschaftsunternehmen, Verbänden, Parteien usw., die Werks-, Kunden- oder Mitgliederzeitungen herausgeben, nur dann vom Medienprivileg profitieren, wenn sie eine von der übrigen Unternehmensverwaltung abgetrennte Organisationseinheit bilden. Eine solche abgetrennte Organisationseinheit war in diesem Fall der Verlag.

Nach § 41 Abs. 1 BDSG sind aus dem Anwendungsbereich des BDSG jedoch nur diejenigen Datenbestände der Medien, die ausschließlich zu eigenen journalistisch-redaktionellen Zwecken (im Gegensatz zur Veröffentlichung einer bloßen Auflistung von Informationen) verarbeitet oder genutzt werden, weitgehend herausgenommen. Erfasst sind hingegen die personenbezogenen Informationen, die von Journalisten, Redakteuren etc. zu Zwecken der Recherche sowie der Vorbereitung und Herstellung von zur Veröffentlichung bestimmten Artikeln, Sendungen oder sonstigen redaktionellen Texten entweder unmittelbar erhoben oder aus anderen Quellen beschafft werden. Neben einer journalistisch-redaktionellen Tätigkeit verlangt die Veröffentlichung für einen unbestimmten Personenkreis eine gewisse schöpferische, der öffentlichen Meinungsbildung dienende Leistung des Redakteurs, die eine planvolle inhaltliche, sprachliche oder grafische Bearbeitung beinhaltet (s. VGH München, Urteil vom 25. März 2015 – 5 B 14.2164). Eine solche Leistung liegt aber gerade hier in der Veröffentlichung von Mitgliederlisten samt Namen, Adressen und Telefonnummern **nicht** vor. § 41 BDSG und § 11a TPG forderten zudem eine Verarbeitung ausschließlich zu journalistisch-redaktionellen Zwecken.

Daran fehlte es in diesem Fall, weil weder der Vorstand noch eine andere Stelle innerhalb des Vereins oder des Verlags, deren sich der Verein zur Veröffentlichung des Mitteilungsblattes bediente, ausschließlich für die Verarbeitung von Informationen zu journalistisch-redaktionellen Zwecken tätig waren. Vielmehr verfolgte der Verein, wie ein Blick in die Satzung zeigte, die Zwecke des Vereins und nicht eine Tätigkeit im Pressewesen. Das hier vorliegende Vereinshandeln ist auf die Umsetzung der Satzung, insbesondere auf die

Nennung der Namen der Mitglieder, gerichtet, nicht jedoch auf die unternehmerische Tätigkeit der Herausgabe von Druckwerken. Das bloße Veröffentlichen von Information mit der vorgenannten Zielrichtung zu anderen Zwecken macht den Veröffentlichenden auch noch nicht zu einem Unternehmen der Presse. Denn dann müsste man jede politische Partei, jedes Wirtschaftsunternehmen und auch jede Privatperson als Presseunternehmen ansehen, wenn sie sich nur mittels einer Homepage mit Informationen über ihre Aktivitäten an die Allgemeinheit wendet (dazu Gola/Schomerus, BDSG, 12. Aufl. 2015, § 41 Rn. 10a).
Im Ergebnis fehlte es daher an einer Verarbeitung von Daten zu ausschließlich journalistisch-redaktionellen Zwecken. Der Zweck der Veröffentlichung lag in der Umsetzung der Vereinssatzung.
Daher war nach Auffassung des TLfDI das BDSG auch auf die Veröffentlichungen in der Zeitschrift anwendbar. Es bedurfte daher für die Verarbeitung und Nutzung, hier in Form der Veröffentlichung im offiziellen Mitteilungsblatt, der personenbezogenen Daten der Mitglieder einer Rechtsvorschrift, die dies erlaubte oder anordnete, oder der Einwilligung der Betroffenen, § 4 Abs. 1 BDSG. Seitens der von der Veröffentlichung betroffenen Mitglieder lagen keine solchen Einwilligungen in die Veröffentlichung ihrer personenbezogenen Daten vor.
Nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG ist das Speichern und Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt. Geschäftszweck im Sinne dieser Vorschrift ist dabei jeder Zweck einer privaten Stelle, also jeder Zweck, der sich nicht im ausschließlich persönlichen oder familiären Bereich bewegt. Geschäftszweck im Sinne der Vorschrift ist daher vorliegend der Vereinszweck. Als berechtigtes Interesse gemäß § 28 Abs. 1 Nr. 2 BDSG kommt jedes von der Rechtsordnung gebilligte Interesse infrage. Es genügt jedes Verlangen, das bei vernünftiger Erwägung durch die Sachlage gerechtfertigt ist. Ein solches berechtigtes Interesse hatte der Vereinsvorsitzende nicht vorgetragen.
Selbst wenn man ein solches berechtigtes Interesse angenommen hätte, hätte dieses im Sinne des § 28 Abs. 1 Satz 1 Nr. 2 BDSG auch erforderlich sein müssen. Erforderlich ist eine Datenverarbeitung

dann, wenn sie notwendig für die Erreichung der berechtigten Interessen ist. Es sprach Vieles dafür, dass es hier an der Erforderlichkeit der vorgenommenen Nutzung und Verarbeitung der personenbezogenen Daten der einzelnen Mitglieder fehlte. Es war nicht erkennbar, zu welchem Zweck und aus welchem Grund diese Personen mit Namen, Adressen und Telefonnummern in einem frei zugänglichen Papier veröffentlicht werden sollten. Hier überwogen ganz klar die Interessen der Betroffenen des Vereins.
Ein berechtigtes Interesse des Vereins daran, neben den Namen der Mitglieder noch deren Adressen und Telefonnummern konkret zu benennen, war auch nicht erkennbar.
Der TLfDI erwog als zuständige Aufsichtsbehörde, gegen den Hundeverband e. V. eine Anordnung zu erlassen, die zum Ziel hatte, die mit dem BDSG nicht zu vereinbarende Veröffentlichung bzw. Übermittlung der Mitgliederliste, wie der Verein sie zu dieser Zeit praktizierte, zu unterbinden.
Der Verein passte seine Satzung demensprechend an. Mit der Änderung der Satzung und deren Umsetzung in die Praxis erachtete der TLfDI das Verwaltungsverfahren für erledigt. Eine Veröffentlichung der Adressen und Telefonnummern wird nach den vorliegenden Informationen in der Zukunft unterbleiben. Es werden nunmehr nur der Name und eine dazugehörige Mitgliedsnummer veröffentlicht. Dies hielt der TLfDI unter Bezugnahme auf die Satzung der verantwortlichen Stelle für datenschutzrechtlich zulässig.

Das „Medienprivileg“, also die weitestgehende Nichtanwendbarkeit des BDSG auf Presseprodukte, gilt nur, soweit dabei ausschließlich redaktionelle oder journalistische Zwecke verfolgt werden. Sobald weitere Zwecke hinzukommen, ist das BDSG anwendbar.

4.4 Falscher Adressat TLfDI

Im Berichtszeitraum erhielt der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) eine schriftliche Anfrage eines Postzustellungsunternehmens. Das Unternehmen hat als Produkt eine sogenannte digitale Poststelle angeboten. So war es für die Kunden möglich, die gesamte Postausgangspost über den Anbieter in digitaler Form laufen zu lassen. Da dem Kundenstamm mehrere öffentliche Stellen nach dem § 2 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) angehörten, erkundigte sich das Unterneh-

men beim TLfDI, ob der TLfDI für datenschutzrechtliche Freigabeverfahren zuständig ist.
Beim erstmaligen Einsatz von automatisierten Verfahren, mit denen personenbezogene Daten verarbeitet werden, bedarf es hinsichtlich der Datenarten und der regelmäßigen Datenübermittlung der vorherigen schriftlichen Freigabe durch die Stelle, die den Datenschutz sicherzustellen hat, § 34 Abs. 2 ThürDSG. Diese Stellen sind jedoch nach § 34 Abs. 1 ThürDSG das zuständige Landesministerium, die Gemeinden und Gemeindeverbände oder sonstige der Aufsicht des Landes unterstehende juristische Personen des öffentlichen Rechts. Über ein automatisiertes Abrufverfahren gem. § 7 Abs. 1 ThürDSG, das die Übermittlung personenbezogener Daten durch Abruf ermöglicht, und über regelmäßige Datenübermittlungen gem. § 7 Abs. 7 ThürDSG ist nach § 7 Abs. 3 ThürDSG der Landesbeauftragte für den Datenschutz unter Mitteilung der Regelungen nach § 7 Abs. 2 ThürDSG vorher zu unterrichten. Ungeachtet der Tatsache, ob es sich bei den Postdienstleistungsunternehmen um ein automatisiertes Abrufverfahren oder eine regelmäßige Datenübermittlung handelt, kann eine Prüfung durch den TLfDI nur dann erfolgen, wenn dies im konkreten Anwendungsfall mit den notwendigen Angaben, hier im Rahmen einer Unterrichtung, vorgelegt wird. Das Unternehmen hatte sich nicht weiter an den TLfDI gewandt. Im Übrigen wäre der TLfDI auch nicht – wie oben dargestellt – für einen Antrag des Freigabeverfahrens vom Postzustellungsunternehmen zuständig gewesen. Somit war das Verfahren seitens des TLfDI beendet.

Eine pauschale Vorabbegutachtung einzelner Produkte des Unternehmens, losgelöst von einem Anwendungsfall, kann seitens des TLfDI nicht erfolgen, da auch das Freigabeverfahren an sich nicht vom TLfDI, sondern wie schon beschrieben von den zuständigen Stellen für die Sicherstellung des Datenschutzes durchgeführt wird und der TLfDI in diesem Zusammenhang nur davon unterrichtet wird und ggf. Hinweise erteilt.

4.5 Datenschutz bei der App-Entwicklung

Im Berichtszeitraum wurde dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) bekannt, dass ein Thüringer Unternehmen mit der Erstellung einer bundesweit eingesetzten sog. App (application software oder auch Anwendungs-

software, häufig im Bereich mobiler Betriebssysteme zu finden) beauftragt wurde, mithilfe derer eine Vielzahl von personenbezogenen Daten erhoben werden könne und diese Daten danach in einer Datenbank gespeichert und auch für verschiedene Anwendungsmöglichkeiten verarbeitet würden. Da durch den Einsatz einer App potenziell eine Vielzahl von Bürgern betroffen sein kann, war dem TLfDI daran gelegen, die genaue Funktionsweise dieser App zu hinterfragen und sicherzustellen, dass sie den datenschutzrechtlichen Anforderungen genügt. Dazu wurde ein Vor-Ort-Termin mit dem entwickelnden Unternehmen vereinbart und die Funktionsweise und Anwendungsmöglichkeiten vor Ort in Augenschein genommen sowie die technischen und organisatorischen Gegebenheiten genau erörtert. Ergänzend dazu wurde durch den TLfDI auch Kontakt zu den weiteren App-Verwendern aufgenommen und auch die Verwender ähnlicher Apps um Auskunft darüber gebeten. Die technischen Abläufe der Datenerhebung und -speicherung sowie die vertraglichen Grundlagen für diese Datenverarbeitungen werden durch den TLfDI derzeit geprüft und ausgewertet. Da aufgrund der komplexen Struktur der Datenverarbeitung noch Rückfragen beim Entwickler notwendig gewesen sind, liegt ein abschließendes Ergebnis der Prüfung noch nicht vor.

Gerade bei der flächendeckenden Nutzung von Anwendungssoftware besteht die Gefahr, dass es eine Vielzahl von Betroffenen gäbe, wenn diese Software datenschutzrechtliche Mängel aufweisen würde. Aus diesem Grund ist der TLfDI bestrebt, die technische Umsetzung derartiger Software-Lösungen direkt beim Entwickler zu hinterfragen und ggf. Nachbesserungen in der Umsetzung herbeizuführen.



Geschützte Daten – momius – fotolia.com

5 Meldungen nach § 42a

5.1 Leaks

Datenlecks, Datenpannen oder Datendiebstähle müssen unter bestimmten Voraussetzungen der zuständigen Aufsichtsbehörde, sprich: für Thüringen dem Thüringischen Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), sowie dem/den Betroffenen gemeldet werden.
Die Meldepflicht entsteht gemäß § 42a Bundesdatenschutzgesetz (BDSG), wenn bei der verantwortlichen Stelle gespeicherte, besonders sensitive Arten von Daten unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind. Zu den besonders sensitiven Arten von Daten gehören nachfolgende Datenkategorien:

1. besondere Arten personenbezogener Daten, hierunter fallen Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben (siehe § 3 Abs. 9 BDSG),

2. personenbezogene Daten, die einem Berufsgeheimnis unterliegen,
3. personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den Verdacht strafbarer Handlungen oder Ordnungswidrigkeiten beziehen und
4. personenbezogene Daten zu Bank- oder Kreditkartenkonten.

Jedoch greift die Pflicht nur, wenn für die Rechte oder schutzwürdigen Interessen der Betroffenen schwerwiegende Beeinträchtigungen drohen. Die verantwortliche Stelle muss eine Gefahrenprognose vornehmen. Dabei sind mögliche Folgen der Datenpanne zu identifizieren und im Hinblick auf die möglicherweise eintretenden Belastungen für den Betroffenen zu bewerten. Hierbei darf aber kein zu enger Maßstab angelegt werden, da bei den oben genannten Datenkategorien schon gute Gründe gegen eine solche schwerwiegende Beeinträchtigung vorliegen müssen. Der § 42a BDSG fordert weder erhebliche materielle Schäden noch erhebliche soziale Nachteile. Die Wahrscheinlichkeit, dass Daten veröffentlicht oder kriminell genutzt werden, reicht schon aus. Im Zweifel sollte die verantwortliche Stelle von einer Meldepflicht ausgehen.

Sofern ein solcher Schaden bereits vorgefallen ist, muss keine Abwägung mehr vorgenommen werden.

Die zuständige Aufsichtsbehörde ist unverzüglich über solch einen Vorfall zu informieren. Die Benachrichtigung des Betroffenen muss unverzüglich erfolgen, sobald angemessene Maßnahmen zur Sicherung der Daten ergriffen wurden und die Strafverfolgung nicht mehr gefährdet wird.

Um den Unternehmen die Einschätzung zu vereinfachen, hat der TLfDI eine Checkliste entwickelt. Diese ist auf der Homepage des TLfDI unter https://www.tlfdi.de/mam/tlfdi/info/checkliste_42bdsgneu.pdf zu finden.

Unter den im Berichtzeitraum gemeldeten Vorfällen findet sich beispielhaft Folgendes:

die Entwendung von externen Sicherungsfestplatten bei einem Einbruch in eine Arztpraxis und eine Vermisstenmeldung eines Speichermediums für Ultraschallbilder.

Problematisch war auch, dass Mitarbeiter

Unterlagen an ihre private E-Mail-Adressen verschickten, z. B. Unterlagen zu einem Kreditkartenantrag oder interne Bankgeschäftsunterlagen mit Dateianhängen (inkl. Kundendaten).
In einer weiteren Meldung wurde angezeigt, dass ein Mitarbeiter versehentlich ein ausgefülltes Formular namens „Selbstauskunft“ an einen anderen Kunden versendet hatte.
Darüber hinaus gab es eine Meldung, dass ein Überweisungsbriefkasten einer Bank aufgebrochen wurde.
Besonders prekär war die Veröffentlichung von sehr privaten Daten eines Kunden eines Berufsgeheimnisträgers auf der privaten Facebookseite einer Mitarbeiterin. Sie hatte die Informationen im Rahmen ihrer Tätigkeit aufgeschnappt und dann sofort in ihrem „Facebook-Freundeskreis“ verbreitet.

§ 42a BDSG verpflichtet nicht-öffentliche Stellen und öffentlich-rechtliche Wettbewerbsunternehmen, den TLfDI und die Betroffenen unverzüglich darüber zu informieren, wenn entsprechend sensible Daten (z. B. Gesundheitsdaten, Konto- und Kreditkarteninformationen) Dritten unrechtmäßig zur Kenntnis gelangt sind (z. B. durch einen Hackerangriff oder einen Diebstahl). Hierbei reicht es, wenn tatsächliche Anhaltspunkte vorliegen, dass unbefugte Dritte mit hoher Wahrscheinlichkeit Kenntnis von den Daten nehmen konnten. Die Meldung muss immer die Art der betroffenen Daten und die Erklärung des Vorfalls, warum die Daten abhandengekommen sind, enthalten. Dem Betroffenen müssen zudem Hilfestellungen aufgezeigt werden. Die Aufsichtsbehörde erhält zusätzlich eine Einschätzung zu den nachteiligen Folgen der unrechtmäßigen Kenntnisnahme und eine Nennung der bisher getroffenen Maßnahmen zur Verhinderung oder Minderung der Folgen (siehe auch o. g. Checkliste). Wer der gesetzlichen Verpflichtung nicht oder nicht rechtzeitig nachkommt, dem droht ein Bußgeld von bis zu 300.000 Euro gemäß § 43 Abs. 2 Nr. 7 BDSG.



Security Camera, CCTV on location, airport - ©alice_photo / Fotolia.com

6 Videoüberwachung

6.1 „1984“ war gestern!

George Orwell würde sich freuen. Vielleicht auch nicht. Nach kurzem Überlegen: Nein, er wäre vermutlich begeistert ob der technologischen Möglichkeiten und entsetzt über das Ausmaß der Überwachung in unserer heutigen Gesellschaft.
Denn: Die technologischen Möglichkeiten zur Überwachung sind weit über das hinausgewachsen, was in seinem ohnehin schon ausreichend beängstigendem Roman „1984“ möglich ist. Viele haben inzwischen Handys, die auf Befehl zuhören und das Gesagte zur Spracherkennung an irgendwelche Server senden, kleine Geräte, die im Wohnzimmer oder Schlafzimmer stehen und auf Zuruf neue Tabs für die Spülmaschine bestellen, allen voran die Videoüberwachung.
Videoüberwachung hat massiv zugenommen. Auch hier im Freistaat Thüringen. Teilweise wird diese von der Bevölkerung sogar begrüßt. Unterhält man sich mit Menschen, bekommt man in der Regel zu hören, es wäre schön, wenn jemand eingreifen könne, sobald etwas passiert. Ein möglicherweise schwerwiegender Irrtum. Nur ein verschwindend geringer Anteil von Videoüberwachungsanlagen ist technisch so ausgestaltet, dass es überhaupt möglich ist, das Gesche-

hen live zu beobachten. Noch ein viel geringerer Anteil dieser Anlagen ist mit jemandem besetzt, der tatsächlich zuschaut oder gar für Hilfe sorgt.
Tatsächlich zeichnen die Videoanlagen nur auf. Alles. Jeden Streit, jeden Kuss, jedes Popeln in der Nase. Eine präzisere Erfassung des menschlichen Verhaltens als das der Videoaufnahme ist kaum möglich. Eingreifen, wenn tatsächlich mal was passiert? Fehlanzeige. Zugegeben, die Aufklärung wird einfacher. Aber ist das Grund genug, um massenhaft Menschen, die sich anstandslos innerhalb der Gesellschaft bewegen, aufzuzeichnen? Dafür gibt es ein Wort: Vorratsdatenspeicherung. In anderem Zusammenhang wurde diese vom Europäischen Gerichtshof bereits mehrmals als rechtswidrig befunden. Trotz mehrerer Anläufe der Bundesregierung, diese umzusetzen. Und auch bei der Videoüberwachung ist im Zuge des internationalen Terrors der Versuch unternommen worden, Freiheitsrechte einzuschränken.
Zum datenschutzrechtlichen Problem wurde die Videoüberwachung erst, als die Technik günstig wurde. Inzwischen sind kleine Anlagen beim Discounter erhältlich. Eine Information über die rechtlichen Voraussetzungen der Videoüberwachung ist dort aber nicht inklusive.
Tatsächlich war die Videoüberwachung, wie auch in den vergangenen Berichtszeiträumen, eines der Schwerpunktthemen des Thüringer Landesbeauftragten für den Datenschutz und die Informationsrfreiheit. Alleine schon wegen der schieren Masse an rechtswidrigen Überwachungen. Der Gesetzgeber hat die Videoüberwachung nämlich an enge Voraussetzungen gebunden, die ein Betreiber von Videoüberwachungsanlagen eigenständig prüfen muss. Insbesondere sind Verfahren zur biometrischen Gesichtserkennung nur unter sehr engen Voraussetzungen zulässig und beim Einsatz von Videoüberwachungen von Privaten überwiegend nicht erforderlich. Zudem besteht hinsichtlich einer Videoüberwachung von nicht-öffentlichen Stellen eine Meldepflicht gemäß § 4d Abs. 1 BDSG (Urteil des VG Saarland vom 18. Mai 2016, Az. 1 K 63/15, nunmehr bestätigt durch Urteil des OVG Saarlouis vom 14. September 2017). Nur wenn die entsprechenden Voraussetzungen erfüllt sind, darf eine solche Anlage rechtmäßig genutzt werden. Sind die Voraussetzungen nicht erfüllt, droht hingegen ein Bußgeldverfahren. Nach derzeitigem Recht mit einer maximalen Bußgeldhöhe von 300.000 Euro.

Ab Ende Mai 2018, mit Geltung der Datenschutz-Grundverordnung erhöht sich dieses Bußgeld für rechtswidrige Datenerhebung auf maximal 20 Millionen Euro.
Auf den folgenden Seiten berichtet der TLfDI von einigen Fällen, die er im Berichtszeitraum geprüft hat.

6.2 Meldungen nicht nur von Wildkameras

In diesem Fall meldete ein privater Jäger das Betreiben einer Wildtierkamera in seinem eigenen Waldstück zum Verfahrensregister des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) an. Seit dem Urteil des *Verwaltungsgerichts Saarland vom 18. Mai 2016, Az.: 1 K 63/15* gilt für die private Jägerschaft und letztlich auch für alle nicht-öffentlichen Stellen, dass auch Wildtierkameras der Meldepflicht des § 4d Bundesdatenschutzgesetz (BDSG) unterliegen. Nach § 4d Abs. 1 BDSG sind Verfahren automatisierter Verarbeitungen vor ihrer Inbetriebnahme von nicht-öffentlichen verantwortlichen Stellen der zuständigen Aufsichtsbehörde nach Maßgabe von § 4e BDSG zu melden. Kameras, die Bilder oder Videoaufnahmen aufzeichnen und abspeichern, stellen eine solche automatisierte Datenverarbeitungsanlage dar, die personenbezogene Daten erhebt und meist zugleich verarbeitet, wenn die Aufnahmen gespeichert werden. Ausnahmen für die Meldepflicht bestehen nach § 4d Abs. 2 und 3 BDSG, wenn die verantwortliche Stelle einen Beauftragten für den Datenschutz bestellt hat. Darüber hinaus entfällt die Meldepflicht, wenn die verantwortliche Stelle personenbezogene Daten für sich erhebt, verarbeitet oder nutzt und dabei nicht mehr als neun Personen mit der Datenerhebung- bzw. -verarbeitung beschäftigt sind und eine Einwilligung der Betroffenen vorliegt oder die Datenerhebung für die Vertragsbegründung oder -durchführung erforderlich ist. Somit unterliegen **alle Videoüberwachungsanlagen von nicht-öffentlichen Stellen**, worunter natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts fallen (§ 2 Abs. 4 BDSG), **der Meldepflicht**, sofern kein Ausnahmetatbestand des § 4d BDSG eingreift, was bei einer Videoüberwachung zumeist nicht der Fall ist. Der Verantwortliche hat die von ihm betriebene Videoüberwachung **vor** der Inbetriebnahme der zuständigen Aufsichtsbehörde zu melden. Örtlich zuständig ist die Aufsichtsbehörde, in der die verantwortliche Stelle ihren Hauptgeschäftssitz hat. In Thüringen ist nach § 42

Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) i. V. m. § 38 Abs. 6 BDSG der Landesbeauftragte für den Datenschutz sachlich zuständige Aufsichtsbehörde für den nicht-öffentlichen Bereich. Zu melden sind nach § 4e Satz 2 i. V. m. § 4d BDSG auch Veränderungen und Beendigungen von bestehenden Verfahren. Grundsätzlich gibt es keine Formvorschrift für die abzugebende Meldung, jedoch hat sich in der Praxis die Schriftform durchgesetzt, d. h. mittels Schreibens oder entsprechenden Formulars. Der Inhalt dieser Meldung ergibt sich aus § 4e Satz 1 BDSG. Dort werden sämtliche erforderlichen Angaben aufgeführt. Der TLfDI hat auf seiner Homepage entsprechende Formulare, sowie Ausfüllhinweise für die verantwortlichen Stellen zur Verfügung gestellt:(https://www.tlfdi.de/mam/tlfdi/datenschutz/video/tlfdi_meldeformular_v__.pdf, https://www.tlfdi.de/mam/tlfdi/datenschutz/video/tlfdi_ausf__llhinweise_zum_meldeformular.pdf).

Die anschließende Aufnahme in das sog. Verfahrensregister bedeutet jedoch nicht, dass die Aufsichtsbehörde die Datenverarbeitung für zulässig erachtet. Es wird bei der Aufnahme lediglich die Vollständigkeit der Angaben überprüft. Die Aufsichtsbehörde ist durch die Meldung nicht gezwungen, diese auch auf die Rechtmäßigkeit der Datenverarbeitung hin zu überprüfen. Nach § 38 Abs. 2 BDSG ist sie lediglich verpflichtet, ordnungsgemäße Verfahren in das Verfahrensregister aufzunehmen. Im Umkehrschluss bedeutet dies aber auch, dass offensichtlich gegen die Datenschutzvorschriften verstoßende Datenverarbeitungen nicht in das Verfahrensregister aufzunehmen sind. Der TLfDI weist hier auch darauf hin, dass es sich bei einer nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig gemachten Meldung um einen Bußgeldtatbestand nach § 43 Abs. 1 Nr. 1 BDSG handelt. Hier kann der TLfDI ein Bußgeldverfahren einleiten.

Grundsätzlich sind von nicht-öffentlichen Stellen sämtliche automatisierte Datenverarbeitungen dem TLfDI zu melden, sofern die verantwortlichen Stellen ihren Hauptgeschäftssitz oder Wohnsitz in Thüringen haben und kein Ausnahmetatbestand nach § 4d Abs. 2 und 3 BDSG eingreift. Zu beachten ist insbesondere, dass die Meldung vor der Inbetriebnahme der Datenverarbeitungsanlage erfolgen

muss. Eine spätere Meldung kann ein Bußgeldverfahren nach sich ziehen. Der Inhalt der erforderlichen Angaben für die Meldung ergibt sich aus § 4e Satz 1 BDSG. Der TLfDI hat auf seiner Homepage entsprechende Formulare, sowie Ausfüllhinweise für die verantwortlichen Stellen zur Verfügung gestellt:(https://www.tlfdi.de/mam/tlfdi/datenschutz/video/tlfdi_meldeformular_v__.pdf, https://www.tlfdi.de/mam/tlfdi/datenschutz/video/tlfdi_ausf__llhinweise_zum_meldeformular.pdf).





6.3 Selbstbedienungsladen ohne Personal, aber mit problematischer Überwachungstechnik?

In Schweden gibt es ein Geschäftsmodell für den ländlichen Raum, das ohne Personal auskommt. Auch ohne Kassen. Kunden müssen sich lediglich registrieren lassen und eine App herunterladen. Über einen Fingerwisch und eine entsprechende Automatik öffnet sich dann die Tür. Die gekaufte Ware müssen die Kunden mit der Handykamera einscannen, gezahlt wird einmal im Monat per Handy-App oder mit EC-Karte. Würde das Konzept auch in Deutschland funktionieren? Ein Unternehmen aus Niedersachsen ist sich da ziemlich sicher. Vorreiter soll Thüringen mit 250 geplanten Standorten sein. Die beschriebenen Selbstbedienungsläden sollen 24 Stunden und sieben Tage die Woche betrieben werden. Aber: Wie schützt sich der Ladenbesitzer gegen unehrliche Kunden? Tatsächlich ist das offenbar ein schwieriges Thema. Die Antwort fängt beim Sortiment an: Das Geschäft führt keine besonders diebstahlgefährdeten Waren wie Zigaretten, Alkohol und Medikamente. Und sie hört bei der Videoüberwachung auf. Geplant waren zehn Kameras im Innen- und zwei Kameras im Außenbereich. Mit der Frage, ob diese Videoüberwachung zulässig sei, wandte sich das Unternehmen an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit

(TLfDI) als Datenschutzaufsicht für den privaten Bereich in Thüringen. Allerdings ist die Zuständigkeit des TLfDI noch nicht eindeutig feststehend. Das geplante Modell sollte zunächst in Thüringen ausgerollt werden. Es war jedoch noch nicht klar, welches Unternehmen sich in das Modell einkaufen und daher dann verantwortliche Stelle sein würde. Nur wenn die Videoüberwachung durch eine Stelle in Thüringen eigenverantwortlich durchgeführt wird, besteht eine Zuständigkeit des TLfDI für die datenschutzrechtliche Bewertung.
Der TLfDI überreichte daher zuerst einmal die „Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen“ des Düsseldorfer Kreises. Sie enthält die Anforderungen, die alle Aufsichtsbehörden in Deutschland an eine zulässige Videoüberwachung stellen und ist auch auf der Homepage des TLfDI unter https://www.tlfdi.de/mam/tlfdi/datenschutz/video/oh-v -durch-nicht- ffentliche-stellen.pdf veröffentlicht.
Sofern der TLfDI unter Berücksichtigung des oben Gesagten für die datenschutzrechtliche Beurteilung zuständig sein sollte, stellte sich die Situation nach den bislang vorliegenden Informationen wie folgt dar:
Sowohl im Hinblick auf die Videoüberwachung innerhalb der Selbstbedienungsläden als auch in Bezug auf die zwei Kameras am Eingang beurteilt sich die Zulässigkeit nach § 6b Bundesdatenschutzgesetz (BDSG), da es sich um öffentlich zugängliche Bereiche handelt. Der § 6b BDSG beinhaltet, dass die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) nur zulässig ist, soweit sie zur Aufgabenerfüllung öffentlicher Stellen, zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Zwar können in diesem Fall den Laden nur vorher registrierte Kunden betreten, die Registrierung ist aber grundsätzlich für jedermann möglich. Damit handelt es sich um einen öffentlich zugänglichen Raum. Da es zum Geschäftsmodell gehört, dass kein Servicepersonal vor Ort ist und sich die Kunden selbst im Laden bedienen und die Waren auch selbstständig vor Ort mit einer App oder mit EC-Karte bezahlen, besteht ein berechtigtes Interesse des Betreibers daran, dass das Geschäft videoüberwacht wird. So kann nachvollzogen werden, wenn

die Waren nicht bezahlt worden sind oder es kann reagiert werden, wenn es im Laden zu einem Vorkommnis kommt, sei es, dass es einem Kunden schlecht geht oder dass es zu einer Sachbeschädigung kommt. Die Aufnahmen sollen durch eine Servicestelle rund um die Uhr beobachtet werden. Die Erforderlichkeit ist auch für die Videoüberwachung des Eingangsbereiches gegeben, sofern der Erfassungsbereich der Kameras, wie vom zukünftigen Betreiber beabsichtigt, auf einen Bereich von einem Meter vor der Eingangstür beschränkt ist. Auf die Videoüberwachung muss darüber hinaus den Anforderungen des § 6b Abs. 2 BDSG entsprechend hingewiesen werden. Wichtig ist, dass sich auch ein Hinweis auf die verantwortliche Stelle findet.

Weiterhin ist sowohl bei der Datenspeicherung, beim Monitoring als auch bei der Fernwartung eine sichere Transportverschlüsselung entsprechend dem aktuellen Stand der Technik einzusetzen, sofern die Bilder an einer anderen Stelle eingesehen werden sollen.

Nach § 6b Abs. 5 BDSG sind die Daten unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen. Das ist der Fall, wenn eine Gefahr nicht mehr abgewendet werden muss oder eine Beweissicherung nicht notwendig ist. Ob eine Sicherung des Materials notwendig ist, dürfte grundsätzlich innerhalb von ein bis zwei Tagen geklärt werden können (vergleiche die Gesetzesbegründung, Bundestagsdrucksache 14/5793, Seite 63). In begründeten Einzelfällen kann eine längere Speicherdauer angenommen werden. Hier ist abzuwarten, ob Zugang zu den Selbstbedienungsläden auch am Wochenende gegeben sein wird.

Bevor die Videoüberwachungsanlage installiert wird, ist der betriebliche Datenschutzbeauftragte verpflichtet, eine Vorabkontrolle nach § 4d Abs. 5 BDSG durchzuführen, da die beabsichtigte Videoüberwachung zweifelsfrei besondere Risiken für die Rechte und Freiheiten der Kunden aufweist, die während des gesamten Einkaufs gefilmt werden. Nach der gesetzlichen Regelung darf ein Unternehmen ein automatisiertes Verfahren, das besondere Risiken für das Grundrecht auf informationelle Selbstbestimmung für den Betroffenen mit sich bringt, nur einsetzen, wenn der betriebliche DSB vorher überprüft hat, ob dieses Verfahren den Anforderungen des BDSG entspricht. Zu weiteren Einzelheiten und Festlegungen wurde empfohlen, sich mit der zuständigen Aufsichtsbehörde in Verbindung zu setzen,

sobald feststeht, welche Stelle für die Videoüberwachung verantwortlich ist. Im Zuge dessen kann auch geprüft werden, ob möglicherweise eine Einwilligung zu der Videoüberwachung im Container über die Allgemeinen Geschäftsbedingungen möglich ist. In die Videoüberwachung im Außenbereich kann nicht wirksam vorab eingewilligt werden, da sich auch Personen dem Container nähern werden, die die näheren Umstände der Videoüberwachung nicht kennen. Für sie ist keine informierte Einwilligung nach § 4a Abs. 1 Satz 2 BDSG möglich.

Eine geplante Videoüberwachung in einem Einkaufscontainer ohne Personal bedarf einer Vorabkontrolle nach § 4d Abs. 5 BDSG durch den betrieblichen Datenschutzbeauftragten der verantwortlichen Stelle. Eine Übersicht über die erforderlichen Prüfungen und Festlegungen bildet die „Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen“.

6.4 Rundumüberwachung einer Wohnungsanlage

Ein Beschwerdeführer wandte sich im Berichtszeitraum wegen einer Videoüberwachungsanlage, welche auf die öffentliche Straße gerichtet war, an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Dieser ermittelte zunächst den Eigentümer des Gebäudes, an dem die Videokameras angebracht waren. Eigentümer war eine thüringische Immobilienverwaltungsgesellschaft, welche dort auch ihre Geschäftsstelle und Mietwohnungen unterhielt. Der TLfDI wandte sich daraufhin mit einem Auskunftsersuchen an diese, um den Sachverhalt abschließend zu ermitteln.
An und in dem Gebäude waren insgesamt sechs Videokameras angebracht. Eine Videokamera befand sich im Wartebereich der Geschäftsstelle der Immobilienverwaltungsgesellschaft. Alle weiteren Kameras befanden sich im Außenbereich. Zwei Kameras bildeten den Parkplatzbereich am Haus ab. Eine weitere erfasste den Stellplatz für die Fahrräder und ein Stück des Gartenbereichs. Weiterhin bildete eine Kamera den Eingangsbereich der Geschäftsstelle ab, wobei der Bereich nur einen Meter ab der Hausfassade erfasst wurde. Der restliche Bereich war geschwärzt. Eine weitere war am Eckbereich des Gebäudes angebracht und bildete jeweils die Fassade des Gebäudes ab. Hier war ebenfalls lediglich ein Meter des Gehweges ab der Hauswand erfasst, der Rest wurde ausgeschwärzt. Die Kame-

ras wurden zur Abschreckung und Abwehr von potenziellenen Straftätern und Störern, zur Beweissicherung von Straftaten und zur Geltendmachung von Schadenersatzansprüchen installiert. Die Aufnahmen wurden für 72 Stunden auf einem Festplattenrecorder gespeichert.

Aufgrund des Beobachtens mit den Videokameras werden personenbezogene Daten erhoben und mittels Speicherung auf dem Festplattenrecorder gleichzeitig verarbeitet. Nach § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG) ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten zulässig, soweit das BDSG oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Zur Zulässigkeit der Videoüberwachung der nicht-öffentlichen Stellen haben die Datenschutzaufsichtsbehörden im Düsseldorfer Kreis eine Orientierungshilfe erarbeitet, welche der TLfDI auch auf seiner Website zur Verfügung stellt (https://www.tlfdi.de/mam/tlfdi/datenschutz/video/oh-v -durch-nicht- ffentliche-stellen.pdf).

Eine Rechtsvorschrift außerhalb des BDSG, welche die hier betriebene Videoüberwachung erlaubt, ist nicht ersichtlich. Auch eine Einwilligung nach § 4a Abs. 1 BDSG scheidet aus.

Die Zulässigkeit der betreffenden Videoüberwachungsanlage beurteilt sich mit Ausnahme der Kamera, welche den Fahrradständer und den Gartenbereich erfasst, vorliegend nach § 6b Abs. 1 Bundesdatenschutzgesetz (BDSG). Diese Bereiche sind als öffentlich zugänglich zu betrachten, da diese von jedermann betreten werden können und öffentlichen Raum wie den Gehweg erfassen. Für die Kamera in der Geschäftsstelle ist dies zumindest während der Geschäftszeiten zu bejahen. Danach ist eine Videoüberwachung in öffentlich zugänglichen Räumen zulässig, soweit sie zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Der angegebene Zweck – Abschreckung und Abwehr potenziellerer Straftäter sowie die Beweissicherung zu diesen Straftaten – wird nur dann seitens des TLfDI als berechtigtes Interesse anerkannt, wenn eine tatsächliche Gefahrenlage durch die verantwortliche Stelle

nachgewiesen werden kann. Dies kann durch Dokumentation der Vorkommnisse bzw. Nennung der polizeilichen Tagebuchnummern oder staatsanwaltschaftlichen Aktenzeichen geschehen. Im vorliegenden Fall hatte die verantwortliche Stelle hierzu keine Angaben gemacht. Zudem ist der Zweck sehr allgemein gefasst, hier müssten seitens der verantwortlichen Stelle konkretere Angaben gemacht werden, z. B. welche Straftaten hier im Besonderen abgewehrt werden sollen. Nur so ist die Geeignetheit der einzelnen Kameras zu beurteilen, um die Erforderlichkeit feststellen zu können. Eine Erforderlichkeit für das Betreiben der Videokameras ist nur dann zu bejahen, wenn diese für den konkret festgelegten Zweck geeignet sind und keine milderen Mittel zur Erreichung des Zwecks bei gleicher Effektivität vorhanden sind. Im vorliegenden Fall bestanden bei der Kamera im Wartebereich und auf dem Parkplatz Bedenken hinsichtlich der Geeignetheit für den jeweiligen Zweck, denn es wird nicht ersichtlich, welche Straftaten dort tatsächlich abgewehrt werden sollen. Zudem bestehen Anhaltspunkte, dass schutzwürdige Interessen von Betroffenen das berechtigte Interesse am Betreiben der Videoüberwachung überwiegen. Insbesondere im Wartebereich halten sich Personen typischerweise länger auf oder kommunizieren miteinander. In einem solchen Bereich kann der einzelne Bürger erwarten, nicht überwacht zu werden. Darüber hinaus wurden auf dem Parkplatz eine Vielzahl von dort parkenden Pkw und damit Personen erfasst. Ferner sind die Bewohner und Besucher der Immobilienverwaltungsgesellschaft auf die Nutzung des Parkplatzes angewiesen und können der Videoüberwachung nicht ausweichen.

Hinsichtlich der Kamera, welche auf die Fahrradständer und einen Teil des Gartenbereichs ausgerichtet ist, handelt es sich um einen nicht-öffentlichen Bereich, welcher nur von den Bewohnern des Hauses betreten werden kann. Die Zulässigkeit der dort angebrachten Kamera richtet sich dann nach § 28 Abs. 1 Nr. 2 BDSG, wonach die Datenerhebung und -verarbeitung sowie Nutzung als Mittel zur Erfüllung eigener Geschäftszwecke zulässig ist, soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass schutzwürdige Interessen der Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegen. Insofern gilt das bereits im Rahmen der Prüfung von § 6b BDSG Gesagte. Auch hier ergeben sich Bedenken hinsichtlich der Geeignetheit für den genannten Zweck. Durch die verantwortliche Stelle muss hier genau konkretisiert werden, welche

Straftaten in diesem Bereich verhindert oder aufgeklärt werden sollen. Die Vorkommnisse aus der Vergangenheit können hier als Grundlage herangezogen werden.
Die Kameras, welche lediglich die Hauswand und einen Meter des Gehweges erfassten, waren datenschutzrechtlich als unbedenklich einzustufen, da diese gem. § 6 Abs. 1 Nr. 2 BDSG im Rahmen der Wahrnehmung des Hausrechts als zulässig zu betrachten sind.
Der TLfDI teilte der verantwortlichen Stelle seine Rechtsauffassung betreffend der betriebenen Videoüberwachungsanlage mit. Das Verwaltungsverfahren ist noch nicht beendet, sodass voraussichtlich in dem nächsten Tätigkeitsbericht über den Abschluss des Verfahrens berichtet werden wird.

Jede Entscheidung über eine Videoüberwachungsanlage ist eine Einzelfallentscheidung. Die einzelnen Kameras sind immer anhand des konkret festgelegten Zwecks zu beurteilen. Insbesondere die Erforderlichkeit der einzelnen Kamera kann nur so geprüft werden. Im vorliegenden Fall konnte noch keine abschließende Entscheidung getroffen werden, da weder ein berechtigtes Interesse am Betreiben der Kameras nachgewiesen wurde, noch konnte die Geeignetheit der betreffenden Kameras aufgrund des unkonkreten Zwecks abschließend bejaht werden. Die verantwortlichen Stellen sollten sich über diese Bereiche der Videoüberwachung genaue Gedanken machen und diese Festlegungen auch schriftlich zur Dokumentation festhalten. Die durch die Datenschutzaufsichtsbehörden erarbeitete „Orientierungshilfe Videoüberwachung für nicht-öffentliche Stellen“ wird auf der Website des TLfDI (https://www.tlfdi.de/mam/tlfdi/datenschutz/video/oh-v__-durch-nicht-__ffentliche-stellen.pdf) als Information und Hinweis bereitgestellt. Die hier genannten Schwerpunkte werden dort ausführlich dargestellt.

6.5 Video versus Vandalismus – Videogaga?

Im Rahmen seiner aufsichtsbehördlichen Tätigkeiten ist der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) darauf aufmerksam gemacht worden, dass in direkter Nachbarschaft des Beschwerdeführers um 360° schwenkbare Kameras installiert worden seien, die beim Betreten und Verlassen des überwachten Bereiches Personen aufzeichneten. Diejenigen, die diesen Ort passierten – vor allem Mieter – seien von der Überwachung betroffen. Auch Fahrzeuge, die die öffentliche Straße in diesem Bereich nutzen, seien im Fokus der Aufnahmen.
Der TLfDI hat sich daraufhin mit einem Auskunftsverlangen nach § 38 Abs. 3 Bundesdatenschutzgesetz (BDSG) an die Beschwerdegegnerin gewandt und um die Beantwortung eines Fragenkataloges gebeten.
Zunächst berichtete die Beschwerdegegnerin in ihrer Antwort vom Anlass, der zur Objektüberwachung geführte habe. Seit etwa zwei Jahren hätten sich auf dem Objekt Sachbeschädigungsdelikte gehäuft und es sei dort vermehrt zu Verstößen gegen das Betäubungsmittelgesetz gekommen. Im Einzelnen seien gesteigert Fassadenteile beschmiert, Schaufenster der ansässigen Gewerbetreibenden verunstaltet und wiederholt Mülltonnen in Brand gesetzt worden. Einige der schwer einsehbaren Nischen auf dem Areal, wie z. B. die Garageneinfahrten und die Treppenaufgänge, seien von Unbekannten immer wieder für ihren Drogenkonsum genutzt worden. Insgesamt habe sich im Jahre 2014 eine Situation auf dem Areal dargestellt, die ein Verwahrlosen des Objektes ernsthaft befürchten ließ und zur zunehmenden Unsicherheit der Bewohner geführt habe. Um dem entgegenzuwirken, wäre das Ergreifen geeigneter Maßnahmen erforderlich gewesen. Zu diesem Zwecke sei ein Kamerasystem installiert worden, welches spürbar zu einem Rückgang an Straftaten geführt habe.
Den vom TLfDI zur Beantwortung gestellten Fragenkatalog indes konnte die Beschwerdegegnerin nur unzureichend beantworten, sodass der TLfDI in großem Maße Nachbesserungsbedarf sah, den er im Nachfolgenden präzisierte.
Zu den einzelnen Kameras hatte sie, wie dargelegt, lediglich angegeben, dass sich auf dem Objektareal Sachbeschädigungsdelikte und Verstöße gegen das Betäubungsmittelgesetz gehäuft hätten.

Nach § 6b Abs. 1 BDSG ist das Beobachten öffentlich zugänglicher Räume per Videoüberwachung unter anderem zulässig, soweit es zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte für das Vorliegen schutzwürdiger Interessen der betroffenen Personen bestehen. Ein berechtigtes Interesse für den Betrieb einer Videoüberwachungsanlage kann ideeller, wirtschaftlicher oder rechtlicher Natur sein. Soll die Videoüberwachung dazu eingesetzt werden, vor Einbrüchen, Diebstählen oder Vandalismus zu schützen, ist darin grundsätzlich ein berechtigtes Interesse zu sehen, wenn eine tatsächliche Gefahrenlage nachgewiesen wird. Zu fordern sind konkrete Tatsachen, aus denen sich eine Gefährdung ergibt.
Der TLfDI bat in diesem Zusammenhang die Beschwerdegegnerin um Übermittlung von Nachweisen zu den von ihr erwähnten Vorfällen. Dies können beispielsweise Aktenzeichen von Anzeigen bei der Polizei oder auch bezahlte Rechnungen von Reparaturen sein.
§ 6b Abs. 1 Nr. 3 BDSG sieht vor, dass die mit der Kameraüberwachung verfolgten Zwecke konkret festgelegt werden. Das bedeutet, dass es für jede Kamera einer Festlegung bedarf, für welchen Zweck sie betrieben wird. Der TLfDI bat die Beschwerdegegnerin insoweit um Vorlage schriftlicher Festlegungen zu jeder Kamera mit Ausführungen dazu, warum die Kamera mit ihrem jeweiligen Aufnahmebereich für den verfolgten Zweck erforderlich ist.
In ihrer Rückantwort äußerte die Beschwerdegegnerin zunächst, dass mittlerweile – auf Hinweis des TLfDI – Hinweisschilder angebracht und die Speicherung auf 48 Stunden beschränkt worden seien.
Es hätte in der Vergangenheit, wie bereits dargelegt, zahlreiche Fälle von Graffiti-Schmierereien vor allem im Bereich der Gewerbeeinheiten gegeben. Zudem seien die Glasscheiben des Objekts der Beschwerdeführerin in diversen Fällen beschädigt worden, was stets zu teils kostenaufwendigen Reparaturen geführt habe. Diese Schäden seien jeweils, soweit bekannt, der Versicherung gemeldet worden.
Aktuell würden weitere Informationen hierzu zusammengetragen und dann an den TLfDI umgehend weitergeleitet werden.
Jede einzelne Kamera diene dem Zweck, Vandalismus-Schäden zu verhindern.
Eine Weiterbearbeitung der Akte wurde obsolet, als dem TLfDI mitgeteilt wurde, dass das streitgegenständliche Objekt veräußert worden war. Im Zuge dieser Veräußerung wurden die streitgegenständlichen Kameras entfernt.

Ein berechtigtes Interesse für den Betrieb einer Videoüberwachungsanlage kann ideeller, wirtschaftlicher oder rechtlicher Natur sein. Soll die Videoüberwachung dazu eingesetzt werden, vor Einbrüchen, Diebstählen oder Vandalismus zu schützen, ist darin grundsätzlich ein berechtigtes Interesse zu sehen, wenn eine tatsächliche Gefahrenlage nachgewiesen wird. Zu fordern sind konkrete Tatsachen, aus denen sich eine Gefährdung ergibt.

6.6 Pizza mit Draufsicht – Videogaga 1

Im Rahmen der Prüfung einer Sondernutzungserlaubnis für einen Biergarten wurde durch die zuständige Dienststelle einer Stadtverwaltung festgestellt, dass zwei kameraähnliche Gegenstände beidseitig am Bogen des Eingangsportals montiert waren. Die Kameras waren jeweils auf die links und rechts des Einganges befindlichen Stühle und Tische ausgerichtet. Ergänzend wurde noch mitgeteilt, dass durch die Erteilung einer Sondernutzungserlaubnis die Fläche nicht entwidmet worden war, sondern weiterhin der Öffentlichkeit zur Verfügung stand. Die Stadtverwaltung übergab den Fall zuständigkeitshalber dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI).
Der TLfDI verschaffte sich bei einer ersten Vor-Ort-Kontrolle einen Überblick. Zwei Kameras waren jeweils im Torbogen angebracht und auf einen großen öffentlichen Platz gerichtet. Es wird auch auf einem Display der Aufzeichnungsbereich gezeigt. Dabei konnte man erkennen, dass weite Teile des Gastraums sowie des Arbeitsbereiches (Küche) durch Kameras überwacht wurden. Insgesamt waren fünf Kameras im Einsatz.
Im Rahmen eines Auskunftsverlangens nach § 38 Abs. 3 Bundesdatenschutzgesetz (BDSG) stellte der TLfDI im Nachgang zu der Vor-Ort-Kontrolle verschiedene Fragen zur durch den Geschäftsführer der Restaurant GmbH betriebenen Videoüberwachungsanlage. Folgende rechtliche Beurteilung erging an den Betreiber: Die von der Restaurant GmbH betriebene Videoüberwachungsanlage ist derzeit insgesamt nicht mit dem BDSG vereinbar und wird damit rechtswidrig betrieben. Der Umgang mit personenbezogenen Daten steht unter einem sogenannten Verbot mit Erlaubnisvorbehalt. Dies bedeutet, dass die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig ist, wenn das BDSG oder eine andere Rechtsvor-

schrift dies erlaubt, anordnet oder der Betroffene eingewilligt hat, § 4 Abs. 1 BDSG.
Durch eine Videoüberwachungsanlage werden personenbezogene Daten erhoben und meist auch verarbeitet.
Eine Einwilligung scheidet in Fällen von Videoüberwachung regelmäßig aus, da sie grundsätzlich schriftlich und vor Datenerhebung bzw. -verarbeitung einzuholen ist. Soweit von der hier gegenständlichen Videoüberwachung auch Mitarbeiter betroffen waren, schied eine Einwilligung ebenfalls aus. Eine solche war ohnehin nur unter äußerst engen Voraussetzungen möglich, da hier in der Regel die für die Einwilligung notwendige Freiwilligkeit fehlte. Eine solche Freiwilligkeit kann nur dann gegeben sein, wenn dem Arbeitnehmer echte Alternativen zu einer Einwilligung aufgezeigt werden und dieser auch ohne eine solche seinen Arbeitspflichten nachkommen kann. Hier musste der videoüberwachte Bereich zwingend von den einzelnen Mitarbeitern betreten werden, weswegen es von vornhinein an der verlangten Freiwilligkeit mangelte, da keine Alternativen zur Verfügung standen.
Hinsichtlich der fünf betriebenen Videokameras war keine gesetzliche Grundlage für den Datenumgang ersichtlich. Als Erlaubnisnorm kam ausschließlich § 6b BDSG in Betracht, da es sich sowohl beim Gastraum eines Restaurants, als auch bei der videoüberwachten Fläche vor dem Restaurant um einen öffentlich zugänglichen Raum handelte und diese spezielle und abschließende Regelung daher den übrigen Regelungen vorging. Zu prüfen war, ob die Videoüberwachung zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich war und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Der Betreiber hatte angeben, dass die Beobachtung und Aufzeichnung zum Eigenschutz gegen Vandalismus und Diebstahl erfolgte, wobei er sodann detailliert ausführte, dass es für Ermittlungen in diesen Bereichen notwendig ist, entsprechende verwertbare Beweise zu schaffen. Dem konnte entnommen werden, dass der von ihm verfolgte Zweck der Videoüberwachung in der Verfolgung zivil- und strafrechtlicher Interessen lag. Diese sind ausschließlich im Rahmen der Voraussetzungen des § 6b Abs. 1 Nr. 3 BDSG zulässig, also zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke.
Zwei der Kameras beobachteten weite Teile des öffentlichen Platzes der Innenstadt. Die Beobachtung dieser Bereiche war für die ange-

gebenen Zwecke nicht erforderlich. Außerdem gab es Anhaltspunkte, dass schutzwürdige Interessen Betroffener überwogen. Es handelte es sich um einen Platz, der tagsüber von einer unbestimmbaren Anzahl an Personen frequentiert wurde. Das Interesse dieser Personen, nicht in den Aufzeichnungsbereich der Kameras zu gelangen, überwog, weil sie unter Berücksichtigung des Zwecks der Videoüberwachung zu ihr in keiner Weise Anlass gegeben haben.
Auch im Fall der Kamera im Eingangsbereich waren deutliche Anhaltspunkte vorhanden, dass schutzwürdige Interessen Betroffener überwogen. Aufgezeichnet wurde nicht nur der Eingang des Restaurants, sondern ebenfalls eine Vielzahl an Sitz- und Stehgelegenheiten im Biergarten. Dieser Bereich diente zur Entspannung und Erholung sowie sonstigen Freizeitgestaltung. Das schutzwürdige Interesse der Gäste an einer unbeobachteten Freizeitgestaltung überwog aber das Interesse an einer dauerhaften Beobachtung der Gäste in den Sitzbereichen.
Hinsichtlich der Kamera, die den Zugang zur Toilette des Lokals und einen Zugang zum Notausgang beobachte, war nicht ersichtlich, inwieweit durch diese Beobachtung dem Schutz vor einer Verletzung seines Eigentums durch Diebstahl und Vandalismus gedient werden sollte. Hier fehlte es an der Erforderlichkeit für die festgelegten Zwecke.
Letztlich verblieb die Kamera, die die Kochzeile beobachtete. Betroffene der Videoüberwachung waren ausschließlich die Arbeitnehmer. Im Ergebnis handelte es sich um eine Arbeitnehmerüberwachung. Diese ist nur unter der Maßgabe des § 32 Abs. 1 Satz 1 BDSG zulässig. Die Voraussetzungen der nach § 32 Abs. 1 Satz 1 BDSG zulässigen Arbeitnehmerüberwachung waren ebenfalls nicht erfüllt. Eine rein präventive Videoüberwachung ohne konkrete Anhaltspunkte für ein strafbares Verhalten von Mitarbeitern genügt den Anforderungen von § 32 Abs. 1 Satz 1 BDSG nicht (Seifert in Simitis, § 32 Rn. 80).
Nachdem der Betreiber die Videokameras am Eingang abmontiert, die Kameras im Gebäude mit Farbe unbrauchbar gemacht (Linse überstrichen) sowie den Bildschirm entfernt hatte, war das Verfahren beim TLfDI abgeschlossen. Dies wurde auch der zuständigen Stadtverwaltung mitgeteilt.

Der Umgang mit personenbezogenen Daten steht unter einem sogenannten Verbot mit Erlaubnisvorbehalt. Dies bedeutet, dass die Er-

hebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig ist, wenn das BDSG oder eine andere Rechtsvorschrift dies erlaubt, anordnet oder der Betroffene eingewilligt hat, § 4 Abs. 1 BDSG. Das schutzwürdige Interesse der Gäste an einer unbeobachteten Freizeitgestaltung überwiegt grundsätzlich das Interesse an einer dauerhaften Beobachtung der Gäste in den Sitzbereichen einer Gaststätte.

6.7 Big Brother auf dem Marktplatz – Videogaga 2

Im Berichtszeitraum wandte sich ein Bürger an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) wegen einer Videoüberwachung an einem alten Einkaufsmarkt, die laut dessen Angaben auf den Marktplatz in einer thüringischen Stadt gerichtet war. Er fühlte sich beobachtet und bat um das Einschreiten des TLfDI. Da der TLfDI nach § 42 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) i. V. m. § 38 Abs. 6 Bundesdatenschutzgesetz (BDSG) sachlich zuständige Behörde zur Kontrolle der Ausführungen des BDSG ist, ging er dieser Anzeige im Rahmen seiner aufsichtsbehördlichen Tätigkeit nach.
Zunächst wurde beim zuständigen Gewerbeamt der Eigentümer des Gebäudes, an dem die Kamera installiert wurde, ermittelt. Dieser kam zunächst als verantwortliche Stelle gem. § 3 Abs. 7 BDSG in Betracht. Aufgrund dieser Angaben wandte sich der TLfDI mit einem Auskunftsersuchen an den Eigentümer. Insbesondere wurde gefragt, ob überhaupt eine Videokamera installiert sei, da es regelmäßig vorkommt, dass sich Bürger über Videoüberwachungsanlagen beschweren und es sich nach – zeitraubenden – Ermittlungen herausstellt, dass es sich nur um einen Bewegungsmelder handelt, der das Licht einschalten soll. In diesem Fall bestätigte sich die Videoüberwachungsanlage.
Wenn eine Videokamera installiert ist, gilt es zu prüfen, welche gesetzlichen Regelungen Anwendung finden und ob diese eingehalten worden sind.
Das Erheben, Verarbeiten und Nutzen von personenbezogenen Daten ist nämlich nach § 4 Abs. 1 BDSG grundsätzlich unzulässig, es sei denn, es gibt eine Erlaubnisnorm in oder außerhalb des BDSG oder der Betroffene hat in die Datenerhebung bzw. -verarbeitung eingewilligt.

Eine Einwilligung im Bereich der Videoüberwachung kommt nur in seltenen Ausnahmefällen in Betracht, da diese nach § 4 a Abs. 1 BDSG schriftlich und vor Erhebung der personenbezogenen Daten vorliegen muss. Diese strengen Voraussetzungen sind für die Betreiber der Videoüberwachung praktisch nicht umsetzbar, da der Betroffene zumeist vor Erteilung der Einwilligung bereits durch die Kameras aufgenommen wird und vor allem der Kreis der Betroffenen überhaupt nicht einzugrenzen ist. Als Erlaubnisnorm kommt hier § 6b BDSG in Betracht, welcher die Zulässigkeit der Beobachtung von öffentlich zugänglichen Räumen mit optisch-elektronischen Einrichtungen abschließend regelt. Öffentlich zugängliche Räume sind Bereiche innerhalb oder außerhalb von Gebäuden, die nach dem erkennbaren Willen des Berechtigten von jedermann genutzt oder betreten werden dürfen.
Im vorliegenden Fall war nach Mitteilung durch den Bürger nicht von vornherein auszuschließen, dass öffentlicher Raum seitens des Eigentümers überwacht wurde. Dann ist für diesen Bereich die Videobeobachtung nur zulässig, soweit sie zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke der verantwortlichen Stelle erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen, § 6b BDSG. Der Gebäudeeigentümer teilte dem TLfDI zur Beantwortung des Auskunftsersuchens mit, dass er eine Videoüberwachungsanlage installiert habe. Als Interesse gab der Eigentümer an, evtl. Einbrüchen, Diebstählen, Vandalismus und Brandstiftungen zu begegnen. Dies könnte zwar ein berechtigtes Interesse für die Installation einer Videokamera darstellen, jedoch muss von der verantwortlichen Stelle der Nachweis einer tatsächlichen Gefahrenlage verlangt werden. Diesen Umstand konnte der Eigentümer durchaus darstellen, denn es war zu einer Brandstiftung und einem Einbruch in den Räumlichkeiten einer dort befindlichen vermieteten Bar gekommen. Auch in der direkten Nachbarschaft war es zu Brandstiftungen und einem Raubüberfall gekommen.
Im Rahmen einer Videoüberwachung sind gemäß § 9 BDSG allerdings auch technisch-organisatorische Maßnahmen zu treffen, welche die Sicherheit der Verarbeitung personenbezogener Daten gewährleisten. Entsprechende Maßnahmen sind in Anlage 1 zu § 9 BDSG aufgezählt. Ob in diesem Fall tatsächlich öffentlich zugänglicher Raum durch die Videoüberwachung erfasst wird, wird derzeit geprüft. Die Auswertung hierzu steht jedoch noch aus, sodass über

den Abschluss des Verwaltungsverfahrens voraussichtlich erst im kommenden Tätigkeitsbericht berichtet werden wird.

Das Erheben, Verarbeiten und Nutzen von personenbezogenen Daten ist nach § 4 Abs. 1 BDSG grundsätzlich unzulässig, es sei denn, es gibt eine Erlaubnisnorm in oder außerhalb des BDSG oder der Betroffene hat eine Einwilligung erteilt. Im Rahmen von Videoüberwachungen kommt für öffentlich zugängliche Räume nur § 6b BDSG als Erlaubnisnorm in Betracht. Öffentlich zugängliche Räume sind Bereiche innerhalb oder außerhalb von Gebäuden, die nach dem erkennbaren Willen des Berechtigten von jedermann genutzt oder betreten werden dürfen. Auf private Eigentums- oder Besitzverhältnisse kommt es hingegen nicht an.

6.8 Videoüberwachung auf Firmengelände – Videogaga 3

Im Berichtszeitraum erhielt der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) eine Anfrage einer Stadtverwaltung. Ein Bürger hatte sich dort über eine Firma beschwert, die eine Kamera an einem Beleuchtungsmast auf ihrem Grundstück installiert hatte und damit auch die am Firmengrundstück vorbeiführende Straße nebst Gehweg als öffentliche Verkehrsfläche überwache. Die Stadtverwaltung wollte sich nun erkundigen, ob die Kamera durch den TLfDI genehmigt worden sei.
Dem TLfDI lagen keine Informationen zu einer solchen Kamera vor, weswegen er sich mittels eines Auskunftsersuchens an den Geschäftsführer der Firma wandte, um die Zulässigkeit der installierten Kamera zu prüfen. Dabei machte er darauf aufmerksam, dass das Erheben, Verarbeiten und Nutzen von personenbezogenen Daten nach § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG) grundsätzlich unzulässig sei, es sei denn, es gibt eine Erlaubnisnorm in oder außerhalb des BDSG oder der Betroffene hat in den Vorgang eingewilligt. Öffentliche Verkehrsflächen sind öffentlich zugängliche Räume. Die Beobachtung und erst recht die Verarbeitung oder Nutzung der erhobenen Daten ist nur in engen Grenzen zulässig und zwar nur dann, wenn die Überwachung zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen, § 6b Abs. 1 BDSG. Darüber hinaus sind der Umstand der Beobachtung und die verant-

wortliche Stelle durch geeignete Maßnahmen erkennbar zu machen, § 6b Abs. 2 BDSG.
Der Geschäftsführer des Unternehmens erklärte, dass der Aufnahmebereich dieser Kamera weder die Straße noch den entlangführenden Weg erfassen würde und wies dies mit Screenshots des Aufnahmebereichs nach. Außerdem seien Hinweisschilder angebracht worden. Er fügte einen Lageplan der Kameras bei und informierte den TLfDI, dass sich noch weitere Kameras auf dem Grundstück befinden. Die Kameraaufzeichnungen würden nach einer Woche überschrieben und damit gelöscht.
Einige Fragen blieben allerdings unbeantwortet. Zum Beispiel ist zur Beurteilung der Zulässigkeit die Angabe des Zwecks der Kameras notwendig. Darüber hinaus müsse der TLfDI erfahren, in welche Aufnahmebereiche die Kunden der Firma Zutritt haben und ob auch Bereiche überwacht werden in der´nen sich dauerhaft Arbeitnehmer aufhalten.
Im weiteren Verlauf teilte die Firma mit, der Zweck der Kameras sei die Wahrung des Hausrechts nach § 6b Abs. 1 BDSG. Die Kameras am Firmengebäude seien ausschließlich zur Sicherung des Gebäudes außerhalb der Geschäftszeiten, insbesondere gegen Einbruch, Diebstahl und Vandalismus, installiert. Schließlich habe es in dem Gewerbegebiet schon mehrfach und in unmittelbarer Nachbarschaft Einbrüche gegeben. Trotz Kameras habe man ergänzend einen Wachdienst beauftragt, der zudem zu bestimmten Zeiten das Objekt kontrolliere. Zur Betroffenheit von Mitarbeitern erläuterte der Geschäftsführer, dass ein dauerhafter Aufenthalt von Mitarbeitern im Kamerabereich ausgeschlossen sei, da die Kameras nur außerhalb der Geschäftszeiten aktiv seien und während der Geschäftszeiten keine Aufnahme stattfinde. Um sich ein genaueres Bild von den Kameras und deren Aufnahmebereichen zu machen, entschied der TLfDI, eine Kontrolle vor Ort durchzuführen.
Dabei wurde festgestellt, dass die Kamera an dem Lichtmast, auf die sich der Beschwerdeführer bezog, so eingestellt war, dass der öffentliche Weg nicht erfasst wurde und sie nur auf das Betriebsgrundstück gerichtet ist. Der von der Firma angegebene Zweck zur Wahrung des Hausrechts rechtfertigt dort eine Videoaufzeichnung, allerdings nur außerhalb der Geschäftszeiten. Ebenfalls nur außerhalb der Geschäftszeiten zulässig war eine auf eine Eingangstür gerichtete Kamera, in deren unmittelbarer Nähe ein Aschenbecher angebracht war,

weil dieser Bereich offenbar von den Mitarbeitern als Raucherbereich genutzt wurde.
Bei einer weiteren Kamera im Empfangsbereich innerhalb des Gebäudes war der Arbeitsplatz der Sekretärin ausgepixelt. Erfasst wurden jedoch die gläserne Haupteingangstür von innen und der Wartebereich für Besucher. Zur Zeit der Kontrolle war bei der Kamera die ständige Aufzeichnung aktiviert. Der TLfDI sah die Kameraüberwachung dann als entbehrlich an, wenn der Empfang besetzt ist. Ist der Platz nicht besetzt, kann eine Videoüberwachung erforderlich sein, da dann der freie Zugang zu mehreren Büros möglich ist.
Die Firmenleitung erwog darüber hinaus, eine weitere Kamera im Lagergebäude zu installieren. Diese würde dann Mitarbeiter und Lieferanten erfassen, um Diebstähle oder Verwechslungen der dort gelagerten Ware bzw. eine irrtümliche Mitnahme aufklären zu können. Die Mitarbeiter seien damit einverstanden. Hierzu wurde dem Geschäftsführer erläutert, dass die Einwilligung der Mitarbeiter die beabsichtigte Videoüberwachung mangels Freiwilligkeit nicht rechtfertigen kann. Auch für diese Videoüberwachung wurde keine Rechtsgrundlage gesehen, da es sich um einen Fall der Mitarbeiterüberwachung handelt, die Voraussetzung des § 32 BDSG jedoch nicht erfüllt ist. Auch aus § 28 BDSG kann eine Zulässigkeit der Videoüberwachung nicht angenommen werden, da davon auszugehen ist, dass schutzwürdige Interessen der Mitarbeiter überwiegen.
Nach § 6b Abs. 5 BDSG sind die Daten der Videoüberwachung unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen. Ob eine Sichtung des Materials notwendig ist, sollte innerhalb von zwei Tagen geklärt werden können. Die Firmenleitung sah jedoch eine längere Speicherung der Daten als notwendig an, da der Firmensitz an Wochenenden und über Feiertage länger als 48 Stunden unbesetzt sein kann. Der TLfDI hielt deswegen eine Speicherdauer von drei Tagen für zulässig.
Zu den Piktogrammen, welche auf die Videoüberwachung hinweisen, monierte der TLfDI den fehlenden Hinweis auf die verantwortliche Stelle. Die Firma versicherte, ein Hinweisschild in Auftrag zu geben, dass allen rechtlichen Vorschriften entspricht.
Erst wenn alle vom TLfDI verlangten Änderungen erfolgt sind und keine datenschutzrechtlichen Mängel mehr vorliegen, kann der Fall

abgeschlossen werden. Bis Redaktionsschluss war dies noch nicht der Fall.

Ein Grundstück gilt datenschutzrechtlich als öffentlich zugänglicher Raum, wenn es nach dem erkennbaren Willen des Berechtigten von jedermann genutzt oder betreten werden darf. Anwendung findet dann der § 6b BDSG. Eine Videoüberwachung wäre zulässig, wenn sie zum Zweck der Wahrnehmung des Hausrechts erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Gemäß § 6b Abs. 2 BDSG ist der Umstand der Beobachtung und die verantwortliche Stelle durch geeignete Maßnahmen erkennbar zu machen.

6.9 Tanken mit Stummfilm – Videogaga 4

Wie dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) im Rahmen seiner Kontrolltätigkeit bekannt wurde, war in einer Thüringer Tankstelle eine Videoanlage installiert. Der Beschwerdeführer befürchtete aufgrund von Angaben der Mitarbeiter, dass an der Tankstelle eine Videoüberwachung mit Tonaufzeichnung stattfindet, da die Mitarbeiter angaben, dass der Stationsleiter über Gespräche in Kenntnis sei, an denen er nicht teilgenommen habe. Er teilte weiterhin mit, dass er auch mit dem Kontaktbereichsbeamten der Gemeinde bezüglich dieses Sachverhaltes Kontakt aufnehmen werde.
Der TLfDI wandte sich mit einem Auskunftsersuchen nach § 38 Abs. 3 Satz 1 Bundesdatenschutzgesetz (BDSG) an den Inhaber, um den Sachverhalt aufzuklären. Der TLfDI legte dem Anschreiben die „Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen“ bei, in welcher die Aufsichtsbehörden der Länder die Anforderungen an eine datenschutzgerechte Videoüberwachung darlegen. Die Orientierungshilfe ist unter https://www.tlfdi.de/mam/tlfdi/datenschutz/video/oh-v -durch-nicht- ffentliche-stellen.pdf auf der Homepage des TLfDI veröffentlicht.
Der Tankstellenbetreiber teilte mit, dass in der besagten Tankstelle keine Videoüberwachung stattfinde, da die Videoanlage wegen eines technischen Defektes außer Betrieb war, sie aber nach Behebung wieder in Be-

trieb genommen werden sollte.
Der TLfDI informierte den Betreiber darüber, dass vor dem Beginn einer neuerlichen Videoüberwachung seitens der verantwortlichen Stelle der konkrete Zweck der Überwachungsmaßnahme schriftlich festzulegen ist. Da es sich um ein Verfahren der automatisierten Datenverarbeitung handelte, musste durch den Betreiber entweder eine Vorabkontrolle durch den betrieblichen Datenschutzbeauftragten nach § 4d Abs. 5 BDSG durchgeführt werden bzw. falls ein solcher nicht bestellt war, musste dem TLfDI eine Meldung nach § 4d Abs. 1 BDSG gemacht werden. Der Inhalt der Meldung ergibt sich dabei aus § 4e Satz 1 BDSG. Der Betreiber wurde gebeten, dem TLfDI vor der Inbetriebnahme der Videoüberwachung entweder die Vorabkontrolle des betrieblichen Datenschutzbeauftragten bzw. die Meldung nach § 4d Abs. 1 BDSG zuzusenden. Ihm wurden das Hauptblatt zum Meldeformular sowie das Anlagenformular zugesandt, das grundsätzlich für jedes Verfahren automatisierter Verarbeitung auszufüllen ist.
Der Betreiber kam den oben genannten Aufforderungen nach, indem sein betrieblicher Datenschutzbeauftragter eine Vorabkontrolle nach § 4d Abs. 5 BDSG durchführte und alle Kameras so ausrichtete, dass Mitarbeiter nicht im Bereich der Kasse aufgenommen wurden. Teils wurden die Bilder entsprechend verpixelt, teilweise die Kameras neu ausgerichtet. Die Videoanlage wurde erst wieder in Betrieb genommen, nachdem eine positive Bewertung der rechtlichen Zulässigkeit vom TLfDI vorlag.

Die Überwachung von öffentlich zugänglichen Flächen und Arbeitsplätzen, wie in diesem Fall in einer Tankstelle, ist **nur** zur Wahrnehmung des Hausrechts oder beim Vorliegen berechtigter Interessen für konkret festgelegte Zwecke (etwa konkreter Diebstahlsverdacht) zulässig. Es dürfen keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Tonaufnahmen sind nicht zulässig. Zur rechtskonformen Videoüberwachung gehört nicht nur die Berücksichtigung schutzwürdiger Interessen der Kunden, sondern auch derjenigen der Mitarbeiter im Rahmen des Arbeitnehmerdatenschutzes.

6.10 Smart-Home-Präsentation: inklusive Videoüberwachung

Im Juni 2016 informierte ein anonymer Anrufer den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) darüber, dass in den Geschäftsräumen eines Sparberaters für Telekommunikation eine Videokamera installiert sei, die von der Eingangstür in den Innenraum gerichtet ist. Dabei handele es sich vermutlich um eine „Smart-Home-Lösung", die den Zugriff per App zulasse. Der Anlageberater habe nur wenige Mitarbeiter, die jedoch durch die Kamera erfasst würden.
Aufgrund des Anrufs und zur Prüfung der rechtlichen Zulässigkeit wandte sich der TLfDI schriftlich an den Sparberater und bat um Auskunft darüber, ob in seinen Geschäftsräumen eine Videokamera im Einsatz ist und inwiefern diese zur Überwachung genutzt wird.
Der Sparberater beantwortete die Fragen des TLfDI zur Kameraüberwachung ausführlich und legte dar, dass es sich nicht um eine Kamerainstallation zur Überwachung von Passanten und Kunden handelte, sondern um eine Smart-Home-Präsentationswand eines deutschen Telekommunikationsunternehmens, die für Vorführungen mit den Kunden genutzt wird. Anhand von Skizzen zur Anordnung der technischen Geräte wurden die Ausführungen untermauert. Nach Darlegung des Sparberaters war diese Präsentationswand ausgerüstet mit verschiedenen sicherheitstechnischen Komponenten, unter anderem einem Rauchmelder, einem Heizthermostat, einem sirenengekoppelten Fensterkontakt und einer Videokamera. Die Kunden können diese technischen Komponenten nach ihrer funktionellen Vorführung erwerben. Darüber hinaus wird diese Sicherheitstechnik außerhalb der Öffnungszeiten als Schutz vor Einbrüchen genutzt und in diesem Sinne zu bestimmten Zeiten eingeschaltet. Im Alarmfall erfolge dann eine digitale Videoaufzeichnung. Nur in diesem Falle werden die Daten gespeichert von Personen, die sich unbefugt Zutritt zu den Räumen verschafft haben.
Aufgrund der Darlegungen des Sparberaters sah der TLfDI die Angelegenheit als erledigt an und keine Notwendigkeit, weitere Maßnahmen zu ergreifen.

Wenn ein Berater für Energieeinsparung und/oder Sicherheitstechnik in seinen Geschäftsräumen entsprechende Technik zu Demonstrationszwecken einsetzt (Videoüberwachung, Bild- und Tonaufnahmetechnik etc.), und eine Videoaufzeichnung nur im Alarmfall stattfin-

det, wenn die Technik gleichzeitig als Schutz vor Einbrüchen eingesetzt wird, liegt kein Verstoß gegen Datenschutzrecht vor.

6.11 Video für Baufortschritt – kein Fortschritt – Videogaga 5

Im Juni 2016 wandte sich der Vorsitzende eines Sportvereins an den TLfDI und bat um die Genehmigung zur Aufstellung einer Videokamera. Die Gemeinde beabsichtigte, den Sportplatz umfassend zu sanieren und der Verein wollte dies mit einer Baustellenkamera dokumentieren. Der Vereinsvorsitzende übersandte dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) alle Informationen über den Standort der Kamera und deren Aufnahmebereich. Der Vereinsvorsitzende teilte mit, dass die Kamera so ausgerichtet werden könne, dass nur die Baustelle selbst in den Beobachtungsbereich der Kamera fällt. Es sollten keine durchgehenden Videoaufnahmen erstellt werden, sondern beispielsweise nur stündlich ein Foto. Die Fotos sollten dann hintereinander geschnitten werden, um so im Zeitraffer den Baufortschritt verfolgen zu können.
Der TLfDI beantwortete die Anfrage des Vereinsvorsitzenden folgendermaßen:
Der TLfDI ist als Aufsichtsbehörde für den Datenschutz im nichtöffentlichen Bereich keine Genehmigungsbehörde für den Einsatz von Videoüberwachung. Eine derartige Maßnahme kann durchgeführt werden, sofern eine Rechtsvorschrift sie erlaubt oder der jeweils Betroffene zugestimmt hat, das sogenannte Verbot mit Erlaubnisvorbehalt, § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG).
Da aufgrund der gestellten Anfrage nicht eindeutig klar war, ob es sich bei dem Bereich, der aufgenommen werden sollte um einen öffentlich zugänglichen Bereich handelte, erläuterte der TLfDI die Rechtslage allgemein:
Die Zulässigkeit der Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Geräten, d. h. Videoüberwachung, ist in § 6b BDSG geregelt. Danach ist die Videoüberwachung nur zulässig, wenn sie zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und wenn schutzwürdige Interessen der Betroffenen nicht überwiegen. Das heißt, wenn öffentlich zugängliche Räume von der geplanten Videoüberwachung betroffen sind, ist diese Maßnahme nur zu Dokumentationszwecken der Baufortschritte nicht zulässig, da hier schutzwürdige Interessen der Betroffenen entgegenstehen. Es

werden nämlich ohne Anlass alle Personen gefilmt, die sich in den Aufnahmebereich der Kamera begeben.
Im Sinne der Verkehrssicherungspflicht müssen Baustellen so abgesperrt sein, dass sie nicht von anderen Personen als den Baustellenarbeitern betreten werden können. Somit ging der TLfDI im vorliegenden Fall davon aus, dass der Baubereich kein öffentlich zugänglicher Bereich ist. Sofern kein öffentlich zugänglicher Raum beobachtet wird, beurteilt sich die Zulässigkeit der Videoüberwachung nach § 28 BDSG. Gemäß § 28 Abs. 1 Nr. 2 BDSG ist das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung für die Erfüllung von eigenen Geschäftszwecken zulässig, soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und wenn schutzwürdige Interessen der Betroffenen nicht überwiegen. Als Betroffene von der Videoüberwachung sind hier im Wesentlichen die Baustellenmitarbeiter, Architekten usw. anzusehen. Aus datenschutzrechtlicher Sicht ist die geplante Videodokumentation nur dann unbedenklich, wenn folgende Regeln eingehalten werden:

- die Ausrichtung der Kamera und die qualitative Auflösung der Bilder dürfen keine Identifizierung der arbeitenden Personen zulassen,
- die Betroffenen müssen im Vorfeld über die Maßnahme informiert werden und
- die Betroffenen müssen über die Beteiligungsrechte ihrer Interessenvertretungen informiert werden.

Aus datenschutzrechtlicher Sicht empfahl der TLfDI, nur Übersichtsaufnahmen ohne Personenbezug von der Baustelle anzufertigen, da dann die schutzwürdigen Interessen der Betroffen nicht tangiert werden.
Der TLfDI bat den Vereinsvorsitzenden darum, ihm Testaufnahmen der Kamera zur Verfügung zu stellen. Hierbei wurde deutlich, dass aufgrund der qualitativ guten Aufnahme jeder Passant und jeder Bauarbeiter, der sich in diesem Bereich aufhielt, erkennbar war. Der TLfDI wies den Vereinsvorsitzenden darauf hin, dass für solche personenbezogenen Aufnahmen die Rechtsgrundlage fehle. Da sich die Bauarbeiter in einem Beschäftigungsverhältnis zum Auftragnehmer befinden, können sie auch keine freiwillige Einwilligung zu den Aufnahmen abgeben, da sie aufgrund des bestehenden Abhängigkeitsverhältnisses nicht frei entscheiden können. Weiterhin war in

den Erfassungsbereich der Kamera ein Weg einbezogen, der von Spaziergängern und als Zugang zum Sportplatz genutzt wurde. Für die Videoüberwachung dieses öffentlich zugänglichen Bereichs fehlte ebenfalls die Rechtsgrundlage. Eine Möglichkeit, die Kamera höher anzubringen (beispielsweise an Flutlichtmasten), um den Aufnahmebereich einzuschränken, bestand nicht.
Daher riet der TLfDI dem Vereinsvorsitzenden datenschutzrechtlich zu folgender Verfahrensweise: Die Kamera sollte lediglich zu einem bestimmten Zeitpunkt nach Ende der Bautätigkeit (ab 18:00 Uhr) für eine Momentaufnahme in Betrieb gesetzt werden, um den Fortschritt der Bautätigkeit zu dokumentieren. Der Vereinsvorsitzende sollte auf dem gesamten Sportplatz Hinweisschilder anbringen, damit jeder rechtzeitig den Aufnahmebereich der Kamera verlassen kann, der nicht auf der Aufnahme gespeichert werden will. Sollten sich auf den Momentaufnahmen nach Durchsicht dennoch Personen befinden, sollten diese nachträglich, beispielsweise mittels Pixeln, unkenntlich gemacht werden. Der Vereinsvorsitzende setzte die Anforderungen des TLfDI um.

Als nicht-öffentliche Stellen unterliegen Vereine den Regelungen des BDSG. Die Installation einer Videokamera zu Dokumentationszwecken einer den Verein betreffenden Baumaßnahme ist zulässig, wenn nur Übersichtsaufnahmen erstellt werden und das Recht des Einzelnen auf informationelle Selbstbestimmung nicht berührt wird. In diesem Sinne sollte die Videokamera erst am Abend, nach Ende der Bautätigkeit, für Momentaufnahmen in Betrieb genommen werden. Des Weiteren sind rund um den Kamerabereich Hinweisschilder zu Aufnahmezeit und Aufnahmebereich der Kamera anzubringen.

6.12 Videoüberwachung der Insolvenzmasse

Im Berichtszeitraum informierte eine Polizeiinspektion (PI) den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) darüber, dass in einem Wohngebiet der Stadt an einem Wohnblock und auf dem zugehörigen Grundstück mehrere Kameras installiert seien. Die PI belegte den Sachverhalt zusätzlich mit entsprechenden Fotoaufnahmen.
Der TLfDI wandte sich zunächst an das Grundbuchamt und bat um Amtshilfe zur Ermittlung des Eigentümers nach § 38 Abs. 1 Bundesdatenschutzgesetz (BDSG). Das Grundbuchamt teilte dem TLfDI

Namen und Anschrift des eingetragenen Hauseigentümers mit. Das Grundstück gehörte einem Privatunternehmen, das sich in Insolvenz befand und für das ein Insolvenzverwalter bestellt war.
Der TLfDI ist die zuständige Aufsichtsbehörde für den Datenschutz nach § 42 Abs. 1 Satz 1 Thüringer Datenschutzgesetz (ThürDSG). Nach § 38 Abs. 1 BDSG kontrolliert er die Einhaltung datenschutzrechtlicher Bestimmungen, die den Einzelnen davor schützen sollen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.
Nach § 4 Abs. 1 BDSG bedarf die Erhebung von Videoaufnahmen einer gesetzlichen Ermächtigung oder der Einwilligung des Betroffenen. Daher bat der TLfDI den Insolvenzverwalter gemäß § 38 Abs. 3 Satz 1 BDSG um eine detaillierte Auskunft zur installierten Videoanlage. Daraufhin teilte der Rechtsanwalt des Insolvenzverwalters dem TLfDI mit, dass sein Mandant inzwischen sämtliche Kameras am betreffenden Gebäude und auf dem Grundstück demontieren ließ. Ausweislich einer dem Schreiben beigefügten Hausmeisterrechnung war die Demontage Ende Dezember 2016 erfolgt.
Daraufhin teilte der TLfDI dem Rechtsanwalt des Insolvenzverwalters mit, dass die Angelegenheit somit datenschutzrechtlich erledigt sei und behielt sich eine Vor-Ort-Kontrolle vor. Weiterhin informierte der TLfDI die PI darüber, dass die Kameras demontiert wurden.

„Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig, soweit eine Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.“ (§ 4 Abs. 1 BDSG). Der TLfDI ist die zuständige Aufsichtsbehörde für den Datenschutz nach § 42 Abs. 1 Satz 1 Thüringer Datenschutzgesetz (ThürDSG). Er kontrolliert nach § 38 Abs. 1 Bundesdatenschutzgesetz (BDSG) die Einhaltung entsprechender datenschutzrechtlicher Bestimmungen.

6.13 Der (Tür)Spion, der die Nachbarn nicht liebte; Videogaga 6

Die Beschwerdeführer wandten sich gegen die Installation einer digitalen Türspion-Kamera, mit der ein Mitmieter sie und andere in dem von ihnen bewohnten Mehrfamilienhaus beobachten würde.
Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) bat die Betreiber der Anlage um Auskünfte, welche Bereiche zu welchen Zwecken und seit wann video-

überwacht, auf welche Art und Weise die erhobenen Daten gespeichert und wie lange die Überwachungsdaten aufbewahrt werden.
Daraufhin teilten die Beschwerdegegner mit, dass sich an ihrer Wohnungstür ein digitaler Türspion befinde, durch welchen die Personen vor ihrer Wohnungstür beobachtet werden könnten. Eine Speicherung der Daten erfolge nicht.
Bei einer Videoüberwachung, die auf einen allgemein zugänglichen Hausflur gerichtet ist, handelt es sich stets um einen Umgang mit personenbezogenen Daten. Dies ist nur dann zulässig, soweit das Bundesdatenschutzgesetz (BDSG) oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder die Betroffenen eingewilligt haben, § 4 Abs. 1 BDSG.
Im Falle einer Videoüberwachung scheidet eine zu einer Zulässigkeit der Anlage führende Einwilligung der Betroffenen in aller Regel aus, da überhaupt nicht absehbar ist, welche Personen in den Bereich der Videoüberwachung gelangen. Daher bedarf es einer Rechtsvorschrift, die diese Videoüberwachung erlaubt.
Maßgebliche Vorschrift für die Zulässigkeitsprüfung einer Videoüberwachungsanlage von öffentlich zugänglichen Bereichen ist regelmäßig § 6b BDSG. Nach § 6b Absatz 1 BDSG ist die Videoüberwachung eine Beobachtung mit optisch-elektronischen Einrichtungen. Von diesem Begriff werden nicht nur handelsübliche Videokameras, sondern jegliche Geräte, die sich zur Beobachtung eignen, erfasst. Hierunter fällt auch der digitale Türspion. Die Videoüberwachung umfasst sowohl die Videobeobachtung, bei der eine Live-Übertragung der Bilder auf einen Monitor, so auch beim digitalen Türspion, erfolgt, als auch die Videoaufzeichnung, bei der Aufnahmen gespeichert werden.
Die Anwendung des § 6b BDSG setzt voraus, dass ein öffentlich zugänglicher Raum (z. B. Hauseingang oder öffentlicher Verkehrsraum) beobachtet wird. Hierbei handelt es sich um Bereiche innerhalb und außerhalb von Gebäuden, die nach dem erkennbaren Willen des Berechtigten (z. B. Grundstückseigentümer, Vermieter etc.) von jedermann genutzt oder betreten werden dürfen. Bei einer Videoüberwachung im Innenbereich von Mehrfamilienhäusern handelt es sich in der Regel nicht um öffentlich zugängliche Räume, weshalb sich die Zulässigkeit nicht nach § 6b BDSG richtet. In diesen Fällen greift § 28 Abs. 1 Nr. 2 BDSG, wonach aber ähnliche Voraussetzungen für eine Videoüberwachung gelten wie in den Fällen des § 6b BDSG.

Die Überwachung des Treppenhauses mit einem digitalen Türspion – unabhängig davon, dass lediglich eine Aufzeichnung und keine Speicherung von Aufnahmen erfolgt – stellt einen erheblichen Eingriff in das informationelle Selbstbestimmungsrecht der Nachbarn dar. Im nicht-öffentlich zugänglichen Raum hat die Privatsphäre eine noch höhere Bedeutung als im öffentlich zugänglichen Raum, denn die anderen Mieter und Mieterinnen sind sich bewusst, dass sie sich in einem Bereich befinden, zu dem nur eine begrenzte Zahl von Personen Zutritt hat. Der Überwachungsdruck wird hier deshalb zumeist noch stärker wahrgenommen als im öffentlich zugänglichen Bereich.
Personenbezogene Daten – hier: Bilddaten – können zur Wahrnehmung berechtigter Interessen nur dann erhoben, gespeichert, verändert oder übermittelt werden, soweit dies erforderlich ist und kein Grund zur Annahme besteht, dass schutzwürdige Interessen der Betroffenen am Ausschluss einer Videoüberwachung überwiegen. Die Zwecke, für die die Daten genutzt werden sollen, sind vor der Erhebung konkret festzulegen. Ein berechtigtes Interesse für den Betrieb einer Videoüberwachungsanlage kann ideeller, wirtschaftlicher oder rechtlicher Natur sein. Sollte die Videoüberwachung dazu eingesetzt werden, vor Einbrüchen, Diebstählen oder Vandalismus zu schützen, ist darin grundsätzlich ein berechtigtes wirtschaftliches Interesse zu sehen, wenn eine tatsächliche Gefahrenlage nachgewiesen werden kann.
Der Einbau einer Türkameraanlage zur Einlasskontrolle ist grundsätzlich datenschutzrechtlich unbedenklich, wenn er jeweils nur anlassbezogen durch das Klingeln an der Tür aktiviert wird, sich der Monitor anschaltet, wenn geklingelt wird, sie nur den unmittelbaren Eingangsbereich vor der Tür erfasst, in dem sich die klingelnde Person aufhält, sie nach kurzer Zeit automatisch wieder deaktiviert wird und keine Aufzeichnung der Bilder erfolgt. Außerdem muss sich an der Tür bzw. der Türklingel ein deutlich sichtbares Hinweisschild befinden, das auf die Kamera aufmerksam macht.
Als Begründung für die Überwachung führten die Beschwerdegegner im vorliegenden Fall aus, sie wollten so verhindern, dass sie weiterhin durch verletzende Bemerkungen der Beschwerdeführer gemobbt würden. Hierbei handelt es sich zwar um ein berechtigtes Interesse, jedoch ist die Videoüberwachung mittels des digitalen Türspions nicht für ihren Zweck – Vorbeugung von Mobbing – geeignet.

Außerdem bestehen Anhaltspunkte, dass die schutzwürdigen Interessen der betroffenen Personen überwiegen. Jeder Mensch hat das Recht, sich in der Öffentlichkeit frei zu bewegen, ohne dass sein Verhalten permanent mithilfe von Kameras beobachtet oder aufgezeichnet wird. Die Tatsache, beobachtet zu werden, bewirkt bei vielen Personen eine Änderung ihres Auftretens. Das eigene Verhalten wird überprüft. Zudem sieht sich der Einzelne einem permanenten Überwachungsdruck ausgesetzt, der eine Beeinträchtigung des Persönlichkeitsrechts darstellt (siehe auch: Bundesverfassungsgericht, Urteil vom 15. Dezember 1983 [BVerfGE 65, 1] – Volkszählung). Nach dieser Entscheidung wird unter den Bedingungen der modernen Datenverarbeitung der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des Art. 2 Abs. 1 Grundgesetz (GG) in Verbindung mit Art. 1 Abs. 1 GG umfasst. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Einschränkungen dieses Rechts auf „informationelle Selbstbestimmung“ sind nur im überwiegenden Allgemeininteresse zulässig.
Der TLfDI hat den Beschwerdegegnern daher mitgeteilt, dass die von ihnen betriebene Videoüberwachungsanlage in der jetzigen Form nicht mit dem BDSG vereinbar ist.
Auf den Hinweis des TLfDI haben die Beschwerdegegner die Türkamera wieder durch einen „normalen“ Türspion ersetzt.

Im Innenbereich von Mehrfamilienhäusern handelt es sich in der Regel nicht um öffentlich zugängliche Räume, sodass bei einer Videoüberwachung in diesen Fällen nicht § 6b BDSG, sondern § 28 Abs. 1 Nr. 2 BDSG anzuwenden ist, bei dem ähnliche Voraussetzungen für eine Videoüberwachung gelten wie in den Fällen des § 6b BDSG. Die Überwachung des Treppenhauses durch einen digitalen Türspion – unabhängig davon, dass lediglich eine Aufzeichnung, aber keine Speicherung von Aufnahmen erfolgt – stellt einen erheblichen Eingriff in das Persönlichkeitsrecht und Selbstbestimmungsrecht der Nachbarn dar, sodass ein solcher nur unter bestimmten Umständen als zulässig anzusehen ist.
Bei der Installation einer Türkameraanlage zur Einlasskontrolle bestehen dabei grundsätzlich keine datenschutzrechtlichen Bedenken, wenn sie jeweils nur anlassbezogen durch das Klingeln an der

Tür aktiviert wird, sich der Monitor anschaltet, wenn geklingelt wird, sie nur den unmittelbaren Eingangsbereich vor der Tür erfasst, in dem sich die klingelnde Person aufhält, sie nach kurzer Zeit automatisch wieder deaktiviert wird und keine Aufzeichnung der Bilder erfolgt. Außerdem muss an der Tür bzw. der Türklingel ein deutlich sichtbares Hinweisschild angebracht sein, das auf die Kamera aufmerksam macht.

6.14 Man kann den Pelz nicht waschen, ohne sich nass zu machen: Videogaga 7

Die Beschwerdeführer wandten sich zunächst mündlich und sodann schriftlich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) wegen der Installation einer Kamera, die sie und andere permanent beobachte.
Ihr Grundstück sei Teil einer Reihenhaussiedlung. Der Beschwerdegegner habe offensichtlich und auffallend an seinem Gebäude eine Kamera in einem Fenster im ersten Stock angebracht. Diese Kamera sei nach mehrfacher Änderung der Befestigung am Fenster jetzt unmittelbar am Haus angebracht.
Eine derartige Kamera mit einem nicht verstellbaren Blickwinkel von ca. 100 bis 110 Grad dürfte ohne ihr Einverständnis nicht zulässig sein. Sie fühlten sich durch diese Beobachtung in ihrer Privatsphäre eingeschränkt und bedroht.
Wie den Beschwerdeführern bereits telefonisch mitgeteilt wurde, ist der TLfDI die zuständige Aufsichtsbehörde für den Datenschutz, § 42 Abs. 1 Satz 1 Thüringer Datenschutzgesetz (ThürDSG) i. V. m. § 38 Abs. 6 Bundesdatenschutzgesetz (BDSG). Nach § 38 Abs. 1 BDSG kontrolliert er die Einhaltung datenschutzrechtlicher Bestimmungen, die den Einzelnen davor schützen sollen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.
In dieser Funktion beabsichtigte der TLfDI, sich in dieser Angelegenheit an den Beschwerdegegner zu wenden, um die Zulässigkeit der Videoüberwachung zu prüfen.
Er bat die Beschwerdeführer in diesem Zusammenhang zunächst, ihm den Namen des Beschwerdegegners und damit mutmaßlichen Betreibers der Videokamera zukommen zu lassen.

Ohne Kenntnis des Namens des Beschwerdegegners kann der TLfDI diesen nur mit erheblichem Zeitaufwand oder gar überhaupt nicht nach § 38 Abs. 3 BDSG zur Auskunftserteilung auffordern.
Daneben hat der TLfDI die Beschwerdeführer auf die Möglichkeit hingewiesen, privatrechtlich gegen die vermeintliche Videoüberwachung vorzugehen. Sollten sie dies anstreben, habe dies keinen Einfluss auf das Tätigwerden des TLfDI. Eine Beratung dazu könne aber leider nicht erfolgen.
Darauf erwiderten die Beschwerdeführer, den Namen des Beschwerdegegners preiszugeben, sei nicht angezeigt, weil dies zwangsläufig zu einer Eskalation führe.
Mangels fehlender Zuarbeit einerseits und der Erkenntnis der Beschwerdeführer andererseits, dass die Einschaltung des TLfDI für das Nachbarschaftsverhältnis nicht förderlich sei, hat der TLfDI die Akte schließlich geschlossen.

Ohne Kenntnis der Adresse und des Namens des Beschwerdegegners kann der TLfDI diesen nur mit erheblichem Zeitaufwand oder überhaupt nicht nach § 38 Abs. 3 BDSG zur Auskunftserteilung auffordern, um dann gegebenenfalls Maßnahmen zu ergreifen.

6.15 Bei Klingeln Aufnahme: BDSG?

Im April 2016 informierte ein Bürger den Thüringer Landebeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) darüber, dass im Klingeltableau am Gebäude eines Wohnhauses eine Kamera integriert sei und diese Kamera von einem privaten Grundstückseigentümer installiert wurde. Diese Kamera sei so angebracht, dass damit die gesamte Straße eingesehen und überwacht werden könne. Der Beschwerdeführer legte dar, dass er selbst diese Straße regelmäßig benutze und dabei sichergestellt wissen wolle, dass keine Privatperson diesen öffentlichen Verkehrsraum überwachen kann.
Der TLfDI prüfte den Sachverhalt und konnte jedoch keinen datenschutzrechtlichen Verstoß feststellen. Die im Klingeltableau integrierte Kamera wurde nur bei Betätigung der Klingel aktiviert und übertrug dabei ein Bild des Eingangsbereichs sowie von der klingelnden Person. Es war nicht möglich, mithilfe der Kamera den Eingangsbereich zu „überwachen“, d. h. der Wohnungseigentümer konnte ohne ein Klingelsignal nicht einfach „nachschauen“ ob sich jemand im Bereich der Klingel befand, da die Bildübertragung erst

durch das Klingeln ausgelöst wurde. Weiterhin wurde die Bildübertragung nach zehn Sekunden unterbrochen. Ein dauerhaftes Aufzeichnen bzw. eine Beobachtung mit der Klingelkamera war nicht möglich.
Datenschutzrechtlich sind solche Klingel-Videoanlagen in der Regel zulässig. Nach § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG) dürfen personenbezogene Daten nur dann erhoben, verarbeitet oder genutzt werden, wenn ein Gesetz dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.
Einwilligungen scheiden bei Videoüberwachungen regelmäßig aus. Allerdings regelt der Gesetzgeber in § 6b BDSG die Beobachtung öffentlich zugänglicher Bereiche abschließend. Danach beurteilen sich auch solche Videokameras, die bei Betätigung der Klingel für kurze Zeit angehen, wenn dabei solche Bereiche erfasst werden, so wie es hier der Fall war.
Die Bildübertragung stellt dabei ein berechtigtes Interesse des Klingelbetreibers dar, was nach § 6b Abs. 1 Nr. 2 BDSG einen der zulässigen Anwendungsbereiche für Videoüberwachung darstellt. Auch gibt es keine Anhaltspunkte dafür, dass bei der Kürze der Beobachtung schutzwürdige Interessen Dritter überwiegen. Eine Speicherung erfolgt nicht.
Voraussetzung für diese Einschätzung ist, dass die Kamera nur aktiv wird, wenn geklingelt wird, und sich innerhalb weniger Sekunden wieder deaktiviert. Ebenfalls darf sie nicht aus der Wohnung heraus aktivierbar sein.

Eine in die Hausklingel integrierte Kamera, die nur durch Betätigung der Klingel ausgelöst wird und dann nur eine kurze, wenige Sekunden dauernde Videosequenz des Besuchers an den Wohnungs- bzw. Hauseigentümer überträgt, ist nach § 6b Abs. 1 BDSG in der Regel zulässig.

6.16 Fenster zum Hof

Im Rahmen seiner aufsichtsbehördlichen Tätigkeit ist der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) darauf aufmerksam gemacht worden, dass an einem Gebäude eine offensichtlich nicht datenschutzgerechte Videoüberwachungsanlage betrieben werde. Bei dieser Videoüberwachungsanlage handele es sich um insgesamt fünf Kameras, die auf den öffentlich

zugänglichen Bereich ausgerichtet seien. Davon befänden sich zwei Kameras an den Fenstern in der ersten Etage und drei Kameras an den Fenstern im Erdgeschoss.
Nach § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG) ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Bei Videoaufnahmen handelt es sich um ein Erheben von personenbezogenen Daten, die nach § 4 Abs. 1 des BDSG einer gesetzlichen Ermächtigung bedürfen.
Der TLfDI hat sich daher mit einem Auskunftsverlangen nach § 38 Abs. 3 BDSG an den Beschwerdegegner gewandt und bat um die Beantwortung eines Fragenkataloges, um den Sachverhalt zu ermitteln.
So wurde der Beschwerdegegner unter anderem befragt, ob er an dem o. g. Gebäude eine Videoüberwachungsanlage betreibe, welche Bereiche zu welchen Zwecken und seit wann videoüberwacht werden.
Der Beschwerdegegner hat in seiner Antwort eingeräumt, Attrappen wegen Verunreinigungen und Beschädigungen seines Eigentumes – unter anderem durch Tiere – einzusetzen. Seit Anbringen der Attrappen gäbe es keine neuen Schäden an seinem Eigentum.
Der TLfDI gab in seiner Erwiderung zu bedenken, dass davon gleichsam ein Überwachungsdruck ausgehe. Auch solche Einrichtungen müssten den im Bundesdatenschutzgesetz (BDSG) geregelten Anforderungen entsprechen, um eine rechtswidrige Verletzung von Grundrechten anderer Bürger zu vermeiden.
Insofern sollte auch bei Verwendung von Attrappen geprüft werden, ob die datenschutzrechtlichen Vorgaben eingehalten werden. In allen Bereichen, in denen sich danach der echte Kameraeinsatz verbietet, sollte somit auch der Einsatz von Kameraattrappen einer Prüfung unterzogen werden. Bei der Beurteilung der Zulässigkeit von Videokameras, die an oder in Wohnhäusern angebracht sind, ist nach dem Erfassungsbereich der Kamera zu unterscheiden. Daher bedarf es auch hier einer Rechtsvorschrift, die eine solche Videoüberwachung erlaubt, es sei denn, es handelt sich um private oder familiäre Aufnahmen, dann ist das BDSG nicht anwendbar. Entscheidend ist, ob auch Personen von der Videokamera erfasst werden können, die in keiner persönlichen oder familiären Verbindung zum Videobetreiber stehen. Die Europäische Datenschutz-Richtlinie sieht für die Daten-

verarbeitung mittels Videoüberwachung eine Ausnahme vor, wenn die Verarbeitung von einer natürlichen Person zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten vorgenommen wird (sog. household exemption). Diese Ausnahme ist nach Ansicht des EuGH allerdings eng auszulegen (Urt. v. 11. Dezember 2014, Az. C-212/13). Daher könne eine Videoüberwachung, die sich auf den öffentlichen Raum erstreckt und dadurch auf einen Bereich außerhalb der privaten Sphäre gerichtet ist, nicht als eine „ausschließlich persönliche oder familiäre Tätigkeit“ angesehen werden. Das BDSG ist also immer einschlägig und der TLfDI damit zuständig, wenn Personen erfasst werden, die mit dem Videobetreiber nicht in enger familiärer Beziehung stehen. Spätestens an Grundstücksgrenzen endet die Beobachtungsbefugnis des Hausrechtsinhabers in der Regel. Nach Sichtung der dem TLfDI vorliegenden Fotos und nach dem Vortrag des Beschwerdegegners sind die Kameraattrappen auch auf die angrenzende öffentliche Straße und den Fußweg ausgerichtet, sodass auch Passanten, Nachbarn oder andere Betroffene in den Erfassungsbereich der Kameraattrappen gelangen können, die in keiner persönlichen oder familiären Verbindung zum Kamerabetreiber stehen.

Kameras, die neben dem eigenen Grundstück/Hof auch den öffentlich zugänglichen Raum in der Umgebung, wie die angrenzende Straße und den Gehweg und die dort befindlichen Personen, mit erfassen, sind nach § 6b BDSG zu beurteilen. Danach ist eine Videoüberwachung öffentlich zugänglicher Räume nur zulässig, soweit sie zur Wahrnehmung des Hausrechts (§ 6b Abs. 1 Nr. 2 BDSG) oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke (§ 6b Abs. 1 Nr. 3 BDSG) erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen von den durch die Videokamera aufgezeichneten Personen entgegenstehen. Auch bevor eine Kameraattrappe installiert wird, sollte festgelegt werden, welches Ziel damit erreicht werden soll. Ein berechtigtes Interesse für den Betrieb kann ideeller, wirtschaftlicher oder rechtlicher Natur sein. Soll die Videoüberwachung dazu eingesetzt werden, vor Einbrüchen, Diebstählen oder Vandalismus zu schützen, ist darin grundsätzlich ein berechtigtes Interesse zu sehen, wenn eine tatsächliche Gefahrenlage nachgewiesen werden kann.

Im Schreiben des Beschwerdegegners sind, wie erörtert, Vorkommnisse genannt. Den genauen Zweck der Kameraattrappen hatte er bisher aber nicht angegeben. Nach derzeitiger Aktenlage diente die

vom Beschwerdegegner durchgeführte vermeintliche Videoüberwachung und die damit verbundene abschreckende Wirkung der Verhinderung künftiger Beschädigungen. Daher bat der TLfDI um eine detaillierte Aufstellung der Vorkommnisse und ggfls. entsprechende Nachweise.
Der Beschwerdegegner teilte indes mit, dass er aufgrund des oben genannten Schreibens des TLfDI die Kameraattrappen entfernen werde, was in der Folgezeit geschah.
Mit dieser Information sah der TLfDI das Verfahren als erledigt an.

Grundsätzlich sollten Attrappen nach den gleichen Maßstäben wie tatsächlich funktionsfähige Kameras zu beurteilen sein, da von ihnen ein ähnlicher Überwachungsdruck ausgeht. Auch solche Einrichtungen sollten den im Bundesdatenschutzgesetz (BDSG) geregelten Anforderungen entsprechen, um eine rechtswidrige Verletzung von Grundrechten anderer Bürger zu vermeiden.

6.17 Auskunftsverweigerungs(un)recht

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) hat Kenntnis davon erlangt, dass ein Beschwerdegegner an der Fassade seines Gebäudes vier Kameras angebracht habe. Neben dem Gebäudeeingang soll sich zudem ein Monitor befinden, auf welchem vier jeweils sich bewegende Kameramitschnitte zu sehen seien. Auf diesen Mitschnitten, die das Grundstück des Beschwerdegegners beträfen, sei wiederrum zu sehen, dass nicht nur sein Privatgrundstück, sondern auch der öffentliche Verkehrsraum erkennbar wäre.
In mehreren Schreiben wandte sich der TLfDI vergeblich an den Beschwerdegegner mit der Aufforderung, sich – jeweils unter Fristsetzung - zum Sachverhalt zu äußern und insbesondere die dort gestellten Fragen zu beantworten. Trotz dieser Fristsetzungen hat sich der Beschwerdegegner zu dem Vorgang nicht geäußert.
Nach § 38 Abs. 3 Satz 1 Bundesdatenschutzgesetz (BDSG) hat die verantwortliche Stelle, vorliegend der Beschwerdegegner, dem TLfDI auf dessen Verlangen die für die Erfüllung seiner Aufgaben erforderlichen Auskünfte unverzüglich zu erteilen. Im Streitfalle betrifft dies vor allem die Frage, ob und bejahendenfalls in welchem Umfang der Beschwerdegegner eine Videoüberwachung betreibt. Nach § 38 Abs. 3 Satz 2 kann der Verpflichtete die Auskunft von

Fragen unter den dort genannten Voraussetzungen verweigern. Die möglichen Gründe einer Auskunftsverweigerung sind ebenfalls in der vom TLfDI gesetzten Frist diesem gegenüber zu erklären.
Der TLfDI hat dem Beschwerdegegner zu diesem Zweck einen Bescheid auf Auskunftserteilung zugestellt, um auf diesem Wege die begehrten Auskünfte zu erlangen. Daraufhin erteilte der Angeschriebene endlich Auskunft. Nach Auswertung der Informationen wurde festgestellt, dass öffentlich zugängliche Bereiche von der Videoüberwachung nicht betroffen waren. Das Verfahren konnte beendet werden.

Nach § 38 Abs. 3 Bundesdatenschutzgesetz (BDSG) hat die verantwortliche Stelle dem TLfDI auf dessen Verlangen die für die Erfüllung seiner Aufgaben erforderlichen Auskünfte unverzüglich zu erteilen, wenn nicht ausnahmsweise ein Auskunftsverweigerungsrecht besteht. Diese Auskünfte können auch durch Vollstreckung des Verwaltungsaktes erzwungen werden. Bestes Mittel ist hierfür regelmäßig das Zwangsgeld. Der TLfDI ist auch ermächtigt, in Fällen, in denen nicht, nicht richtig oder nicht rechtzeitig Auskunft erteilt wird, ein Bußgeldverfahren einzuleiten. Hiervon macht er regelmäßig Gebrauch.

6.18 Der abgeschottete Nachbar

Im Berichtszeitraum 2014/2015 hatte sich ein Bürger beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) darüber beschwert, dass in seiner Nachbarschaft eine Überwachungskamera am Carport angebracht worden sei. Der Beschwerdeführer mutmaßte, dass mit der Kamera der Eingangsbereich seines Hauses überwacht würde und ebenso der Verkehrsraum einer öffentlichen Straße. Er bat den TLfDI um eine datenschutzrechtliche Überprüfung.
Um die rechtliche Zulässigkeit der dargelegten Videoüberwachung bewerten zu können, bat der TLfDI den Betreiber der Kamera zunächst um eine Stellungnahme zu den Vorwürfen des Beschwerdeführers. Nach § 42 Abs. 1 Satz 1 Thüringer Datenschutzgesetz (ThürDSG) i. V. m. § 38 Abs. 6 Bundesdatenschutzgesetz (BDSG) ist der TLfDI die zuständige Aufsichtsbehörde für den Datenschutz gemäß § 38 Abs. 1 BDSG. Er kontrolliert die Einhaltung datenschutzrechtlicher Bestimmungen, die den Einzelnen davor schützen

sollen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht verletzt wird (§ 1 Abs. 1 BDSG).
In diesem Sinne bat der TLfDI insbesondere um Informationen über den Zweck der Videoüberwachung, den Zeitpunkt der Kamerainstallation, die Kameraeinstellungen (Höhe, Erfassungswinkel usw.), Art und Dauer der Datenspeicherung sowie um einen Lageplan und tabellarische Übersichten zu Zeiten der Datenerfassung. Außerdem wollte der TLfDI wissen, ob die Bildaufnahmen mit weiteren Daten verknüpft werden, beispielsweise für einen Personenabgleich.
Nach § 38 Abs. 3 BDSG sind die der Kontrolle des TLfDI unterliegenden Stellen und die mit deren Leitung beauftragten Personen verpflichtet, dem TLfDI die für seine Tätigkeit als Aufsichtsbehörde erbetenen Auskünfte zu erteilen. Dieser Kontrolle unterfallen nichtöffentliche Stellen Dazu zählen „natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts“, § 2 Abs. 4 BDSG.
Der Kamerabetreiber teilte mit, dass er seit knapp einem Jahr zwei Kameras auf seinem Grundstück installiert hatte, eine Kamera an der Haustür und die andere am Hoftor. Nach eigener Aussage hatte er die Kameras ausschließlich zur Überwachung seines eigenen Grundstücks installiert zur Einlasskontrolle am Hoftor und an seiner Haustür. Beide Kameras erfassten allerdings auch in geringem Umfang öffentlich zugängliche Räume.
Beide Kameras waren weder automatisch schwenkbar noch verfügten sie über eine Zoom-Funktion. Die Kameras waren an zwei Monitore angeschlossen, deren Beleuchtung in der Grundeinstellung ausgeschaltet war. Nur bei Wahrnehmung einer Bewegung wurden die Monitore „aktiviert“ und zeigten die Bilder der Kameras. Somit war ausgeschlossen, dass der Bereich vor dem Hoftor permanent aufgezeichnet wird und es konnten auch keine Bewegungsprofile von zufällig am Hoftor vorbeigehenden Passanten erstellt werden. Zugriff auf die Bilddaten hatten der Kamerabetreiber und dessen Mutter. Die aufgenommenen Bilddaten wurden durch Selbstüberschreibung regelmäßig gelöscht. Als Nachweis für seine Darlegungen hatte der Kamerabetreiber dem TLfDI mehrere Bildaufnahmen mit geöffnetem und ungeöffnetem Hoftor zur Verfügung gestellt. Die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten durch nicht-öffentliche Stellen (Unternehmen und Privatpersonen) mittels Datenverarbeitungsanlagen ist im BDSG geregelt. Dies war

durch die Videoüberwachung der Fall. Nach § 4 Abs. 1 BDSG ist eine Videoüberwachung grundsätzlich – wie jeder Umgang mit personenbezogenen Daten – nur dann möglich, wenn eine Einwilligung aller gefilmten Personen vorliegt oder die Videoaufzeichnung gesetzlich erlaubt ist bzw. angeordnet wird. Anderenfalls ist die Videoüberwachung unzulässig. Eine Einwilligung kam naturgemäß in diesem Fall nicht in Betracht. Als Erlaubnisnorm für die Zulässigkeit war § 6b BDSG heranzuziehen. Danach ist eine Videoüberwachung in einem öffentlich zugänglichen Raum zulässig, soweit sie zur Wahrnehmung des Hausrechts (§ 6b Abs. 1 Nr. 2 BDSG) oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke (§ 6b Abs. 1 Nr. 3 BDSG) erforderlich ist. Dabei dürfen jedoch keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der aufgezeichneten Personen beeinträchtigt werden. Die Kamera umfasste auch den Teil des Gehweges vor der Eingangstür bzw. dem Hoftor und insofern einen kleinen Teil des öffentlichen Raums.
Der TLfDI teilte dem Kamerabetreiber mit, dass für das Tatbestandsmerkmal „öffentlich / nicht-öffentlich zugänglicher Raum“ die Eigentumsverhältnisse am Beobachtungsobjekt keine große Rolle spielen. Nicht-öffentlich zugänglich sind Räume, die nur von einem bestimmten Personenkreis betreten werden können oder dürfen. Allein die bestehende Zugangsmöglichkeit begründet keine Öffentlichkeit, wenn der entgegenstehende Wille des Grundstückseigentümers aus den Umständen erkennbar ist (Scholz in Simitis, BDSG, § 6b, Rn. 42, 43, 48). Im vorliegenden Fall war die Zufahrt zum Grundstück durch ein Hoftor abgeschlossen, auch wenn dieses offen stand. Das Tor ließ erkennen, dass es sich hier um ein Privatgrundstück handelt, das nicht für jedermann zugänglich ist. Doch selbst wenn eine Videoüberwachung zum Zweck der Einlasskontrolle an der eigenen Haustür im Sinne von § 1 Abs. 2 Nr. 3 BDSG durchgeführt wird, kann sie unzulässig sein, falls Anhaltspunkte bestehen, dass schutzwürdige Interessen der „Überwachten“ überwiegen. Im vorliegenden Fall überwachte der Kamerabetreiber neben seinem Privatgrundstück auch den öffentlichen Verkehrsraum. Auf Seiten von Passanten oder Besuchern im öffentlichen Raum bestand daher ein berechtigtes Interesse daran, dass die Aufnahmen von ihnen nicht gespeichert werden.
Nach § 6b Abs. 5 BDSG sind die Daten der Videoüberwachung unverzüglich zu löschen, wenn sie für ihren Zweck nicht mehr erforderlich sind oder wenn schutzwürdige Interessen der Betroffenen

einer weiteren Speicherung entgegenstehen. Daher hätten die aufgezeichneten Bilddaten spätestens dann gelöscht werden müssen, wenn der Person, die vor der Haustür oder dem Hoftor steht, geöffnet wurde oder wenn sie das Grundstück wieder verlassen hat. Somit verstieß die Speicherung der Aufnahmen gegen das BDSG und war damit rechtswidrig. Für den Zweck der Einlasskontrolle war eine Speicherung der Bilder nämlich nicht erforderlich.
Dementsprechend forderte der TLfDI den Kamerabetreiber dazu auf, eine Alternative zu wählen, die weniger in die Grundrechte auf informationelle Selbstbestimmung von Passanten oder Besuchspersonen eingreift. In diesem Sinne käme eine Videoüberwachung als reines „Monitoring“ infrage, bei dem die Bilder an den Monitor gesendet, jedoch nicht auf einer SD-Karte gespeichert werden.
Weiterhin forderte der TLfDI den Kamerabetreiber dazu auf, eindeutige Hinweisschilder anzubringen, die auf die Videoüberwachung durch den Grundstücksbesitzer hinweisen (§ 6b Abs. 2 BDSG). Passanten oder Besucher müssen einschätzen können, welcher Bereich von den Kameras erfasst wird, damit sie ggf. der Überwachung ausweichen können. Die Kontaktdaten des Kamerabetreibers müssen auf dem Hinweisschild vermerkt sein, damit der Betroffene erkennt, an wen er sich bezüglich der Wahrung seiner Rechte wenden kann. Das Hinweisschild muss gut sichtbar und in Augenhöhe befestigt werden.
Der Kamerabetreiber bestätigte dem TLfDI schriftlich, dass er die geforderten Maßnahmen betreffend die Bildspeicherung und die Hinweisschilder umgesetzt hatte. Damit erklärte der TLfDI die Videoüberwachung der beiden Kameras als zulässig und teilte dem Beschwerdeführer mit, dass die Videoüberwachung nunmehr mit den Regelungen des BDSG vereinbar ist und er somit nicht in seinem Recht auf informationelle Selbstbestimmung beeinträchtigt wird.

In einem öffentlich zugänglichen Raum ist eine Videoüberwachung zulässig, soweit sie zur Wahrnehmung des Hausrechts (§ 6b Abs. 1 Nr. 2 BDSG) oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke (§ 6b Abs. 1 Nr. 3 BDSG) erforderlich ist und dabei keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der aufgezeichneten Personen beeinträchtigt werden. Für das Tatbestandsmerkmal „öffentlich / nicht-öffentlich zugänglicher Raum“ sind die Eigentumsverhältnisse am Beobachtungsobjekt jedoch unbeachtlich. Auch in einem nicht-öffentlich zugänglichen

Raum muss die Videoüberwachung erforderlich sein, um den vorgesehenen Zweck zu erreichen. In diesem Sinne ist eine Videoüberwachung zu unterlassen, wenn die damit verknüpfte Speicherung der Bilder gegen § 4 Abs. 1 BDSG verstößt und somit rechtswidrig ist. Gemäß § 6b Abs. 2 BDSG sind in Augenhöhe eindeutige Hinweisschilder auf eine Videoüberwachung anzubringen, die auf die Kameraüberwachung und die dafür verantwortliche Stelle hinweisen.

6.19 Postkartenmotiv „Videokamera“

Auf der Suche nach einem außergewöhnlichen Postkartenmotiv entdeckte ein wachsamer Bürger zwei Videokameras an einem Wohnhaus. Er stellte dies erst im Nachhinein fest, als er die von ihm aufgenommenen Bilder durchsah. Er wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und wollte wissen, ob es überhaupt erlaubt ist, dass er gefilmt wird, wenn er an dem Gebäude vorbeiläuft. Ganz einverstanden war er damit nämlich nicht. Als Nachweis schickte er ein Foto von den Videokameras.
Routinemäßig wandte sich der TLfDI an den Hausbesitzer und bat um Aufklärung der Vorwürfe. Der Hausbesitzer gab zu, dass er der Betreiber der Videokameras ist, allerdings handelt es sich bei den Objekten um funktionsuntüchtige Kameras. In der Vergangenheit musste er viele Schmierereien und Graffiti an seiner Hauswand hinnehmen und um die Vandalen abzuschrecken, hielt er die Lösung für eine gute und kostengünstige Variante. Er war ziemlich frustriert darüber, dass er in der Vergangenheit schon etliche Kosten und Mühe zur Beseitigung der Schmierereien hatte in Kauf nehmen müssen. Die Anzeigen bei der Polizei waren leider erfolglos verlaufen.
Der TLfDI wies den Betreiber der Attrappen darauf hin, dass auch solche Geräte in das Persönlichkeitsrecht Dritter eingreifen können. Der Betreiber nahm Änderungen an deren Ausrichtung vor. Datenschutzrechtlich waren die Attrappen dann nicht mehr zu beanstanden.

Auch für private Haushalte gelten die Regeln des Datenschutzrechts. Werden diese nicht eingehalten, drohen Verwaltungs- und Bußgeldverfahren. Zusätzlich können private Haushalte durch Mitbürger über den zivilrechtlichen Weg in die Haftung genommen werden.

6.20 Videoüberwachung eines öffentlichen Raumes der Stadt Rudolstadt durch Privatperson

Eine Thüringer Stadtverwaltung (SV) informierte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) über eine Videoüberwachung durch eine Privatperson. Diese Videoüberwachungsanlage soll nicht nur das Grundstück der Person, sondern auch den Gehweg, also den öffentlich zugänglichen Raum direkt vor dem Grundstück, miterfassen. Der TLfDI wandte sich daraufhin an den vermeintlichen Betreiber der Kamera. Dieser teilte dem TLfDI mit, dass er am besagten Haus (an der gemeldeten Adresse) keine Kamera betreiben würde, er aber an seinem direkten Wohnsitz (in derselben Straße) eine Kamera installiert habe. Er begründete dies mit vergangenen Angriffen auf sein Haus und wollte sich damit schützen. Er sei gegen die Täter vorgegangen und als „Revanche“ wurde sein Privateigentum beschädigt. Weiterhin erklärte er, dass die Aufzeichnungen nur dann zu Beweiszwecken gespeichert werden, wenn es zu Angriffen kommt. Andernfalls würden die Daten überschrieben werden. Einsicht in diese Aufzeichnungen hätte nur er selbst.
Der TLfDI teilte dem Betreiber daraufhin mit, dass die Aufzeichnung von Videoaufnahmen eine Erhebung und Verarbeitung von personenbezogenen Daten darstellt. Diese ist nach § 4 Abs. 1 Satz 1 Bundesdatenschutzgesetz (BDSG) nur zulässig, soweit dieses Gesetz oder eine andere Rechtvorschrift sie erlaubt oder der Betroffene eingewilligt hat. Da eine Einwilligung der Betroffenen nicht vorliegt, kommt es darauf an, ob die Videoüberwachung nach § 6b Abs. 1 BDSG zulässig ist, da vorliegend öffentlich zugängliche Räume erfasst wurden Nach dieser Vorschrift ist die Videoüberwachung nur zulässig, soweit sie zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Das Hausrecht umfasst die Befugnis, grundsätzlich frei darüber zu entscheiden, wem der Zutritt zu einer Örtlichkeit gestattet und wem er verwehrt wird. Ein berechtigtes Interesse für den Betrieb einer Videoüberwachungsanlage kann ideeller, wirtschaftlicher oder rechtlicher Natur sein. Sollte die Videoüberwachung dazu eingesetzt werden, vor Einbrüchen, Diebstählen oder Vandalismus zu schützen, ist darin grundsätzlich ein berechtigtes wirtschaftliches Interesse zu sehen, wenn

eine tatsächliche Gefahrenlage nachgewiesen werden kann. Hier sind konkrete Tatsachen, aus denen sich eine Gefährdung ergibt, beispielsweise Beschädigungen oder besondere Vorkommnisse in der Vergangenheit, nachzuweisen. Da die Videoüberwachungsanlage auch den öffentlichen Raum, sprich den Fußweg, miterfasste, bestehen Anhaltspunkte, dass die schutzwürdigen Interessen der betroffenen Personen nicht gewahrt sind. Jeder Mensch hat das Recht, sich in der Öffentlichkeit frei zu bewegen, ohne dass sein Verhalten permanent mithilfe von Kameras beobachtet oder aufgezeichnet wird. Zudem sieht sich der Einzelne einem permanenten Überwachungsdruck ausgesetzt, der eine Beeinträchtigung des Persönlichkeitsrechts darstellt. Nach § 38 Abs. 5 Satz 1 BDSG kann der TLfDI als Aufsichtsbehörde zur Gewährleistung der Einhaltung dieses Gesetzes und anderer Vorschriften über den Datenschutz Maßnahmen zur Beseitigung festgestellter Verstöße bei der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten oder technischer oder organisatorischer Mängel anordnen. Nach § 6b Abs. 2 BDSG sind der Umstand der Beobachtung und die verantwortliche Stelle durch geeignete Maßnahmen erkennbar zu machen. Der TLfDI bat den Betreiber um Nachweise der tatsächlichen Gefahrenlage durch sorgfältige Dokumentation der Ereignisse.
Gleichzeitig wandte sich der TLfDI an die SV und teilte dieser mit, dass es an der gemeldeten Adresse keine Videoüberwachungsanlage durch den vermeintlichen Eigentümer geben würde, sondern an seinem Wohnsitz in derselben Straße. Aufgrund der örtlichen Nähe zur streitgegenständlichen Videoüberwachungsanlage wollte der TLfDI von der SV wissen, ob die Kamera zwischenzeitlich entfernt worden ist und bat Bilder der noch vorhandenen Kamera zu übersenden. Kurz darauf teilte die SV mit, dass die Kamera entfernt wurde.
Damit sah der TLfDI das Verfahren als erledigt an und teilte dies dem Betreiber der Videokameras mit.

Der TLfDI ist die zuständige Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich, § 42 Abs. 1 Satz 1 Thüringer Datenschutzgesetz, § 38 Abs. 6 BDSG. Nach § 38 Abs. 1 BDSG kontrolliert der TLfDI die Einhaltung datenschutzrechtlicher Bestimmungen, die den Einzelnen davor schützen sollen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird. Nach § 4 Abs. 1 Satz 1 BDSG ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur

zulässig, wenn der Betroffene eingewilligt hat oder dieses Gesetz oder eine andere Rechtvorschrift sie erlaubt. Wenn eine Einwilligung der Betroffenen nicht vorliegt, kommt es darauf an, ob die Videoüberwachung nach § 6b Abs. 1 BDSG zulässig ist, sofern, wie in diesem Fall, öffentlich zugängliche Bereiche videoüberwacht werden Nach dieser Vorschrift ist die Videoüberwachung nur zulässig, soweit sie zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Das Hausrecht umfasst die Befugnis, grundsätzlich frei darüber zu entscheiden, wem der Zutritt zu einer Örtlichkeit gestattet und wem er verwehrt wird. Ein berechtigtes Interesse für den Betrieb einer Videoüberwachungsanlage kann ideeller, wirtschaftlicher oder rechtlicher Natur sein.

6.21 Videoüberwachung nicht über den Maschendrahtzaun hinaus?

Aufgrund eines Nachbarschaftsstreits um einen versetzten Maschendrahtzaun informierte sich eine sog. Teilbesitzerin des Zauns, ob eine Videoüberwachung auf ihrem Grundstück aus datenschutzrechtlicher Sicht zulässig ist. Hintergrund sei, dass es vermehrt zu Streitereien zwischen ihr und dem Nachbarn gekommen ist, was das unbefugte Versetzen des Maschendrahtzauns auf den Grundstücksgrenzen betraf. Auch würden andere Anwohner an ihrem Maschendrahtzaun diversen Vandalismus betreiben. Ihr Anliegen war es nun, eine Videoüberwachungsanlage zu installieren, damit sie zum einen mitbekommt, wenn der Nachbar wieder unbefugt den Maschendrahtzaun auf ihr Grundstück versetzen sollte, und zum anderen, damit sie erfährt, wenn die Kinder von Anwohnern wiederholt diverse Gegenstände am Zaun entsorgen.
Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) konnte hier nur allgemein auf ihre Anfrage antworten, da sie noch keine Videoüberwachung installiert hatte. Des Weiteren wurde im geschilderten Sachverhalt davon ausgegangen, dass die Betroffene die Videoüberwachung lediglich auf ihrem Grundstück betreiben und der Aufnahmebereich nicht auf Nachbargrundstücke oder angrenzende, öffentlich zugängliche Bereiche, wie Straßen oder Gehwege, ausgerichtet sein wird.

Allgemein wurde ausgeführt: Bei einer Videoüberwachung werden aufgrund der Beobachtung personenbezogene Daten erhoben und, sofern die Aufnahmen aufgezeichnet werden, gleichzeitig verarbeitet. Dies ist nur dann zulässig, soweit das Bundesdatenschutzgesetz (BDSG) oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder die Betroffenen eingewilligt haben, § 4 Abs. 1 BDSG. Im Falle einer Videoüberwachung scheidet eine Einwilligung der Betroffenen bereits aus logischen Gründen aus, da überhaupt nicht absehbar ist, welche Personen in den Bereich der Videoüberwachung gelangen. Es bleibt daher bei der Notwendigkeit einer Rechtsvorschrift, die die Videoüberwachung erlaubt. Eine Überwachung im privaten Bereich ist nur unter bestimmten Umständen rechtlich zulässig. Bei der Beurteilung der Zulässigkeit von Videokameras, die an oder in Wohnhäusern angebracht sind, ist nach dem Erfassungsbereich der Kamera zu unterscheiden. Handelt es sich um private oder familiäre Aufnahmen, dann ist das BDSG nicht anwendbar, vgl. § 1 Abs. 2 Nr. 3 BDSG. Die Videoüberwachung des eigenen, allein genutzten Grundstücks ist daher zulässig. Sollte die Videoüberwachung nicht die Voraussetzungen des § 1 Abs. 2 Nr. 3 BDSG erfüllen, ist für die nicht-öffentliche Stelle die maßgebliche Erlaubnisnorm der § 6b BDSG. Hier hat der Gesetzgeber im § 6b Abs. 1 Nr. 2 bis 3 BDSG klar geregelt, welche Voraussetzungen erfüllt sein müssen, damit die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen durch nicht-öffentliche Stellen zulässig ist. § 6b Abs. 1 Nr. 1 BDSG ist hier nicht zutreffend, da es um die Aufgabenerfüllung öffentlicher Stellen geht. Im oben genannten Einzelfall ist zunächst die Variante des § 6b Abs. 1 Nr. 2 BDSG – zur Wahrung des Hausrechts – zu prüfen. Allerdings ist zu betonen, dass die Beobachtungsbefugnis des Hausrechtsinhabers grundsätzlich an den Grundstücksgrenzen endet. Wer außer seinem Grundstück auch öffentlichen Raum wie Straßen, Gehwege oder Parkplätze überwacht, kann sich nicht auf sein Hausrecht stützen, da sich dieses Recht nur auf den privaten Grund und Boden erstreckt. In diesem Fall wäre dann der § 6b Abs. 1 Nr. 3 BDSG nach seiner Zulässigkeit im Einzelfall zu prüfen. Berechtigte Interessen, beispielsweise der Schutz des Eigentums, stehen in diesen Fällen hinter den schutzwürdigen Interessen der Personen, die in den Erfassungsbereich der Kamera geraten, wie Nachbarn, Passanten und sonstige Verkehrsteilnehmer, in der Regel zurück. Die zur Überwachung und zum Schutz des eigenen Grundstücks zulässig eingesetzte Videoüberwa-

chungstechnik darf daher nicht zur Folge haben, dass – quasi nebenbei – auch anliegende öffentliche Wege und die sich dort aufhaltenden Personen mit überwacht werden. Eine Überwachung öffentlich zugänglicher Räume liegt auch dann vor, wenn außer einem privaten Grundstück auch der öffentliche Verkehrsraum in der Umgebung und die sich dort befindlichen Personen erfasst werden können. Auch lässt die Rechtsprechung (vgl. AG Berlin-Mitte vom 18. Dezember 2003 Az.: 16 C 427/02) je nach der Ausgestaltung des Einzelfalls zu, dass der öffentliche Raum in einer Breite von bis zu einem Meter aufgenommen wird.
Hinzu kommt noch, sollte die Videoüberwachung nach § 6b Abs. 1 BDSG zulässig sein, dass die Videoüberwachungsanlage eine automatisierte Verarbeitung nach dem BDSG und diese meldepflichtig nach § 4d BDSG ist. Nicht-öffentliche Stellen, die Videoüberwachungsanlagen einsetzen, sind verpflichtet, dies dem TLfDI als zuständiger Aufsichtsbehörde zu melden, wenn sie keinen betrieblichen Datenschutzbeauftragten haben. Der oben genannte Fall stellt eine solche Meldepflicht dar. Hierzu gibt es auch ein Urteil vom Oberverwaltungsgericht (OVG) Saarland vom 14. September 2017. Genaueres dazu kann auch in der Pressemitteilung vom TLfDI „Meldepflicht für (Wild-)Kameras bestätigt!“ (siehe Anlage 5) nachgelesen werden. Bei allgemeinen Anfragen verweist der TLfDI immer auf die „Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen“ des Düsseldorfer Kreises, in der die Grundsätze zulässiger Videoüberwachung aufgeführt sind. Diese Orientierungshilfe stellt der TLfDI auf seiner Website (https://www.tlfdi.de/mam/tlfdi/datenschutz/video/oh-v__-durch-nicht-__ffentliche-stellen.pdf) zur Verfügung.

Ob die Betroffene letztendlich Videoüberwachung auf ihrem Grundstück – gestützt auf ihr Hausrecht – betreibt, ist dem TLfDI nicht bekannt.

Es empfiehlt sich immer, bevor Videoüberwachungsanlagen installiert werden – egal an welchem Standort –, den TLfDI mit einzuschalten und das Vorhaben aus datenschutzrechtlicher Sicht prüfen zu lassen.

6.22 Videoüberwachung auf eigenem Grundstück zulässig?

Ein Anwohner fühlte sich durch eine am Gebäude seines Nachbarn angebrachte Kamera so sehr in seinem Persönlichkeitsrecht beeinträchtigt, dass er sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) wandte. Der Anwohner vermutete, dass die Kamera so ausgerichtet war, dass diese womöglich seinen Eingangsbereich, Teile des Grundstücks und auch des öffentlichen Bereichs filmte.
Der TLfDI nahm die Beschwerde zum Anlass und erkundigte sich beim Betreiber der Videokamera – sprich beim Nachbarn. Der Betreiber erhielt vom TLfDI – wie es üblich ist – einen umfangreichen Fragenkatalog zu seiner installierten Kamera. Der Betreiber war kooperationsbereit und arbeitete dem TLfDI die benötigten Auskünfte zu dem Fragenkatalog zu. Er skizzierte in Lageplänen den Standort der installierten Kamera. Jedoch stellte sich bei der Beantwortung des Fragenkatalogs heraus, dass es sich nicht um eine funktionstüchtige Kamera handelte, sondern um eine Kameraattrappe. Die Kamera war oberhalb auf der Eingangstür angebracht, ausgerichtet auf den privaten Hauseingang und Vorgarten des Betreibers. Die Attrappe war ausschließlich auf das Grundstück des Besitzers ausgerichtet. Bei Hauseingängen ist zu beachten, dass es sich dabei regelmäßig um öffentlich zugänglichen Raum handelt. Innerhalb solcher Bereiche ist die Videoüberwachung nur nach Maßgabe von § 6b BDSG zulässig. Außerdem ist auf die Videoüberwachung hinzuweisen. Im Ergebnis war die Attrappe datenschutzrechtlich nicht zu beanstanden.
Das Ergebnis der datenschutzrechtlichen Prüfung wurde auch dem Beschwerdeführer – also den Anwohner, der sich an den TLfDI gewandt hatte – mitgeteilt, jedoch war das Ergebnis dessen Unverständnis. Der Bitte einer nochmaligen Prüfung ist der TLfDI nicht nachgegangen, da hier die Rechtslage eindeutig war.

Die Beurteilung von datenschutzrechtswidrig oder datenschutzzulässig installierten Kameras ist sehr komplex, da die rechtliche Einordnung von unterschiedlichen Umständen des Einzelfalls abhängig ist. Unter Umständen kann auch eine installierte Kamera aus datenschutzrechtlicher Sicht zulässig sein; leider auch zum Unverständnis anderer.

6.23 Achtung: Im Vogelhaus nistet eine Kamera! – Videogaga 8

Ein Bürger wandte sich mit einer E-Mail an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Er fühlte sich seit geraumer Zeit durch seinen Nachbarn beobachtet und in seiner Privatsphäre gestört. Besagter Nachbar hatte, getarnt durch ein Vogelhaus, eine Überwachungskamera installiert.
Die Rückfrage bei dem besagten Nachbarn ergab folgenden Sachverhalt: Die „nistende“ Kamera war über Funk mit einem Monitor verbunden, der im Vorbau des Einfamilienhauses installiert war. Dieser gab nur Bilder wieder, wenn die Klingel am Gartentor betätigt wurde. Die Kamera diente zur Erkennung der Personen, die am Eingang zum Grundstück klingelten. Das Eingangstor befand sich etwa 20 Meter vom Hauseingang entfernt und war vom eigentlichen Hauseingang nicht einsehbar. Das Vogelhaus, in dem die Kamera „nistete“, war in einer Entfernung von sieben Metern zur Grundstücksgrenze aufgestellt. Die Kamera war nicht schwenkbar und verfügte über keine Zoomfunktion. Der Monitor zur Kamera war von 8:00 bis 21:00 Uhr eingeschaltet. Es erfolgte keine Aufzeichnung und keine Speicherung der Bilder. Weiterhin gab es keinen Anschluss der Kamera an einen Computer. Einblick auf den Monitor hatten nur der Nachbar und seine Frau.
Die von ihm vorgenommene Videoüberwachung wurde nach Auswertung der vorliegenden Informationen vom TLfDI wie folgt bewertet:
Das Bundesdatenschutzgesetz (BDSG) verfolgt den Zweck, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird, § 1 Abs. 1 BDSG. Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch nicht-öffentliche Stellen (Unternehmen, Privatpersonen) wird durch das BDSG geregelt, soweit sie die Daten unter Einsatz von Datenverarbeitungsanlagen verarbeiten, nutzen oder dafür erheben. Der TLfDI hat hingegen keine Zuständigkeit, wenn die Erhebung, Verarbeitung oder Nutzung der Daten ausschließlich für persönliche oder familiäre Tätigkeiten erfolgt, § 1 Abs. 2 Nr. 3 BDSG. Nach einem Urteil des Europäischen Gerichtshofs vom 11. Dezember 2014 mit dem Aktenzeichen C-212/13 ist diese Regelung allerdings eng auszulegen. Entscheidend sei, ob auch Personen von der Videokamera erfasst werden können,

die in keiner persönlichen oder familiären Verbindung zum Videobetreiber stehen. Das BDSG ist also immer einschlägig und der TLfDI damit zuständig, wenn Personen videoüberwacht werden, die nicht dem eigenen familiären Bereich zuzuordnen sind. Der Aufnahmebereich der hier kontrollierten Kamera erfasste zum Teil die Straße vor dem Grundstück des Videobetreibers. Da sich der Aufnahmebereich über sein eigenes Grundstück hinaus erstreckte, hatte er keinen Einfluss darauf, wer sich in diesen Bereich hinein bewegte. Es bestand die Möglichkeit, dass Dritte in den Aufnahmebereich der Kamera gelangen konnten, so etwa Spaziergänger, Nachbarn oder Besucher.
Nach § 4 Abs. 1 BDSG ist eine Videoüberwachung grundsätzlich wie jeder Umgang mit personenbezogenen Daten nur dann möglich, wenn eine Einwilligung aller gefilmten Personen vorliegt oder die Videoaufzeichnung durch eine gesetzliche Vorschrift erlaubt wird. Ist keine der beiden Voraussetzungen gegeben, so ist die Videoüberwachung unzulässig. Eine Einwilligung ist im Rahmen des Einsatzes einer Videoüberwachung schwer umsetzbar. Als Erlaubnisnorm kommt vorliegend nur der § 6b BDSG infrage. Demnach ist eine Videoüberwachung zulässig, soweit sie zur Wahrnehmung des Hausrechts (§ 6b Abs. 1 Nr. 2 BDSG) oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke (§ 6b Abs. 1 Nr. 3 BDSG) erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen von den durch die Videokamera aufgezeichneten Personen entgegenstehen. Die vom besagten Nachbarn angebrachte Videoüberwachung sollte zu Beobachtungszwecken in Form eines verlängerten Auges als präventives Mittel dienen, um zu sehen, wer bei ihm am Gartentor klingelte.
Besagter Nachbar gab an, dass die Kamera installiert wurde, damit seine Frau auf dem Monitor frühzeitig erkennen konnte, ob ungebetene Gäste den Zutritt zu ihrem Grundstück erzwingen wollten und entscheiden konnte, ob sie die Haustür öffnete oder eben nicht.
Vor dem Einsatz eines Videoüberwachungssystems ist zu überprüfen, ob es tatsächlich für den festgelegten Zweck geeignet und erforderlich ist, § 6b BDSG. Die Erforderlichkeit einer Videoüberwachungsanlage kann nur dann bejaht werden, wenn keine gleich wirksamen Mittel in Betracht kommen, die weniger stark in das Recht auf informationelle Selbstbestimmung Dritter eingreifen. Zu dem vom Videobetreiber verfolgten Zweck stellt sich keine mögliche Alternative dar, die weniger in Rechte Dritter eingreift. Zumal er die Videobeobachtung in den o. g. eingeschränkten Zeiten durchführte. Selbst

wenn eine Erforderlichkeit der Videokamera gegeben ist, kann sie gleichwohl unzulässig sein, wenn Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Der Erfassungsbereich der Kamera ging über das Grundstück des Nachbarn hinaus. Auf den von der Kamera aufgenommenen Bildern war die Straße vor seinem Grundstück ersichtlich. Wie oben bereits dargestellt, hatte er keinen Einfluss darauf, wer sich in diesen Bereich hinein bewegte. Dies stellte einen Eingriff in das Persönlichkeitsrecht der Passanten und/oder seiner Nachbarn dar. In dem Urteil des Amtsgerichts Berlin-Mitte vom 18. Dezember 2003 mit dem Aktenzeichen 16 C 427/02 wurde entschieden, die Videoüberwachung mittels der Videokamerasysteme (Anzahl: drei) im Bereich des Arkadenganges der betroffenen Straße in Berlin zu unterlassen, soweit diese über einen 1 Meter breiten Streifen entlang der Schaufensterseite sowie einen 1 Meter breiten Streifen links und rechts der Arkadensäulen einschließlich des darüber befindlichen Luftraums hinausgeht.
Es überwiegen die schutzwürdigen Interessen Dritter am Ausschluss einer Videobeobachtung die Interessen des Nachbarn, zu sehen, wer bei ihm geklingelt hat.
Nach Einschreiten des TLfDI wurde die Kamera entsprechend diesen Vorgaben ausgerichtet.
Ferner fehlte ein eindeutiges Hinweisschild, welches den Umstand der Videoüberwachung sowie die verantwortliche Stelle erkennen lässt, § 6b Abs. 2 BDSG. Der Betroffene muss einschätzen können, welcher Bereich von einer Kamera erfasst wird, damit er in die Lage versetzt wird, gegebenenfalls der Überwachung auszuweichen oder sein Verhalten anzupassen. Bei Benennung der verantwortlichen Stelle auf dem Hinweisschild ist entscheidend, dass für den Betroffenen problemlos feststellbar ist, an wen er sich bezüglich der Wahrung seiner Rechte ggf. wenden kann. Daher war der besagte Nachbar als verantwortliche Stelle verpflichtet, seine Kontaktdaten explizit auf dem Hinweisschild zu benennen. Bei der Anbringung des Hinweisschildes war ebenfalls darauf zu achten, dass dieses gut sichtbar war und in Augenhöhe befestigt wurde.
Der TLfDI kam zum Ergebnis, dass die „nistende“ Kamera erst mit den datenschutzrechtlichen Bestimmungen des Bundesdatenschutzgesetzes vereinbar war, nachdem der Blickwinkel der Kamera derart verändert wurde, dass der Erfassungsbereich höchstens einen Meter entlang der Grundstücksgrenze verlief. Darüber hinaus musste der

Nachbar ein Hinweisschild anbringen, dass den o. g. Forderungen aus § 6 Abs. 2 BDSG genügte.
Eine neuerliche Prüfung durch den TLfDI ergab, dass die Auflagen durch den besagten Nachbarn erfüllt wurden. Der TLfDI konnte keinen datenschutzrechtlichen Verstoß mehr feststellen. Eine Aufzeichnung von öffentlich zugänglichen Räumen vor der Grundstücksgrenze fand, nach Veränderung des Standorts des Vogelhäuschens nebst der Kamera nicht mehr statt. Ein Eingriff in das Recht auf informationelle Selbstbestimmung in rechtswidriger Art und Weise lag nun nicht mehr vor.

Grundsätzlich ist die Videoüberwachung auf dem eigenen und allein genutzten Grundstück zulässig. Die Beobachtungsbefugnis des Hausrechtsinhabers endet jedoch an der Grundstücksgrenze. Eine darüber hinausgehende Beobachtung in den öffentlichen Raum ist seit der Entscheidung des Amtsgerichts Berlin-Mitte vom 18. Dezember 2003, Az. 16 C 427/02 lediglich bis zu einem Meter über die Grundstücksgrenze hinaus zulässig. Darüber hinaus darf eine Videoüberwachung in den öffentlichen Raum nicht erfolgen.

6.24 Dome

Eine an einer Garage befestigte Dome-Kamera war ein Fall für den Datenschutzbeauftragten. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) erhielt darüber Kenntnis, dass in einem Ort in Thüringen ein Hausbewohner eine Dome-Kamera an seiner Garagenwand installiert hatte. Bei der Dome-Kamera konnte man allerdings nicht die Ausrichtung erkennen, da die Kamera von einem runden schwarzen Gehäuse umhüllt war.
Bei der Beurteilung der Zulässigkeit von Videokameras, die an Wohnhäusern bzw. Garagen angebracht sind, ist nach dem Erfassungsbereich der Kamera zu unterscheiden. Es verbleibt daher bei der Notwendigkeit einer Rechtsvorschrift, die eine solche Videoüberwachung erlaubt, es sei denn es handelt sich um private oder familiäre Aufnahmen, dann ist das Bundesdatenschutzgesetz nicht anwendbar, vgl. § 1 Abs. 2 Nr. 3 Bundesdatenschutzgesetz (BDSG). Nach einem Urteil des Europäischen Gerichtshofs vom 11. Dezember 2014 mit dem Aktenzeichen C-212/13 ist diese Regelung allerdings eng auszulegen. Entscheidend ist, ob auch Personen von der Videokamera erfasst werden können, die in keiner persönli-

chen oder familiären Verbindung zum Videobetreiber stehen. Das BDSG ist also immer einschlägig und der TLfDI damit zuständig, wenn öffentlich zugängliche Räume beobachtet werden, die von Personen frequentiert werden können, die mit dem Videobetreiber nicht in enger familiärer Beziehung stehen. Die Videoüberwachung des eigenen, allein genutzten Grundstücks ist daher oftmals schon allein wegen der Nichtanwendbarkeit des BDSG durch die Aufsichtsbehörde nicht bewertbar. Spätestens an den Grundstücksgrenzen endet die Beobachtungsbefugnis des Hausrechtsinhabers in der Regel.
Soweit mit einer Videokamera neben dem eigenen Grundstück auch der öffentlich zugängliche Raum in der Umgebung wie Straßen, Gehwege oder Parkplätze und die dort befindlichen Personen miterfasst werden können, ist maßgebliche Vorschrift für die Zulässigkeitsprüfung einer Videoüberwachungsanlage § 6b BDSG. Danach ist eine Videoüberwachung zulässig, soweit sie zur Wahrnehmung des Hausrechts (§ 6b Abs. 1 Nr. 2 BDSG) oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke (§ 6b Abs. 1 Nr. 3 BDSG) erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen von den durch die Videokamera aufgezeichneten Personen entgegenstehen.
In einem weiteren Urteil des Amtsgerichts Berlin-Mitte vom 18. Dezember 2013 Az.: 16 C 427/02 wurde entschieden, dass eine Videoüberwachungsanlage einen 1 Meter breiten Streifen entlang der Grundstücksgrenzen einschließlich des darüber befindlichen Luftraums aufzeichnen dürfe, wenn dies für Zwecke des Hausrechts erforderlich ist. Voraussetzung hierfür ist allerdings, dass durch geeignete Maßnahmen nach § 6b Abs. 2 BDSG auf die Videoüberwachung hingewiesen wird und Passanten oder Nachbarn gefahrlos einer Bildaufnahme ausweichen können.
Die Erfüllung der gesetzlichen Voraussetzungen konnte der Betreiber der Dome-Kamera glaubhaft nachweisen und der TLfDI bewertete die Dome-Kamera als rechtlich zulässig.

Videokameras sind heutzutage leider allgegenwärtig. Im unternehmerischen Bereich als auch in privaten Haushalten sind sie auf dem Vormarsch. Dabei gelten auch für private Haushalte die Regeln des Datenschutzrechts. Werden diese nicht eingehalten, drohen Verwaltungs- und Bußgeldverfahren. Noch dazu setzt man sich der Gefahr

aus, dass man von seinen Mitbürgern zivilrechtlich in die Haftung genommen wird.

6.25 Wanderer zeigen Bein: Videogaga 9

Im Mai 2016 erreichte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) eine E-Mail der Verwaltung eines Naturparks in Thüringen. Der TLfDI musste prüfen, ob es zulässig sei, Kameras am Wanderweg zu installieren. Die Kameras sollten einem Studenten, der im Zuge seiner Bachelorarbeit für die Betreuung und Auswertung der Zählerstationen entlang des Leine-Werra-Wanderwegs verantwortlich war, dazu dienen, die Anzahl der Besucher zu erfassen.
Der TLfDI stellte folgende Bedingungen, damit der Installation keine datenschutzrechtlichen Bedenken entgegenstanden: Die Kameras durften keine personenbezogenen Daten erfassen, d. h. die Identifizierung der Personen durfte nicht möglich sein. Der Student erklärte, dass die Kameras so bodennah installiert werden könnten, dass sie nicht sichtbar wären und nur die Beine der Spaziergänger erfasst werden würden. Durch diese bodennahe Bildperspektive war sichergestellt, dass keine personenbezogenen Daten erfasst wurden. Das sollte auch noch dadurch unterstützt werden, dass eine grobe Bildauflösung zu wählen war.
Nachdem der Student diese Informationen erhalten hatte, wollte er die Kameras wie geplant aufstellen, jedoch musste er feststellen, dass seine Kameras nicht für diesen Einsatzzweck geeignet waren. Aus Kosten- und Zeitgründen hat er sich entschlossen, eine manuelle Besucherzählung durchzuführen. Die Kameras kamen nicht zum Einsatz.

Aus datenschutzrechtlicher Sicht ist ein Einsatz der Kameras auf Wanderwegen zum alleinigen Zweck der Überprüfung der an Zählstationen gemessenen Besucherzahlen dann unbedenklich, wenn dadurch keine personenbezogenen Daten erhoben werden. Dafür ist gesorgt, wenn eine grobe Bildauflösung gewählt wird und die Kamera nur einen Ausschnitt der Beine der Wanderer erfasst.

6.26 Kamera im Mehrfamilienhaus beliebt: Videogaga 10

Ein Ehepaar wandte sich mit einer allgemeinen Anfrage an den Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und teilte mit, dass ihr Vermieter in ihrem Mietshaus mit mehreren Mietparteien eine Kamera installiert hat und wollte wissen, ob dies zulässig ist und der Zustimmung durch die Mieter bedarf. Die Überwachungsanlage befindet sich im Inneren des Hauses. Der Vermieter hat die Mieter nicht über das Bildaufnahmegerät informiert und dies ohne deren Zustimmung angebracht. Die Betroffenen wollten auch wissen, welche Vorschriften für die Auswertung der Daten existieren und wie Verstöße sanktioniert werden.

Der TLfDI teilte den Anfragenden mit, dass grundsätzlich eine Videoüberwachung in einem Mietshaus zulässig ist, wenn die gesetzlichen Voraussetzungen dafür vorliegen. Dies lässt sich nicht pauschal, sondern immer nur im Einzelfall feststellen. Einer Zustimmung der Mieter bedarf es in diesem Fall nicht. Für die datenschutzrechtliche Bewertung ist bedeutsam, ob die Kamera öffentlich zugänglichen Raum aufnimmt, in diesem Fall wäre § 6bBundesdatenschutzgesetz (BDSG) einschlägig. Handelt es sich hingegen um einen nicht-öffentlich zugänglichen Bereich, wie bei dem Innenbereich eines Mehrfamilienhauses, greift die Bestimmung des § 28 BDSG. Danach ist das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt. Genauere Anforderungen finden sich in der „Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen“, die auf der Website des TLfDI unter https://www.tlfdi.de/mam/tlfdi/datenschutz/video/oh-v -durch-nicht- ffentliche-stellen.pdf veröffentlicht ist. Diese Orientierungshilfe ließ der TLfDI dem Ehepaar zukommen.



Grundsätzlich stellt eine dauerhafte Überwachung im Innenbereich eines Mehrfamilienhauses einen Eingriff in das allgemeine Persönlichkeitsrecht dar. Außerdem haben die Eheleute gegenüber dem

Betreiber der Videoüberwachung ein Auskunftsrecht nach § 34 Abs. 1 BDSG. Aufgrund des nicht genau beschrieben Sachverhalts des Ehepaars ließ sich grundsätzlich nicht sagen, ob es sich hier um einen Verstoß handelt. Die Beschwerdeführer haben sich nach der Information durch den TLfDI nicht mehr gemeldet.

Sollten Bewohner eines Mietshauses feststellen, dass dort eine Videoüberwachung vorliegt, können sie sich an den TLfDI wenden. Genauere Angaben zu den Anforderungen an eine zulässige Videoüberwachung finden sich in der „Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen“, die auf der Website des TLfDI unter https://www.tlfdi.de/mam/tlfdi/datenschutz/video/oh-v__-durch-nicht-__ffentliche-stellen.pdf veröffentlicht ist.

6.27 Störung des Hausfriedens durch Videoüberwachung – Videogaga 11

Ein Mieter beschwerte sich bei seiner Hausverwaltung, da in dem Mietshaus Kameras angebracht wurden, die unter anderem auf die Eingangstür des Hauses gerichtet waren. Er verlangte eine schriftliche Begründung der Maßnahme von der Hausverwaltung. Die Hausverwaltung begründete die Kameraüberwachung damit, dass sie wiederholt Sachbeschädigungen in dem Haus feststellen musste. Um die Werte zu erhalten und zukünftige Straftaten zu verhindern, habe der Eigentümer, eine Wohnungsgesellschaft, entschieden, den Eingangsbereich überwachen zu lassen. Laut Schreiben an den Mieter werden die gesammelten Daten in regelmäßigen Abständen gesichtet, und, wenn darauf keine Straftat erkennbar ist, gelöscht. Der Beschwerdeführer bemerkte daraufhin, dass die Bewohner des Hauses nicht nach einer Zustimmung gefragt wurden und er bat den Vermieter, die Verhältnismäßigkeit der Überwachungsmaßnahme zu prüfen.

Der Beschwerdeführer wandte sich zudem an den Thüringer Landebeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), damit dieser die Angelegenheit datenschutzrechtlich prüfen konnte.
Der TLfDI richtete dann eine Nachricht an die Hausverwaltung, um Auskunft nach § 38 Abs. 3 Satz 1 Bundesdatenschutzgesetz (BDSG) über die angebrachten Kameras zu erhalten. Außerdem wies er als zuständige Aufsichtsbehörde darauf hin, dass nach § 4 Abs. 1 BDSG die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig ist, soweit das Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Eine solche Einwilligung liegt nicht vor, im Gegenteil, der Beschwerdeführer hatte ein Beschwerdeschreiben verfasst, in dem mehrere Mieter gegen die Videoüberwachung unterzeichnet hatten.
Auf das Auskunftsersuchen erhielt der TLfDI die Antwort, dass es sich lediglich um Kameraattrappen handele, allerdings demnächst aktive Kameras angeschafft werden sollen. Auch wenn es sich um Kameraattrappen handelte, bat der TLfDI die Hausverwaltung darzulegen, zu welchem Zweck die Attrappen angebracht wurden und welchen vermeintlichen Aufnahmebereich sie haben.
Die Hausverwaltung erklärte dem TLfDI, dass nicht sie, sondern die Eigentümergemeinschaft den Beschluss gefasst hatte, dass in dem Haus eine Videoüberwachung stattfinden solle. Der TLfDI erläuterte, dass nach § 3 Abs. 7 BDSG die verantwortliche Stelle jede Person oder Stelle ist, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt. Sollte die Eigentümergemeinschaft also die Hausverwaltung mit der Videoüberwachung beauftragt haben, müssten sie einen Vertrag nach § 11 BDSG über die Datenverarbeitung im Auftrag geschlossen haben. Dieser Vertrag müsste dann dem TLfDI vorgelegt werden. Auf die Nachfrage, wie man eine Überwachung durchführen könne, ohne gegen das geltende Recht zu verstoßen, fügte der TLfDI die „Orientierungshilfe Videoüberwachung bei nicht-öffentlichen Stellen“ (https://www.tlfdi.de/mam/tlfdi/gesetze/orientierungshilfen/oh-v__-durch-nicht-__ffentliche-stellen.pdf) dem Schreiben bei. Diese wurde von den Datenschutzaufsichtsbehörden im Düsseldorfer Kreis erarbeitet, um den privaten Betreibern von Videoüberwa-

chungsanlagen das nötige Wissen hinsichtlich der datenschutzrechtlichen Anforderungen zu übermitteln. Sie soll darüber informieren, unter welchen Voraussetzungen eine Videoüberwachung zulässig ist und welche gesetzlichen Vorgaben dabei einzuhalten sind. Daraus ergibt sich auch, dass ein berechtigtes Interesse für den Betrieb einer Videoüberwachungsanlage im Sinne von § 6b Abs. 1 Nr. 3 BDSG von ideeller, wirtschaftlicher oder rechtlicher Natur sein kann. Soll die Videoüberwachung wie im vorliegenden Fall dazu eingesetzt werden, vor Einbrüchen, Diebstählen oder Vandalismus zu schützen, kann darin grundsätzlich ein berechtigtes Interesse gesehen werden, wenn eine tatsächliche Gefahrenlage nachgewiesen werden kann. Dafür forderte der TLfDI konkrete Nachweise, aus denen sich eine Gefährdung ergibt, beispielsweise Beschädigungen in nicht geringem Ausmaß oder besondere Vorkommnisse in der Vergangenheit.
Die Hausverwaltung bestätigte nun explizit, dass der Betreiber der geplanten Videoüberwachung die durch die Hausverwaltung vertretene Wohnungseigentümergemeinschaft ist. Außerdem erklärte sie, dass es in den letzten Jahren häufig zu Vandalismus und versuchten Wohnungseinbrüchen gekommen ist. Laut der Hausverwaltung habe die Wohnungseigentümergemeinschaft sich unter Abwägung der verschiedenen Interessen entschieden, den Bereich der Hauseingangstür und den Bereich der Tür des Fahrstuhls mittels Kameras zu überwachen bzw. zunächst dort Attrappen anzubringen. Erste Erfolge seien bereits erkennbar: So war nach der Anbringung der Kameras kein Vandalismus mehr erkennbar. Geplant sei daher, diese Bereiche durch aktive Kameras dauerhaft zu überwachen. Die dabei erhobenen Daten sollen für eine Dauer von vier bis sieben Tagen in einem verschlossenen Raum digital gespeichert werden und sich fortlaufendend überschreiben. Die Auswertung der Daten solle durch einen bewohnenden Eigentümer erfolgen, da dieser Polizist und dadurch nach Ansicht der Hausverwaltung ausreichend dafür qualifiziert ist. Mit diesem Schreiben erhielt der TLfDI einen Lageplan der angebrachten Kameras und eine Stellungnahme des Eigentümers, der die Daten auswerten soll.
Die Hausverwaltung ließ sich nun in der Angelegenheit durch einen Anwalt vertreten, der auch auf die Fragen des Auskunftsersuchens antwortete.
Der TLfDI beschloss, eine Kontrolle vor Ort durchzuführen, dafür verabredete er sich mit dem Beschwerdeführer. Während der Kontrolle war ersichtlich, dass zwei Wohnungseingangstüren in den

Beobachtungsbereich fielen. Es handelte sich hier um sogenannte Wildkameras, die bei Bewegungen im Erfassungsbereich Einzelbilder erstellen, das heißt auch, dass dies grundsätzlich funktionsfähige Kameras sind, also keine Attrappen. Außerdem stellte der TLfDI fest, dass sich auch an der Außenwand des Gebäudes eine Kamera befand, die ausschließlich auf den öffentlich zugänglichen Raum gerichtet waren.
Der TLfDI teilte dem Beschwerdeführer und der Eigentümergemeinschaft mit, dass die Kameras in und an dem Mietobjekt nicht mit dem geltenden Datenschutzrecht vereinbar sind. Zwar wurden von der verantwortlichen Stelle Gründe für die Videoüberwachung angeführt, die berechtigte Interessen nach § 28 Abs. 1 Nr. 2 BDSG begründen können. Allerdings liegen die Vorfälle schon einige Zeit zurück. Außerdem besteht Grund zu der Annahme, dass im konkreten Fall das schutzwürdige Interesse der Mieter des Hauses an dem Ausschluss der Verarbeitung oder Nutzung überwiegt. Jeder Besucher des Hauses wird potenziell von der Kamera erfasst, wenn er dieses betritt. Passiert er die Treppe, wird er ebenfalls aufgenommen. Damit liegt eine möglicherweise permanente Überwachung vor, der eine betroffene Person nicht ausweichen kann, da die Bewohner auch bei der dauerhaften Überwachung von Eingängen auf die Nutzung des überwachten Bereichs angewiesen sind. Damit ist eine Rundumüberwachung des sozialen Lebens in dem Miethaus verbunden, die nicht dadurch gerechtfertigt werden kann, dass der Vermieter mit der Überwachung Verschmutzungen oder Vandalismus verhindern möchte.
Darauf nahm der Anwalt der Hauseigentümerschaft Bezug und listete die Schäden auf, die in den letzten Jahren durch Vandalismus entstanden sind, zudem nannte er die veranlassten strafrechtlichen Ermittlungsverfahren. Wenig später teilte der Beschwerdeführer dem TLfDI mit, dass die angebrachten Kameras entfernt wurden. Der TLfDI erhielt auch ein Schreiben des Anwaltes; dort wurde aufgeführt, dass, nachdem die Kameras ihren Zweck erfüllt hatten und keine weiteren Delikte auftraten, diese, um den Hausfrieden zu wahren, demontiert wurden.

Bei einer Videoüberwachung im Innenbereich eines Mehrfamilienhauses handelt es sich in der Regel um nicht-öffentlich zugängliche Räume, weshalb sich die Zulässigkeit nach § 28 BDSG richtet. So stellt eine dauerhafte Überwachung im Innenbereich eines Mehrfa-

milienhauses, zum Beispiel in Treppenaufgängen, im Fahrstuhlvorraum und im Fahrstuhl selbst, einen schweren Eingriff in das allgemeine Persönlichkeitsrecht der Betroffenen dar. Eine Rundumüberwachung des sozialen Lebens kann nicht dadurch gerechtfertigt werden, dass der Vermieter mit der Überwachung Schmierereien, Verschmutzungen oder geringfügigen Vandalismus verhindern möchte. In der Regel überwiegen daher die schutzwürdigen Interessen der Mieter und Besucher als Betroffene.

6.28 Rund um die Uhr ein Blick ins Unternehmen – Videogaga 12

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) erhielt den Hinweis, dass in einem Thüringer Unternehmen vor Kurzem in der Produktionshalle, dem Lagerbereich, dem Bürotrakt und im Außenbereich Videokameras installiert worden seien. Die Kameras würden sich drehen und schwenkten im Innenbereich auch zu den Aufenthaltsräumen und den Mitarbeitertoiletten. Die Vorgesetzten könnten die Mitarbeiter jederzeit über ihren Bildschirm beobachten. Es deute alles darauf hin, dass die Kameras über eine Zoomfunktion verfügten und akustische Aufnahmen anfertigten. An den Türen seien Aufkleber angebracht worden, die auf die Videoüberwachung hinweisen. Ansonsten sei den Mitarbeitern nichts Konkreteres zur Videoüberwachung mitgeteilt worden. Ein Datenschutzbeauftragter sei nicht bestellt, ein Betriebsrat existiere auch nicht.
Der TLfDI wandte sich mit einem Auskunftsersuchen nach § 38 Abs. 3 Bundesdatenschutzgesetz (BDSG) an die Geschäftsführung des Unternehmens und bat um nähere Auskunft. Die Geschäftsleitung führte aus, man habe eine Videoüberwachungsanlage mit insgesamt vier Kameras installiert. Beweggrund dafür sei die Abgelegenheit des Firmengeländes am Ende eines neu erschlossenen Gewerbegebiets gewesen. Immerhin lägen circa 100 m zwischen dem Unternehmen und anderen Gewerbeobjekten bzw. Wohnhäusern. Da das Firmengebäude nur zu den täglichen Geschäftszeiten besetzt sei, keine Schicht- oder Wochenendarbeit stattfinde und kein Werkschutz vorhanden sei, wollte man einen möglichen Einbruch, aber auch Schäden durch Wasser, Sturm und Hagel etwa zu Nachtzeiten und am Wochenende zeitnah bemerken können. Zu diesem Zweck sollten es die vier installierten Netzwerkkameras in der Fertigungs-

halle, im Lager, im Flur der Büroräume und im Außenbereich dem Geschäftsführer bequem ermöglichen, von zu Hause aus über einen Web-Browser unter Nutzung des Internets den Zustand der Zugangstüren, der Hallentore, des Zufahrttores sowie von Teilbereichen der Innenräume auf unbefugten Zutritt live zu überprüfen. Auf eine Aufzeichnung der Aufnahmen habe man allerdings aus Speicher- und Netzkapazitätsgründen verzichtet. Man prüfe noch die technischen Möglichkeiten, die Kameras zeitgesteuert nur in den Abend- bzw. Nachtstunden sowie am Wochenende zu betreiben, um eine eventuelle Überwachung der Mitarbeiter auszuschließen.

Eine Videoüberwachung, die in nicht-öffentlich zugänglichen Räumen stattfindet und nicht im Zusammenhang mit dem Beschäftigungsverhältnis steht, ist an den Voraussetzungen des § 28 Abs. 1 Satz 1 Nr. 2 BDSG zu messen. Der Einsatz von Videotechnik muss zur Wahrung berechtigter Interessen des Arbeitgebers erforderlich sein und schutzwürdige Interessen des Beschäftigten dürfen nicht überwiegen. Ausnahmsweise können Eigentumsinteressen des Arbeitgebers eine Videoüberwachung rechtfertigen, wenn der Beschäftigte nicht im Fokus der Überwachung steht und nicht permanent erfasst wird. Dabei ist vorab zu prüfen, ob weniger einschneidende Mittel in Betracht kommen und ob die Videoüberwachung für den dargelegten Zweck auch geeignet ist. Insbesondere die Geeignetheit warf weitere Fragen auf. Kann der Geschäftsführer über sein Handy oder seinen PC zu Hause, wenn er nicht permanent den Livestream beobachtet, denn tatsächlich feststellen, dass ein Tor oder eine Tür unbefugt geöffnet wurde?

Nach entsprechenden Arbeiten wurde berichtet, man habe die Anlage neu konfiguriert. Hauptaugenmerk sind nun die Zugangstüren. Danach übertragen die Kameras, die schwenken und zoomen können, nur noch außerhalb der Geschäftszeiten die Bilder aus menschenleeren Räumen. Bevor die ersten Mitarbeiter morgens eintreffen, werden die Kameras automatisch abgeschaltet. Zusätzlich hat man die Hinweise auf die Videoüberwachung konkretisiert und auch den Mitarbeitern die Informationen über die konkreten Festlegungen und Modalitäten zukommen lassen.

Da das Unternehmen keinen Datenschutzbeauftragten nach § 4f BDSG bestellt hatte, war die Videoüberwachung als Verfahren automatisierter Verarbeitung vor ihrer Inbetriebnahme gemäß § 4d Abs. 1 BDSG dem TLfDI als Datenschutzaufsicht zu melden. Hierfür stellt der TLfDI auf seiner Homepage entsprechende Formulare

und Muster zur Verfügung. Die Meldung zum Register ist zwischenzeitlich erfolgt.

Die Videoüberwachung menschenleerer Räume kann zur Wahrung berechtigter Interessen aus Gründen der Sicherheit zulässig sein. Auch wenn letztendlich ausgeschlossen werden kann, dass Mitarbeiter erfasst werden, sollten sie dennoch eine Information über die Festlegungen erhalten. Sichtbare Kameras, auch wenn sie nicht eingeschaltet sind, erzeugen ebenso wie laufende Kameras insbesondere auf Mitarbeiter einen Überwachungsdruck, den man durch entsprechende Information minimieren kann.

6.29 Campingplatzatmosphäre – Videogaga 13

Im Berichtszeitraum wandte sich ein Bürger an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und bat um die Prüfung der rechtlichen Zulässigkeit einer Videoüberwachungsanlage. Die Anlage befand sich an einer Gaststätte auf einem Campingplatz. Eigentümer der Gaststätte war die Stadt, aber betrieben wurde sie von einem privaten Pächter. Vor etwa zwei Jahren installierte der Betreiber, nach Informationen des Beschwerdeführers, sechs Kameras an den Außenwänden der Immobilie, um das Umfeld des Gebäudes zu überwachen. Die Campinggäste fühlten sich durch die Kameras überwacht. Der Beschwerdeführer sendete als Anlage Bilder der Außenwand, um die Standorte der Kameras zu dokumentieren. An dem gesamten Gebäude befindet sich nur ein Hinweis darauf, dass eine Videoüberwachung stattfindet. Der Beschwerdeführer informierte den TLfDI ebenfalls darüber, dass eine Aufzeichnung der Aufnahmen stattfände. Außerdem sei kein Grund für die Überwachung ersichtlich, da in den letzten Jahrzehnten keine Straftat wie etwa Einbruch oder Diebstahl gegen die Gaststätte bekannt geworden ist. Zwar sei 2016 ein Softeis-Automat gestohlen worden, allerdings waren zu der Zeit die Kameras bereits angebracht, einen Beitrag zur Aufklärung des Verbrechens konnten diese aber nicht leisten.
Daraufhin erbat der TLfDI von der Stadt den Namen des Betreibers, um diesen kontaktieren zu können. Nach Erhalt der Auskunft sendete der TLfDI dem Betreiber einen Fragebogen zu, in dem er zu der Videoüberwachung Stellung nehmen konnte. Denn gemäß § 6b Bundesdatenschutzgesetz (BDSG) ist die Beobachtung öffentlich

zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) nur zulässig, soweit sie zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.
Als Antwort erhielt der TLfDI die Information, dass die Kameras bereits entfernt wurden. Zur Bestätigung sendete der Betreiber Fotografien der Außenwand an der sich die Kameras befunden hatte.

Nach § 6b BDSG ist eine Videoüberwachung öffentlich zugänglicher Räume nur zulässig, soweit sie zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

6.30 Zeugnisverweigerungsrecht schließt Vorgehen des TLfDI nicht aus

Beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) ging eine Anzeige eines Anwohners ein, der sich darüber beschwerte, dass an einem Haus in seiner Straße eine Videoüberwachungskamera angebracht worden sei. Der Beschwerdeführer teilte die Adresse sowie den Namen der Person mit, die auf dem Klingelschild an dem Haus aufgeführt war. Zur Sicherheit führte der TLfDI eine Abfrage bei der Meldebehörde der betreffenden Gemeinde durch, um in Erfahrung zu bringen, welche volljährigen Personen unter der genannten Adresse gemeldet waren. Nachdem der TLfDI die Auskunft von der Meldebehörde erhalten hatte, wandte er sich mit einem Auskunftsersuchen an den Betreiber. Als keine Reaktion erfolgte, sandte er die gleiche Anfrage nochmals mit Postzustellungsurkunde zu. Daraufhin meldete sich der Rechtsanwalt des Betreibers und forderte zunächst Akteneinsicht, die ihm natürlich gewährt wurde. Der Rechtsanwalt teilte im Anschluss daran mit, dass sich sein Mandant in der Sache nicht erklären werde. Daraufhin erließ der Thüringer Landesbeauftragte ein Auskunftsersuchen nach § 38 Abs. 3 Satz 1 i. V. m. Abs. 5 Satz 1 Bundesdatenschutzgesetz (BDSG). Er wollte wissen, wie viele Videokameras auf dem Grundstück zu welchem Zweck betrieben werden und fragte verschiedene Einzelheiten zum Betrieb der Kameras ab. Hiergegen

legte der Rechtsanwalt des Betreibers Klage beim Verwaltungsgericht Weimar ein. Im Laufe des Verfahrens stelle sich heraus, dass sich der Betreiber auf sein Zeugnisverweigerungsrecht nach § 38 Abs. 3 Satz 2 BDSG beruft. Dies hatte er im vorangegangenen Verwaltungsverfahren nicht deutlich zum Ausdruck gebracht. Der TLfDI nahm daraufhin seinen Bescheid zurück.
Dass der Betreiber einer Videoüberwachungsanlage keine Auskunft über seine Tätigkeit geben muss, sofern er sich damit strafgerichtlicher Verfolgung oder einem Verfahren nach dem Gesetz über Ordnungswidrigkeiten aussetzen würde, ändert nichts daran, dass möglicherweise eine unzulässige Videoüberwachungsanlage betrieben wird, gegen die der TLfDI vorgehen muss. Er wandte sich daher an die Stadt mit einem Amtshilfeersuchen und bat um Mitteilung, ob das Gebäude gewerblich genutzt wird und, wie viele Wohneinheiten sich in dem Haus befinden, außerdem um Fotos von der Front des Gebäudes. Die Stadt teilte mit, dass das Gebäude nicht gewerblich genutzt werde. An der Außenwand des Gebäudes waren zwei Kameras befestigt, Hinweise auf die Videoüberwachung fanden sich nicht. Der TLfDI leitete daraufhin ein Ordnungswidrigkeitenverfahren gegen den Betreiber ein und beantragte beim zuständigen Amtsgericht die Beschlagnahme der Videoüberwachungsanlage. Die Polizei vor Ort führte eine Durchsuchung des Gebäudes durch. Die Auswertung des festgestellten Tatbestands ist noch nicht abgeschlossen.

Ein Auskunftspflichtiger kann gegenüber dem TLfDI die Auskunft auf solche Fragen verweigern, deren Beantwortung ihn selbst oder einen Angehörigen der Gefahr strafgerichtlicher Verfolgung oder eines Verfahrens nach dem Gesetz der Ordnungswidrigkeiten aussetzen würde. Im Rahmen der Durchführung eines Bußgeldverfahrens besteht jedoch die Möglichkeit, nach den Vorschriften der Strafprozessordnung gegen den Betroffenen zu ermitteln. Hierzu gehört auch, dass mit entsprechender amtsgerichtlicher Anordnung eine Hausdurchsuchung, gegebenenfalls mit einer Beschlagnahme, durchgeführt werden kann.

6.31 Videoüberwachung – der TLfDI hilft, wenn er weiß, wo: Videogaga 14

Der Eigentümer eines Mehrfamilienhauses wandte sich mit folgendem Anliegen an den Thüringer Landesbeauftragten für den Daten-

schutz und die Informationsfreiheit (TLfDI): Einer seiner Mieter hatte sich darüber beschwert, dass an dem Autohaus auf dem Nachbargrundstück eine Videoüberwachungsanlage angebracht worden sei. Er forderte die Entfernung der Videokameras, da er diese sogar in seiner Küche auf sich gerichtet sieht. Die Kameras überblickten ebenfalls den öffentlich zugänglichen Innenhof, die gemeinschaftlich genutzten Grünflächen, einige private Stellplätze und die Terrassen der Wohnungen im Erdgeschoss.
Nach § 6b Bundesdatenschutzgesetz (BDSG) ist das Beobachten öffentlich zugänglicher Räume per Videoüberwachung nur zulässig, soweit es zur Wahrung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist. Die Beobachtungsbefugnis endet an den eigenen Grundstücksgrenzen. In diesem Fall war ein berechtigtes Interesse für die Installation der Kameras nicht ersichtlich. Außerdem wäre eine Alternativlösung wie die Absicherung des Innenhofs durch ein Rollgitter mit Zentralschlüssel möglich gewesen. Auf diese Weise würde weniger in die Persönlichkeitsrechte des Einzelnen eingegriffen.
Der TLfDI wollte die vom Autohaus durchgeführte Videoüberwachung datenschutzrechtlich prüfen, stieß aber auf ein praktisches Problem. Unter der vom Beschwerdeführer genannten Adresse fand sich kein Autohaus und eine Handelsregisteranfrage ergab, dass ein Autohaus mit dem vom Beschwerdeführer genannten Namen nicht existierte.
Der Hauseigentümer wurde daraufhin erneut kontaktiert. Er informierte darüber, dass der sich beschwerende Mieter bereits aus dem Haus ausgezogen ist und der neue Mieter sich durch die Videoanlage nicht gestört fühlt. Der Vermieter sah den Sachverhalt damit als erledigt an und wollte nicht weiter gegen den Gewerbetreibenden vorgehen und war auch nicht bereit, die Adresse des Wohnhauses zu benennen. Da dem TLfDI nur die Adresse des Vermieters, nicht aber die des betroffenen Wohnhauses bekannt war, konnte er die Angelegenheit nicht weiterverfolgen. Gegen den Vermieter konnte der TLfDI nicht vorgehen, da dieser nicht die für die Videoüberwachung zuständige Stelle war.

Der TLfDI kann gegen eine unzulässige Videoüberwachung nur vorgehen, wenn ihm zumindest der Ort des Verstoßes bekannt ist.

6.32 Hotelgäste und Mitarbeiter pausenlos auf Video? Videogaga 15

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) erhielt den Hinweis, dass die Betreiber eines Hotels unbemerkt für die „Filmstars“ per App das Treiben im Rezeptionsbereich und im Schwimmbad rund um die Uhr in Bild und Ton überwachen könnten.
Da eine „Fernüberwachung“ im Hinblick auf die Datensicherheit problematisch ist, entschied der TLfDI, sich dies nach § 38 Abs. 4 Bundesdatenschutzgesetz (BDSG) vor Ort unangekündigt anzusehen und die Einhaltung der datenschutzrechtlichen Vorschriften zu überprüfen. Nach § 38 Abs. 4 BDSG ist der TLfDI bzw. sind die von diesem beauftragten Personen zu diesem Zweck befugt, soweit es zur Erfüllung der der Aufsichtsbehörde übertragenen Aufgaben erforderlich ist, während der Betriebs- und Geschäftszeiten Grundstücke und Geschäftsräume der zu kontrollierenden Stelle zu betreten und dort Prüfungen und Besichtigungen vorzunehmen. Diese Personen können geschäftliche Unterlagen, insbesondere die Übersicht nach § 4g Abs. 2 Satz 1 BDSG sowie die gespeicherten personenbezogenen Daten und die Datenverarbeitungsprogramme einsehen. Der Auskunftspflichtige hat diese Maßnahmen zu dulden.
Während der unangekündigten Vor-Ort-Kontrolle wurde festgestellt, dass im Bereich der Eingangstheke und im Schwimmbad des Hotels Kameras installiert waren, die Bild und Ton von 22:00 Uhr bis 6:00 Uhr morgens aufnahmen und für sieben Tage auf einer Festplatte eines PCs im Büro des Geschäftsführers speicherten. Eine Abrufbarkeit über eine App auf mobile Endgeräte konnte nicht festgestellt werden. Die Tonaufzeichnung war unverzüglich abzuschalten, da nach § 201 des Strafgesetzbuches sich strafbar macht, wer unbefugt das nicht-öffentlich gesprochene Wort eines anderen auf einen Tonträger aufnimmt. Dem kamen die Betreiber sofort nach. Der TLfDI hat letztendlich keinen Strafantrag gestellt, weil die Prüfung vor Ort ergab, dass zum Zeitpunkt der Kontrolle keine Tonaufnahmen angefertigt wurden und zur Nachtzeit aufgenommene Stimmen nicht verständlich waren und keinen Personen zugeordnet werden konnten. Gegen die Bildaufnahmen zur Wahrung des Hausrechts und zur Sicherheit der Gäste war grundsätzlich nichts einzuwenden, da in jüngster Vergangenheit Einbrüche bzw. unberechtigter Zutritt zum Hotel zu verzeichnen waren. Zur Aufnahmezeit waren die Rezeption

nicht besetzt und das Schwimmbad geschlossen. Also konnte sich im Aufnahmebereich der Kameras eigentlich niemand befugt aufhalten. Auch spät zurückkehrende Hotelgäste mussten diesen Bereich nicht betreten. Allerdings musste die Speicherdauer der Aufnahmen auf der Festplatte des PCs erheblich verkürzt werden, denn für den angegebenen Zweck war nur eine kurze Speicherfist von maximal 48 Stunden angemessen. In diesem Zeitraum ist es durchaus möglich, etwaige Vorkommnisse festzustellen und auszuwerten.
Da das Hotel aber keinen Datenschutzbeauftragten bestellt hatte, musste es für das Videoüberwachungssystem, auch wenn es letztendlich nur zum Schutz gegen unbefugtes Betreten installiert war, eine Anmeldung gemäß § 4d BDSG zum Register nach § 38 Abs. 2 BDSG beim TLfDI abgeben. Da eine verspätete Meldung zum Register nach § 43 Abs. 1 Nr. 1 BDSG eine Ordnungswidrigkeit darstellt, wird die Einleitung eines Bußgeldverfahrens geprüft.

Videoüberwachung zur Wahrung des Hausrechts eines Hotels ist zulässig, wenn dokumentierte Vorkommnisse wie Einbrüche oder unbefugter Zugang zu Nachtzeiten vorliegen. Tonaufnahmen sind immer unzulässig und sogar strafbar. Hat ein Unternehmen keinen eigenen Datenschutzbeauftragten nach § 4f BDSG bestellt, muss es die eingesetzte Videotechnik dem TLfDI zum Register nach § 38 Abs. 2 BDSG melden.

6.33 Grundstücksgrenze = Ende der Beobachtungsbefugnis

Eine Anwohnerin wandte sich an das für sie zuständige Ordnungsamt. Ihr Nachbar hatte an seinem Haus eine Kamera angebracht. Im Erfassungsbereich der Kamera lagen die öffentliche Straße sowie das Grundstück der Beschwerdeführerin. Das Ordnungsamt leitete die Beschwerde an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) weiter. Der TLfDI schrieb daraufhin den Eigentümer des Hauses mit der installierten Videoüberwachungsanlage an und verlangte weitere Informationen bezüglich der installierten Kamera.
Dieser teilte dem TLfDI mit, dass die Kamera noch nicht in Betrieb sei, dies jedoch zeitnah geschehen solle. Der Zweck der Kamera sei die Abschreckung von Straftätern, da es in der Vergangenheit schon mehrfach Vorkommnisse gegeben habe. Unter anderen sei der Briefkasten gesprengt worden. Außerdem befände sich in dem Gebäude

ein Lager mit Waren im Wert von über 150.000 €. Der Eigentümer erläuterte zudem, dass nur das eigene Grundstück überwacht werden solle, öffentlich zugängliche Räume sollen nicht von der Kamera erfasst werden. Die Inbetriebnahme der Kamera solle erst geschehen, wenn deren Zulässigkeit derer durch den TLfDI geprüft wurde.
Der TLfDI kam zu dem Ergebnis, dass, solange die Kamera nur auf das Privatgrundstück und nicht auf den öffentlich zugänglichen Bereich gerichtet ist, keine datenschutzrechtlichen Bedenken bestehen. Eine Meldepflicht nach § 4d BDSG besteht nicht, weil die personenbezogenen Daten nur für eigene Zwecke erhoben werden, § 4d Abs. 3 Satz 1 BDSG. Sobald die Kamera aber auf Bereiche außerhalb des eigenen Grundstücks gerichtet wird, muss die Videoüberwachungsanlage nach § 4d Abs. 1 Bundesdatenschutzgesetz (BDSG) dem TLfDI gemeldet werden, da in diesem Fall nicht mehr von einer rein persönlichen Nutzung ausgegangen werden kann. Dies wurde auch durch das Urteil des Verwaltungsgerichts Saarlouis vom 18. Mai 2016 bestätigt (vgl. hierzu die Pressemitteilung des TLfDI vom 19. Mai 2017 unter https://www.tlfdi.de/mam/tlfdi/presse/pm19052016.pdf).
Nachdem der TLfDI die Zulässigkeit der angebrachten Kamera festgestellt hatte, teilte er dies dem zuständigen Ordnungsamt und der Beschwerdeführerin mit.

Die Videoüberwachung des eigenen, allein genutzten Grundstücks ist zulässig, allerdings endet die Beobachtungsbefugnis des Hausrechtsinhabers grundsätzlich an den Grundstücksgrenzen. Sobald die Kamera auf Bereiche außerhalb des eigenen Grundstücks gerichtet wird, muss die Videoüberwachungsanlage nach § 4d Abs. 1 Bundesdatenschutzgesetz (BDSG) dem TLfDI gemeldet werden.

6.34 Und weg ist die Attrappe: Videogaga 16

Das Ordnungsamt einer Stadt wurde von aufmerksamen Bürgen darüber informiert, dass sich an einem Gebäude eine private Videoanlage befindet. Der Sachverhalt wurde an dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) zuständigkeitshalber weitergegeben. Der TLfDI ist nach § 42

Abs. 1 Satz 1 Thüringer Datenschutzgesetz (ThürDSG) und § 38 Abs. 6 Bundesdatenschutzgesetz (BDSG) die zuständige Behörde für den Datenschutz. Nach § 38 Abs. 1 BDSG kontrolliert er die Einhaltung datenschutzrechtlicher Bestimmungen, die den Einzelnen davor schützen sollen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.
Der TLfDI kontaktierte den Eigentümer, bat diesen, den Einsatz seiner Videoüberwachungstechnik darzulegen und konkrete Fragen zur Art und Speicherung der Daten zu beantworten. Der Eigentümer des Gebäudes berichtete, es handle sich schlicht um eine Attrappe einer Überwachungsanlage.
Das vom Bundesverfassungsgericht in seiner Erklärung zur Volkszählung vom 15. Dezember 1983 weiterentwickelte Grundrecht auf informationelle Selbstbestimmung beinhaltet auch einen Schutz gegen Kameraattrappen.
Der TLfDI klärte den Eigentümer auf, dass, wenn eine Attrappe nicht von einer tatsächlich betriebenen Kamera zu unterscheiden ist, davon trotzdem ein Überwachungsdruck ausgeht. Denn das Bundesverfassungsgericht hat in seiner Entscheidung 1 BvR 209/83 u. a. vom 15. Dezember 1983 festgestellt, dass eben wesentlicher Inhalt der informationellen Selbstbestimmung der ist, dass dem Einzelnen bekannt ist, wer was wann und bei welcher Gelegenheit über ihn weiß. Damit liegt ein Eingriff in das Grundrecht auf informationelle Selbstbestimmung vor. Dazu bedarf es einer Rechtsgrundlage oder einer Einwilligung. Daraufhin teilte der Eigentümer des Gebäudes mit, dass die Kameraattrappen bereits entfernt worden seien.

Das BDSG beinhaltet auch einen Schutz gegen Kameraattrappen, da für unbeteiligte Dritte trotzdem der Eindruck erweckt wird, aufgenommen zu werden. Datenschutzrechtlich wird daher eine Kameraattrappe durch den TLfDI gleichermaßen gewertet wie eine tatsächlich funktionierende Kamera. Nach § 6b Absatz 1 BDSG ist das Beobachten öffentlich zugänglicher Räume per Videoüberwachung nur zulässig, soweit es zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist. Es ist nicht zulässig, wenn benachbarte Grundstücke oder Straßen im Erfassungsbereich der Kamera liegen.

6.35 Kamera als Abschreckung zulässig?: Videogaga 17

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) erlangte Kenntnis darüber, dass in einem Hauseingang im Erdgeschoss eines Mietobjektes eine Überwachungskamera installiert wurde. Die Mieter hatten sich bereits an den Hauseigentümer gewandt, der die Kamera angebracht hatte, jedoch war dieser nicht bereit, die Kamera wieder abzumontieren und erklärte außerdem, dass es sich lediglich um eine Attrappe handle. Dies bestätigte er ebenfalls dem TLfDI auf dessen Auskunftsverlangen nach § 38 Abs. 3 Bundesdatenschutzgesetz (BDSG).
Die Kameraattrappe sei zum Schutz vor illegalen Aktivitäten angebracht worden, da sich in dem Wohnhaus schon mehrfach nicht identifizierbare Personen befunden haben. Der TLfDI klärte den Hauseigentümer über die Voraussetzungen einer zulässigen Videoüberwachung auf. Nach § 6b BDSG ist die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) nur zulässig, soweit sie zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Genauere Anforderungen finden sich in der „Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen“, die auf der Website des TLfDI unter https://www.tlfdi.de/mam/tlfdi/datenschutz/video/oh-v -durch-nicht- ffentliche-stellen.pdf veröffentlicht ist. Hierauf wurde der Eigentümer hingewiesen. Nach Rücksprache mit seinem Anwalt hat der Vermieter sich daraufhin entschlossen, die Kameras zu entfernen.



Sollten Bewohner eines Mietshauses feststellen, dass dort eine Videoüberwachung vorliegt, können sie sich an den TLfDI wenden. Nach § 6b BDSG ist die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) nur zulässig, soweit sie zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

6.36 Videoüberwachung durch Rechtsanwaltskanzlei

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) wurde im Rahmen seiner aufsichtsbehördlichen Tätigkeit darauf aufmerksam gemacht, dass durch eine Rechtsanwaltskanzlei missbräuchlich die Halterdaten eines Beschwerdeführers ermittelt worden sein sollen. Letztendlich wurde seitens des TLfDI festgestellt, dass diese Beschwerde unbegründet war, jedoch wurde im Rahmen dieser Ermittlungen aufgedeckt, dass die angezeigte Kanzlei eine umfangreiche Videoüberwachung auf ihrem Gelände betrieb.

Durch das Beobachten mittels Videokameras werden personenbezogene Daten erhoben und, falls diese Daten auch gespeichert werden, gleichzeitig auch verarbeitet. Das Erheben, Verarbeiten und Nutzen personenbezogener Daten ist nach § 4 Abs. 1 BDSG nur zulässig, soweit das Bundesdatenschutzgesetz (BDSG) oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Deshalb hat der TLfDI die Zulässigkeit der Videoüberwachung anhand der geltenden Gesetze zu prüfen.

Mithilfe eines Auskunftsersuchens nach § 38 Abs. 3 BDSG konnte der Sachverhalt ermittelt und so eine Kontrolle der Videoüberwachungsanlage ermöglicht werden. Es waren insgesamt sechs Videokameras auf dem Kanzleigelände installiert, die auf den Eingangsbereich mit Pkw-Stellplätzen, das übrige Grundstück und den Innenhof gerichtet waren. Die Aufnahmen wurden 96 Stunden auf einer Festplatte gespeichert. Ein Hinweisschild befand sich im Eingangsbereich an der Klingel und trug die Aufschrift: „Dieses Objekt wird videoüberwacht“.

Die Zulässigkeit der Videoüberwachung muss hinsichtlich des Zwecks und des Erfassungsbereichs für jede installierte Videokamera einzeln beurteilt werden. Daher sind solche Verfahren, die auch die Vielzahl im aufsichtsbehördlichen Bereich darstellen, in der Regel sehr zeit- und arbeitsaufwendig.

Die Videokameras, die auf den Eingangsbereich sowie auf die Pkw-Stellplätze der Kanzlei gerichtet waren, beurteilen sich nach § 6b BDSG, da es sich bei diesem Bereich um einen öffentlich zugänglichen Raum handelt. Öffentlich zugänglich sind Bereiche innerhalb oder außerhalb von Gebäuden, die nach dem erkennbaren Willen des Berechtigten (z. B. Grundstückseigentümer) von jedermann genutzt

oder betreten werden dürfen. Während der Öffnungszeiten der Anwaltskanzlei ist davon auszugehen, dass es sich bei dem Eingangsbereich mit den dazugehörigen Pkw-Stellplätzen um einen öffentlich zugänglichen Raum handelt, da dann vorab eine unbestimmte Personengruppe (Mandanten und solche, die es werden wollen sowie anderen Personen) diesen Bereich passiert. Der Bereich des übrigen Grundstücks und des Innenhofs ist als nicht-öffentlicher Raum zu betrachten, da dieser Bereich nicht von jedem, sondern nur von einem bestimmten und abschließend definierten Personenkreis betreten werden kann. Das sind in dem vorliegenden Fall die Eigentümer und Mitglieder der Kanzlei. Insofern wird die Zulässigkeit der Kameras, die auf den Park und Innenhof gerichtet sind, nicht nach § 6b BDSG, sondern nach § 28 Abs. 1 Nr. 2 BDSG beurteilt. Beide unterliegen aber ähnlichen Voraussetzungen.
Eine Videoüberwachung nach § 6b Abs. 1 BDSG ist dann zulässig, soweit sie zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Auch im Rahmen des § 28 Abs. 1 Nr. 2 ist das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass schutzwürdige Interessen der Betroffenen an dem Ausschluss der Verarbeitung überwiegen. Diese Voraussetzungen konnten seitens der Kanzlei alle erfüllt werden. Der TLfDI bemängelte jedoch das von der verantwortlichen Stelle angebrachte Hinweisschild dahingehend, dass die verantwortliche Stelle mit den entsprechenden Kontaktdaten hierauf nicht zu erkennen war. Der Betroffene muss problemlos, ohne weitere Zwischenschritte, feststellen können, an wen er sich bezüglich der Wahrung seiner Rechte wenden kann.
Darüber hinaus war die Speicherdauer der personenbezogenen Daten zu lang und daher ebenfalls zu bemängeln. Die Daten sind unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind, § 6b Abs. 5 BDSG. Das ist der Fall, wenn eine Gefahr nicht weiter abgewendet werden muss oder eine Beweissicherung nicht notwendig ist und dies festgestellt werden konnte. Ob eine Sicherung notwendig ist, dürfte grundsätzlich innerhalb von ein bis zwei Tagen geklärt werden können. Deswegen hält der TLfDI

im vorliegenden sowie vergleichbaren Fällen eine Speicherdauer von max. 48 Stunden für erforderlich, aber auch ausreichend. In begründeten Einzelfällen kann eine längere Speicherfrist angenommen werden, etwa wenn an Wochenenden und Feiertagen kein Geschäftsbetrieb erfolgt. Dies ist jedoch seitens der verantwortlichen Stelle vorzutragen. Die Anwaltskanzlei kam sämtlichen seitens des TLfDI gemachten Forderungen nach, sodass die Videoüberwachung nach Einschreiten des TLfDI nunmehr im zulässigen Rahmen betrieben wird.

Grundsätzlich ist zwischen einer Videoüberwachung in öffentlich zugänglichen Räumen und nicht-öffentlich zugänglichen Räumen zu unterscheiden. Diese Unterscheidung bekommt Bedeutung im Rahmen der Hinweispflicht nach § 6b Absatz 2 BDSG. Diese besteht nur für öffentlich zugängliche Bereiche und ist Rechtmäßigkeitsvoraussetzung für die Datenverarbeitung. Der Umstand der Beobachtung und die verantwortliche Stelle sind durch geeignete Maßnahmen in Form eines entsprechenden Hinweises erkennbar zu machen. Dabei kann der Hinweis mithilfe entsprechender Schilder oder grafischer Symbole (z. B. Piktogramm nach DIN 33450) erfolgen. Der Hinweis ist so anzubringen, dass der Betroffene vor dem Betreten des überwachten Bereichs den Umstand der Beobachtung erkennen kann. Er muss in die Lage versetzt werden, der Überwachung ggfs. ausweichen oder sein Verhalten anpassen zu können. Auch die für die Datenverarbeitung verantwortliche Stelle, welche die Videodaten erhebt, verarbeitet oder nutzt, muss mit Adresse angegeben sein. Die Kontaktdaten sind daher auf dem Hinweisschild explizit zu nennen, was viele Kamerabetreiber nicht beachten und was seitens des TLfDI häufig beanstandet werden muss.

6.37 Allgemeine Anfragen zur Videoüberwachung

Während des Berichtszeitraums hat der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) verschiedene Anfragen hinsichtlich des Betreibens von Videoüberwachungsanlagen erhalten.
Zum einen wurde von einer niederländischen Datenschutzaufsichtsbehörde angefragt, inwieweit eine Überwachung von Saunaeingängen, insbesondere der angebrachten Drehkreuze, zulässig sei. Besonders war zu berücksichtigen, dass es sich hierbei um eine Sauna mit

homosexuellen Gästen handelte. Die Beurteilung der Zulässigkeit von Videoüberwachungen in einem solchen Bereich richtet sich nach § 6b Bundesdatenschutzgesetz (BDSG). Danach ist eine Videoüberwachung von öffentlich zugänglichen Räumen zulässig, soweit sie zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Problematisch ist hier insbesondere die Erforderlichkeit für den zumeist verfolgten Zweck, den unbefugten Zutritt von Personen zu verhindern. Die reine Überwachung der Drehkreuze ist in diesem Fall nicht erforderlich, da durch Erhöhen der Drehkreuze der unbefugte Zutritt zu der Sauna oder auch zu Schwimmbädern erschwert werden kann. Darüber hinaus kann die Sexualität der Besucher nach § 3 Abs. 9 BDSG eine besondere Art von personenbezogenen Daten sein, was im Rahmen der Abwägung der schutzwürdigen Interessen mit den berechtigten Interessen des Kamerabetreibers zu berücksichtigen ist und auch zum Überwiegen der Interessen der Betroffenen führen kann. Eine generelle Unzulässigkeit kann hieraus jedoch nicht hergeleitet werden.

Eine weitere Anfrage kam von einem Bürger, welcher wissen wollte, an wen man sich wendet, wenn eine private Videoüberwachung den öffentlichen Raum miterfasst und wie man diese abstellen kann. Zwar kann ein privater Hauseigentümer im Rahmen seines Hausrechts grds. sein eigenes Grundstück überwachen. Eine solche Überwachung fällt unter die Privilegierung des § 1 Abs. 2 Nr. 3 BDSG, da die personenbezogenen Daten lediglich zu familiären und persönlichen Zwecken erhoben, verarbeitet oder genutzt werden. In einem solchen Fall sind die Vorschriften des BDSG nicht anwendbar. Geht die Überwachung jedoch über die eigenen Grundstücksbereiche hinaus, werden also Straßen, Gehwege oder Nachbargrundstücke erfasst, also außerhalb der privaten Sphäre desjenigen, der Daten auf diese Weise verarbeitet, kann sie nicht als eine ausschließlich „persönliche oder familiäre“ Tätigkeit angesehen werden. Das hat der Europäische Gerichtshof in seinem Rynes-Urteil vom 11. Dezember 2014 Az.: C-212/13 abschließend entschieden. In einem solchen Fall können sich Betroffene an die örtlich zuständige Aufsichtsbehörde für den Datenschutz wenden. Für Thüringen ist dies der TLfDI. Die Aufsichtsbehörde prüft dann die Vereinbarkeit der Videoüberwachungsanlage mit den Vorschriften des BDSG. Sollte ein Verstoß vorliegen, wird die Aufsichtsbehörde entspre-

chende Anordnungen treffen und diese durchsetzen. Ferner ist es möglich, den Zivilrechtsweg einzuschlagen und gegen die Persönlichkeitsrechtsverletzung, welche durch eine Videokamera hervorgerufen wird, vorzugehen.

Der Einsatz von Videoüberwachungen kommt in allen Bereichen des täglichen Lebens vor. Jede Entscheidung über die Zulässigkeit der eingesetzten Videoüberwachung ist eine Einzelfallbetrachtung, deswegen können solche allgemeinen Fragen nur oberflächlich beantwortet und insgesamt nur generelle Aussagen getroffen werden. Verantwortlich für diese Zulässigkeitsprüfung ist jedoch der Verwender der Videoüberwachung, und zwar bevor diese eingerichtet wird. Nach Erfahrung des TLfDI ist Videoüberwachung nämlich in der Regel zumindest in Teilen unzulässig, wenn diese geprüft wird. Der TLfDI stellt den nicht-öffentlichen Stellen auf seiner Website die „Orientierungshilfe Videoüberwachung durch nicht-öffentlichen Stellen“ (https://www.tlfdi.de/mam/tlfdi/datenschutz/video/oh-v__-durch-nicht-__ffentliche-stellen.pdf) als Hilfe und Information zur Verfügung. Zusätzlich weist der TLfDI darauf hin, dass alle Videoüberwachungen von nicht-öffentlichen Stellen nach § 4d Abs. 1 BDSG zu melden sind, soweit die Ausnahmetatbestände des § 4d Abs. 2 und 3 BDSG nicht eingreifen. Die entsprechenden Meldeformulare mit Anlage sind ebenfalls auf der Website des TLfDI abrufbar (https://www.tlfdi.de/mam/tlfdi/datenschutz/video/tlfdi_meldeformular_v__.pdf, https://www.tlfdi.de/mam/tlfdi/datenschutz/video/tlfdi_v___anlagenformular.pdf).

Der Einsatz von Videoüberwachungen ist vielfältig und kommt mittlerweile in fast sämtlichen Lebensbereichen vor. Die Anfragen und Beschwerden beim TLfDI nehmen daher immer mehr zu. Diese sind genauso vielseitig wie die Einsatzbereiche der einzelnen Videoüberwachungskameras selbst.

6.38 Videoüberwachungsverbesserungsgesetz – Verbesserung? – Anwendbarkeit?

Das am 4. Mai 2017 in Kraft getretene „Videoüberwachungsverbesserungsgesetz“ – Gesetz zur Änderung des Bundesdatenschutzgesetzes – Erhöhung der Sicherheit in öffentlich zugänglichen großflächigen Anlagen und im öffentlichen Personenverkehr durch optisch-elektronische Einrichtungen - musste bereits im Vorfeld seiner Verabschiedung erhebliche Kritik der Datenschutzbehörden von Bund und Ländern einstecken. Das Gesetz sieht in § 6b Abs. 1 Bundesdatenschutzgesetz (BDSG) (neu) vor, dass bei einer Videoüberwachung von öffentlich zugänglichen großflächigen Anlagen, wie insbesondere Sport-, Versammlungs- und Vergnügungsstätten, Einkaufszentren, Parkplätzen oder Fahrzeugen und öffentlich zugänglichen großflächigen Einrichtungen des öffentlichen Schienen-, Schiffs- und Busverkehrs, der Schutz von Leben, Gesundheit oder Freiheit von sich dort aufhaltenden Personen als ein besonders wichtiges Interesse gilt. Die Gesetzesänderung soll dazu beitragen den privaten Stellen das Betreiben der Videoüberwachung zu erleichtern. Vordergründig sollen mit dem Gesetz insbesondere terroristische Anschläge wie in Ansbach, Berlin oder München durch die Ausweitung der Videoüberwachung privater Stellen verhindert und die Sicherheit der Bevölkerung erhöht werden.
Die einzelnen Datenschutzbehörden der Länder waren sich darin einig, dass solche Anschläge mittels Betreibens einer Videoüberwachung nicht verhindert werden können. Hierzu wäre eine Videoüberwachung auf den in dem Gesetz genannten Plätzen erforderlich, die eine Live-Beobachtung ermöglicht. Außerdem müsste das gleichzeitige Eingreifen eines Wachschutz- oder Sicherheitspersonals bei einem Vorfall gegeben sein. Das ist bei den Videoüberwachungsanlagen meist nicht der Fall, da die hohen Kosten für zusätzliches Personal die Unternehmen abschrecken. Meist kommen hier sog. Black-Box-Verfahren zum Einsatz. Die personenbezogenen Daten werden gespeichert und für eine gewisse Dauer zum Abruf

bereitgehalten. Hierdurch wird lediglich im Nachgang die Möglichkeit der Strafverfolgung durch die zuständigen Behörden erleichtert. Eine tatsächliche Erhöhung der Sicherheit der Bevölkerung geht damit nicht einher. Lediglich das subjektive Sicherheitsgefühl der Personen wird hierdurch gesteigert. In der Praxis sind die Betreiber zumeist nicht in der Lage, ein Live-Monitoring durchzuführen und die Bilder der vielen Kameras durch ihr eigenes Personal so auszuwerten, dass bei Gefahren direkt und schnell eingegriffen werden kann. Zudem verkennt der Referentenentwurf des Bundesinnenministeriums zu dem Gesetz, dass Terroristen und irrational handelnde Einzeltäter ihren eigenen und den Tod der anderen bewusst in Kauf nehmen und gerade die öffentliche Zurschaustellung ihrer Taten beabsichtigen.

Darüber hinaus wurden bereits im Rahmen der alten Regelung des § 6b Abs. 1 BDSG die Sicherheitsinteressen von Unternehmen hinsichtlich des Zwecks Hausrecht und berechtigte Interessen sowie der Schutz von Leib und Leben im Rahmen der Abwägung der schutzwürdigen Interessen von den Datenschutzbehörden hinreichend berücksichtigt, sofern der private Betreiber eine tatsächliche Gefahrenlage für diese Rechtsgüter nachweisen konnte. Ein Überwiegen dieser Interessen gegenüber dem informationellen Selbstbestimmungsrecht der Betroffenen lag dann i. d. R. auch vor. Jedoch kam dies immer auf den Einzelfall an, da jede Videoüberwachung einer Einzelfallprüfung unterliegt. Letztendlich ist die Regelung darauf gerichtet, dass dem Schutz von Leib und Leben in der rechtlichen Abwägung ein stärkeres Gewicht zuzumessen ist, was aber auch der bisherigen aufsichtsbehördlichen Praxis entspricht. Eine abstrakte Gefährdung aller großflächigen Anlagen und des Personennahverkehrs hinsichtlich der im Gesetz genannten Rechtsgüter wird durch die Aufsichtsbehörden der Länder bezweifelt.

Abschließend ist noch darauf hinzuweisen, dass sich die Aufsichtsbehörden der Länder darin einig sind und waren, dass es nicht Aufgabe der privaten Stellen ist, die Sicherheit der Bevölkerung zu gewährleisten. Diese Aufgabe obliegt nicht ohne Grund den Sicherheitsbehörden des Bundes und der Länder. Die Gesetzesänderung stellt aber gerade eine solche Übertragung der hoheitlichen Aufgabe Schutz und Sicherheit der Bevölkerung auf Private dar.

Trotz dieser Bedenken und Einreichung einer umfangreichen Stellungnahme durch die Datenschutzkonferenz aller Datenschutzbehörden von Bund und Ländern wurde die Gesetzesänderung beschlossen

und in Kraft gesetzt. Wie sich diese Änderung bei der Beurteilung der Zulässigkeit der zu prüfenden Videoüberwachungsanlagen auswirken wird, ist noch nicht absehbar. Ab dem 25. Mai 2018 wird außerdem die Europäische Datenschutz-Grundverordnung (EU-DS-GVO) Geltung in allen europäischen Staaten der EU erlangen. Der Bundesgesetzgeber hat in einem seit dem 5. Juli 2017 in Kraft getretenem Anpassungsgesetz zu dieser Verordnung (EU-DSAnpUG-EU) mit § 4 EU-DSAnpUG EU eine eigene Regelung hinsichtlich des Betreibens von Videoüberwachungskameras in öffentlichen Bereichen von privaten Stellen getroffen, welche dem jetzt geänderten § 6bAbs. 1 BDSG entspricht. Auch hier ist noch unklar, ob diese Regelung überhaupt seitens der Aufsichtsbehörden bei der Zulässigkeitsprüfung angewendet werden kann, da das europäische Recht den nationalen Gesetzen vorgeht und die Europäische Datenschutz-Grundverordnung dem nationalen Gesetzgeber keine Befugnis zu eigenen Regelungen in diesem Bereich eingeräumt hat.

Am 4. Mai 2017 ist das „Videoüberwachungsverbesserungsgesetz“ – Gesetz zur Änderung des Bundesdatenschutzgesetzes – zur Erhöhung der Sicherheit in öffentlich zugänglichen großflächigen Anlagen und im öffentlichen Personenverkehr durch optisch-elektronische Einrichtungen – in Kraft getreten. Es regelt, dass der Schutz von Leben, Gesundheit oder Freiheit von Personen, die sich in den im Gesetz genannten Anlagen aufhalten, als besonders wichtiges Interesse gilt. Ziel der Gesetzesänderung ist es, dass durch Ausweitung der Videoüberwachung der privaten Stellen eine höhere Sicherheit der Bevölkerung erreicht werden soll. Bereits im Gesetzgebungsverfahren wurde die Gesetzesänderung von den Aufsichtsbehörden abgelehnt. Trotz der Bedenken ist das Gesetz in Kraft getreten. Inwieweit sich in der Praxis hierdurch Änderungen hinsichtlich der Beurteilung der Zulässigkeit von Videoüberwachungen ergeben, ist noch nicht absehbar. Eine abstrakte Gefährdung aller großflächigen Anlagen und des Personennahverkehrs hinsichtlich der im Gesetz genannten Rechtsgüter wird durch die Aufsichtsbehörden des Bundes und der Länder insoweit nicht angenommen, sodass weiterhin Einzelfallprüfungen erfolgen. Ob das neue Recht angesichts der Anwendungsvorrang genießenden EU-DS-GVO überhaupt anzuwenden ist, wird gerade diskutiert.

6.39 Keine Meldepflicht bei Firmenüberwachung?

Im Berichtszeitraum wurde der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) durch eine Firma angefragt, ob eine Videoüberwachung auf dem Firmengelände meldepflichtig sei, wenn keine festangestellten Mitarbeiter dort beschäftigt sind und nur zeitweise ein Geschäftsbetrieb erfolgen würde. Hierzu teilte der TLfDI dem betreffenden Firmeninhaber mit, dass auch diese Videoüberwachung zu melden sei. Nach § 4d Abs. 1 Bundesdatenschutzgesetz (BDSG) sind Verfahren automatisierter Verarbeitungen vor der Inbetriebnahme von nicht-öffentlichen verantwortlichen Stellen der zuständigen Aufsichtsbehörde nach Maßgabe der Angaben aus § 4e BDSG zu melden. Digitale Videoüberwachungen stellen grundsätzlich ein meldepflichtiges Verfahren dar, da es sich dabei immer auch um eine automatisierte Verarbeitung handelt. Hierbei ist nicht relevant, ob das Firmengelände nur zeitweise genutzt wird oder keine festangestellten Mitarbeiter dort tätig sind, da jedenfalls zu den Zeiten, in denen sich Personen auf dem Gelände aufhalten, personenbezogene Daten automatisiert verarbeitet werden. Eine Unterscheidung zwischen Personen, die fest angestellt sind, und solchen, die nur vorübergehend beschäftigt sind, nimmt das BDSG – glücklicherweise – nicht vor.
Die Meldepflicht entfällt allerdings dann, wenn seitens der verantwortlichen Stelle ein Beauftragter für den Datenschutz bestellt wurde, § 4d Abs. 2 BDSG. Ein weiterer Ausnahmetatbestand liegt vor, wenn die Daten für eigene Zwecke erhoben, verarbeitet oder genutzt werden, hierbei in der Regel höchstens neun Personen ständig mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beschäftigt sind und eine Einwilligung des Betroffenen vorliegt (§ 4d Abs. 3 BDSG). Beide Ausnahmetatbestände wurden durch die anfragende Firma nicht vorgetragen, sodass die von ihr geplante Videoüberwachung zu melden war.

Digitale Videoüberwachungen von nicht-öffentlichen Stellen unterfallen generell der Meldepflicht nach § 4d Abs. 1 BDSG, sofern die vorhergehend genannten Ausnahmetatbestände nicht eingreifen. Durch die Entscheidung des Verwaltungsgerichts Saarland vom 18. Mai 2016 Az. 1 K 63/15 wurde diese generelle Meldepflicht nunmehr bestätigt. Der TLfDI stellt auf seiner Website den Unternehmen entsprechende Meldeunterlagen bereit, um den verantwortli-

chen Stellen eine Meldung in das durch den Landesbeauftragten für den Datenschutz zu führende Melderegister nach § 38 Abs. 2 BDSG zu erleichtern und einen Leitfaden an die Hand zu geben. Diese Meldeunterlagen sind auf der Website unter https://www.tlfdi.de/tlfdi/datenschutz/videoüberwachung.de abrufbar.



6.40 Baden und Entspannen unter Beobachtung – Videogaga 18

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) wurde im Rahmen einer Umfrage einer anderen Aufsichtsbehörde um Mitteilung gebeten, inwieweit eine Beurteilung der Zulässigkeit der Videoüberwachung eines bestimmten Spaßbades erfolgt ist. Da ein solches Spaßbad keinen Standort in Thüringen hatte, konnte kein Kontakt festgestellt oder eine Bewertung vorgenommen werden. Kontakte zu Schwimmbädern in Thüringen hatte und hat der TLfDI jedoch in diesem Zusammenhang bereits mehrfach.

Die Videoüberwachung in Schwimmbädern oder Spaßbädern beurteilt sich nach dem Bereich, in dem sie eingesetzt werden soll und dem hierfür festgelegten Zweck unterschiedlich. Insbesondere genießen Schwimmbadbesucher besonderen Schutz, da sie sich im Schwimmbad/Erlebnisbad zum Zweck der Freizeitgestaltung aufhalten und eine Videoüberwachung in diesem Bereich einen sehr intensiven Eingriff in deren informationelles Selbstbestimmungsrecht darstellt. Zum Einsatz von Videoüberwachungen in Schwimmbädern wurde im Rahmen des Düsseldorfer Kreises eine Orientierungshilfe erarbeitet, welche der TLfDI auf seiner Website https://www.tlfdi.de/mam/tlfdi/datenschutz/video/01_zusatz_zur_oh_v__.pdf zur Verfü-



gung stellt. Dort werden die wichtigsten Fakten zur Zulässigkeit von Videoüberwachungen in Schwimmbädern aufgeführt. Die Zulässigkeit der Videoüberwachung beurteilt sich, wenn es sich um Schwimmbäder in privater Trägerschaft handelt, während der Öffnungszeiten nach § 6b Abs. 1 Bundesdatenschutzgesetz (BDSG). Das Beobachten mit Videokameras ist danach nur dann zulässig, soweit dies zur Wahrnehmung des Hausrechts oder berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Auch hier ist immer eine **Einzelfallprüfung** vorzunehmen. Jedoch kann man folgende allgemeine Hinweise geben:

Im Eingangs- und Kassenbereich eingesetzte Videoüberwachung zur Verhinderung des unbefugten Zutritts oder von Manipulationen oder Beschädigungen von Kassenautomaten wird zumeist nicht erforderlich sein. An der Erforderlichkeit fehlt es, wenn der Zweck auch mit anderen, weniger einschneidenden Mitteln erreicht werden kann, z. B. hier durch Positionierung von Kassenautomaten im Sichtfeld des Kassenpersonals oder Erhöhen der Drehkreuze.

Die Überwachung von Umkleidekabinen, Duschen, Saunen und Toilettenräumen als geschützte Bereiche der Intimsphäre stellt einen besonders intensiven Eingriff in das informationelle Selbstbestimmungsrecht der betroffenen Badegäste dar. Eine Videoüberwachung ist dort **immer** unzulässig.

Differenziert sind die Kleider- und Wertspindschließfächer zu betrachten. Sofern eine Trennung von Umkleidekabine und Wertschließfach vorlieg, ist es möglich, den Bereich zu überwachen, jedoch ist darauf zu achten, dass die spärlich bekleideten Badebesucher nicht in den überwachten Bereich gelangen, d. h., die Kameras sind entweder nur auf den Spind zu richten oder den Badegästen ist eine Wahlmöglichkeit zu lassen, indem man Bereiche, die nicht überwacht werden, kennzeichnet. Problematisch wird die Videoüberwachung in jedem Fall dann, wenn die Spindbereiche mit Bänken oder anderen Sitzmöglichkeiten ausgestattet sind. Dann sind diese als Umkleidebereich zu werten, was zur Unzulässigkeit der Videoüberwachung führt.

Die personenscharfe Überwachung des Bade- und Ruhebereichs ist im Regelfall unzulässig. Sofern es nur um die Feststellung von Verstößen gegen die Haus- und Badeordnung geht, stehen die schutzwürdigen Interessen der Badebesucher entgegen. Ein Ausschluss des

Haftungsrisikos gegenüber Ansprüchen von Badegästen ist ebenfalls wegen des Überwiegens schutzwürdiger Interessen von Betroffenen unzulässig. Zudem unterliegt eine mögliche Haftung der Beweispflicht des Geschädigten.
Im Badebereich kann eine Videoüberwachung jedoch zur Unterstützung der Aufsicht in besonders gefahrträchtigen Bereichen (z. B. Sprungtürme, Rutschen, Kinderbecken) in Betracht kommen. Die Gefährlichkeit muss sich aufgrund objektiver Anhaltspunkte ergeben. Der Einsatz der Videoüberwachung kann aber kein Ersatz für die Aufsicht durch das Badepersonal sein, deswegen sind eine Speicherung und eine personenscharfe Videoüberwachung nicht erforderlich. Ein Monitoring ohne personenscharfe Aufnahmen ist hier ausreichend, sofern die Möglichkeit besteht, dass das Badepersonal die Kamerabilder ständig überwacht, um im Notfall schnell eingreifen zu können. Zudem ist darauf hinzuweisen, dass eine reine Aufzeichnung (sog. Black-Box-Verfahren) für rein präventive Zwecke nicht geeignet ist, da dann keine Interventionsmöglichkeit besteht. Das bedeutet, dass eine solche Videoaufzeichnung zur Verhinderung von Unfällen oder gar Straftaten nicht geeignet und damit nicht erforderlich ist.
Die Schwimmbadbetreiber sollten sich generell vor dem Einsatz einer Videoüberwachungsanlage hinsichtlich des Zwecks und auch des Einsatzes von möglichen milderen Mitteln genaue Gedanken machen und ggfs. zuvor den TLfDI um Rat fragen.

Zum Einsatz von Videoüberwachungen in Schwimmbädern wurde im Rahmen des Düsseldorfer Kreises eine Orientierungshilfe erarbeitet, welche der TLfDI auf seiner Website https://www.tlfdi.de/mam/tlfdi/datenschutz/video/01_zusatz_zur_oh_v__.pdf zur Verfügung stellt. Dort werden die wichtigsten Fakten zur Zulässigkeit von Videoüberwachungen in Schwimmbädern aufgeführt. Aufgrund der ab Mai 2018 Geltung erlangenden Europäischen Datenschutz-Grundverordnung (EU-DS-GVO) und des seit

Anfang Juli in Kraft getretenen Anpassungsgesetzes zur EU-DS-GVO können sich hierzu Änderungen ergeben. Alle Orientierungshilfen hinsichtlich von Videoüberwachungen im nicht-öffentlichen Bereich werden entsprechend der neuen Gesetze überarbeitet.

6.41 Videoüberwachung im Restaurant – bei nebulösen Angaben keine Beratung

Während seiner aufsichtsbehördlichen Tätigkeit bekam der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) seitens einer Rechtsanwaltskanzlei eine Beratungsanfrage zu einer Videoüberwachung in einem Restaurantbetrieb. Die Anwaltskanzlei übersandte lediglich eine Skizze, auf der die geplanten Videokameras eingezeichnet waren, sonstige Angaben erfolgten nicht. Grundsätzlich hat die Aufsichtsbehörde nach § 38 Abs. 1 Satz 2 Bundesdatenschutzgesetz (BDSG) die verantwortlichen Stellen sowie die Beauftragten für den Datenschutz auf deren typische Bedürfnisse hin zu beraten. Jedoch ist dabei zu berücksichtigen, dass ein entsprechendes datenschutzrechtliches Konzept vorgelegt werden sollte, damit der TLfDI eine Bewertung zur Zulässigkeit machen kann. Die Zulässigkeit von Videoüberwachungsanlagen beurteilt sich entweder nach § 6b BDSG für öffentlich zugängliche Bereiche oder nach § 28 Abs. 1 Nr. 2 BDSG für den nicht-öffentlich zugänglichen Bereich. Auf Grundlage dieser beiden Erlaubnisnormen ist ein Konzept seitens der verantwortlichen Stellen zu entwickeln. Insbesondere ist zu erarbeiten, welche Zwecke mit der Videoüberwachung verfolgt werden sollen. Darüber hinaus ist bei der Zulässigkeitsprüfung die Erforderlichkeit der Videoüberwachung für diese Zwecke zu erörtern. Insbesondere ist dabei darzustellen, ob es für den genannten Zweck nicht ein anderes gleich geeigneteres Mittel gibt. Die verantwortlichen Stellen sollten sich hier Gedanken über mögliche Alternativen zu der Videoüberwachung machen und Gründe benennen können, warum diese Alternativen nicht ergriffen wurden. Weiterhin muss dargelegt werden, wie ein Eingriff in schutzwürdige Interessen vermieden werden kann oder warum die eigenen Interessen am Betreiben der Videoüberwachung überwiegen. Ferner werden technische Angaben der Videoüberwachungsanlage bzw. jeder einzelnen Kamera benötigt, u. a. Marke/Typenbezeichnung der Kamera, Schwenk- und Zoomfähigkeit, Audiofunktion, Auflösung (bestmögliche), Sichtwinkel, Beobachtung (Monitoring) oder Aufzeichnung

sowie Dauer der Speicherung, Löschung der Daten, Personenabgleich/Gesichtserkennung. Zusätzlich zu den technischen Angaben der Kameras sind schriftliche Festlegungen in Form von technisch-organisatorischen Maßnahmen gem. § 9 Satz 1 BDSG zu treffen, um die datenschutzgerechte und sichere Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten zu erreichen. Hier können insbesondere Speicherfristen, Betriebszeiten, Zugriffsschutz, Zugangskontrollen etc. festgelegt werden. Diese Angaben wurden allesamt seitens des Mandanten der Rechtsanwaltskanzlei nach Anforderung nicht gemacht, sodass eine abschließende Beratung nicht erfolgen konnte.

Die verantwortlichen Stellen sollten bei einer gewünschten Beratung im Rahmen einer Videoüberwachung durch den TLfDI ein den vorgenannten Angaben entsprechendes datenschutzrechtliches Konzept vorlegen. Hilfreich können hierzu das auf der Homepage des TLfDI hinterlegte Erfassungsblatt für Kameras (https://www.tlfdi.de/mam/tlfdi/datenschutz/video/video__berwachung_erfassungsblatt_kameras.pdf) sowie die Orientierungshilfe des Düsseldorfer Kreises (https://www.tlfdi.de/mam/tlfdi/datenschutz/video/oh-v__-durch-nicht-__ffentliche-stellen.pdf) sein. In diesem Zusammenhang wird darauf hingewiesen, dass am 25. Mai 2018 die Europäische Datenschutz-Grundverordnung (DS-GVO) Geltung in allen Mitgliedstaaten der Europäischen Union erlangen wird. Auch aufgrund des zwischenzeitlich am 5. Juli 2017 in Kraft getretenen Anpassungsgesetzes zur EU-DS-GVO werden sich Änderungen hinsichtlich der rechtlichen Grundlagen, aufgrund derer eine Videoüberwachung in Deutschland durchgeführt werden kann, ergeben. Die bis jetzt geltenden Grundsätze in der Orientierungshilfe des Düsseldorfer Kreises für den nicht-öffentlichen Bereich werden insofern an die neue Rechtslage angepasst und überarbeitet.

6.42 Datenschutz: durchgesetzt! – Videogaga 19

Ein weiterer Fall in Sachen Videoüberwachung beschäftigt den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) immer noch. Bereits im 2. Tätigkeitsbericht zum Datenschutz im nicht-öffentlichen Bereich unter Punkt 4.61 wurde darüber berichtet, dass ein Betreiber einer Videoüberwachungsanlage nicht einsichtig war, dass auch für ihn die gesetzlichen Bestimmungen gelten. Er verweigerte die Beantwortung des Fragenkatalogs vom TLfDI, da es sich um ausgemusterte Vorführgeräte handele und er demzufolge die Fragen nicht beantworten würde. Der Betreiber sollte unter anderem Auskunft darüber geben, auf welche Bereiche die Kameras ausgerichtet sind und er sollte die Ausrichtung mittels eines Lageplans darstellen. Auch wenn es sich um Kameraattrappen handeln sollte, ist der Betreiber gesetzlich verpflichtet, dem Auskunftsersuchen des TLfDI nach § 38 Abs. 3 Bundesdatenschutzgesetz (BDSG) nachzukommen und es nicht einfach zu verweigern. Zum Abschluss des Verwaltungsverfahrens ist es bis jetzt noch nicht gekommen.

Wie auch im vorherigen Tätigkeitsbericht schon deutlich zum Ausdruck gebracht, hat der TLfDI als zuständige Aufsichtsbehörde das Mittel der Anordnung unter Androhung eines Zwangsgeldes, um Auskünfte zu erhalten. Denn nur wenn der Sachverhalt feststeht, können rechtliche Bewertungen vorgenommen werden. Zum Mittel des Auskunftsbescheides wird allerdings nur gegriffen, wenn vorher auf einfache Schreiben hin keine Auskunft erteilt wird.

6.43 Wenn der Datenschutz zweimal klingelt

Im 2. Tätigkeitsbericht zum Datenschutz im nicht-öffentlichen Bereich wurde unter dem Punkt 4.62 über eine installierte Videoüberwachungsanlage eines Hausbesitzers berichtet. Die Videoüberwachungskamera war am Balkon des Hauses angebracht. Wie der Betreiber auf Nachfrage mitteilte, sei lediglich eine Kameraattrappe installiert und er sähe darin keinen datenschutzrechtlichen Verstoß nach dem Bundesdatenschutzgesetz (BDSG). Der Betreiber teilte jedoch dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) mit, dass die Attrappe abgebaut wurde.

Leider war die Sache damit beim TLfDI nicht abgehakt. Um sicher zugehen, dass die Auskunft des Betreibers auch stimmte, bat der TLfDI die zuständige Stadtverwaltung um Amtshilfe mittels einer Vor-Ort-Kontrolle. Diese stellte dabei fest, dass zwar die Kameraattrappe am Balkon abgebaut wurde, sich jedoch eine weitere Videoüberwachungskamera auf dem Grundstück befand. Der Hausbesitzer filmte nun von seinem Carport aus Teile seines Hofgrundstücks und die Einfahrt.
Daraufhin wandte sich der TLfDI erneut an den Betreiber, um zu klären, ob die Kamera datenschutzkonform nach § 6b BDSG betrieben wird. Hierbei kommt es insbesondere auf die Ausrichtung der Kamera an und darauf, welche Bereiche sie abbildet. Wenn die Kamera das eigene Grundstück erfasst und öffentlich zugängliche Räume nicht erfasst werden oder durch die Videoüberwachung nicht auf eine andere Weise die persönliche Sphäre verlassen wird, wie dies zum Beispiel durch Erfassen eines Nachbargrundstücks der Fall wäre, ist der Anwendungsbereich des BDSG gemäß § 1 Abs. 2 Nr. 3 schon nicht eröffnet. Der Betreiber bestätigte gegenüber dem TLfDI, dass durch die Kamera keine öffentlich zugänglichen Bereiche des Grundstücks erfasst, also keine Personen gefilmt werden, die auf sein Grundstück gehen müssen, um an der Haustür zu klingeln, an die Haustür zu gelangen und an den Briefkasten zu kommen. Somit konnte in diesem Fall festgestellt werden, dass eine unzulässige Erhebung von personenbezogenen Daten ausgeschlossen ist und der Betreiber konnte die Videoüberwachungsanlage weiter für seine privaten Zwecke nutzen.

Datenschutzrelevant ist der Erfassungsbereich der Kamera auf dem Grundstück. Hier muss unterschieden werden, ob es sich beim Aufnahmebereich um einen öffentlich zugänglichen Bereich handelt oder nicht. Sollte die Videoüberwachung den nicht-öffentlich zugänglichen Bereich erfassen, dann sind die Regelungen im BDSG nur maßgebend, sobald auch das Nachbargrundstück oder fremde Personen aufgenommen werden. Das BDSG greift nicht, wenn nur das eigene Grundstück gefilmt wird, Allerdings ist für den öffentlich zugänglichen Bereich (z. B. der Hauseingang) § 6b BDSG einschlägig.

6.44 Videoüberwachung versus Vandalen

Was wäre der Datenschutz ohne den aufmerksamen Bürger? Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) erhält regelmäßig von Bürgern den Hinweis auf Videoüberwachungsanlagen. Auch im folgenden Fall entdeckte ein Bürger drei Videokameras an einer Garage in Erfurt. Er informierte zunächst die Erfurter Stadtverwaltung. Die Mitarbeiter der Stadtverwaltung reagierten sofort und leiteten die Beschwerde zuständigkeitshalber an den TLfDI weiter.

Der TLfDI wandte sich im Zuge eines Auskunftsverlangens nach § 38 Abs. 3 BDSG an den Nutzer der Garage. Der Besitzer der Garage und somit auch Betreiber der Videokameras wurde aufgefordert, Auskunft über die Videoüberwachungsanlage zu geben, unter anderem, welche Bereiche gefilmt werden und zu welchem Zweck die Videoüberwachung dient. In seiner Antwort begründete der Betreiber, dass er des Öfteren Opfer von Vandalismus auf seinem Grundstück gewesen sei und dies auch mehrfach zur Anzeige bei der Polizei gebracht hätte. Außerdem führte er aus, dass er mit den Videokameras lediglich die „Vandalen“ abschrecken möchte. Seine Kameras waren so ausgerichtet, dass Bereiche vor der Garage gefilmt wurden; über weitere Funktionen wie Zoom- oder Schwenktechnik verfügen die Kameras nicht. Die Nachbargrundstücke waren über feste Filter ausgeblendet. Mit Hinweisschildern an der Garage wurde auf die Videokameras hingewiesen.

Bei einer Videoüberwachung werden aufgrund der Beobachtung personenbezogene Daten erhoben und – sofern die Aufnahmen aufgezeichnet werden – gleichzeitig verarbeitet. Dies ist nur dann zulässig, soweit das Bundesdatenschutzgesetz (BDSG) oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder die Betroffenen eingewilligt haben, § 4 Abs. 1 BDSG. Im Falle einer Videoüberwachung scheidet eine Einwilligung der Betroffenen bereits aus logischen Gründen aus, da überhaupt nicht absehbar ist, welche Personen in den Bereich der Videoüberwachung gelangen. Es verbleibt daher bei der Notwendigkeit einer Rechtsvorschrift, die die Videoüberwachung erlaubt. Einschlägige Rechtsvorschrift bei der Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen ist § 6b BDSG. Hierzu ist im § 6bAbs. 1 Nr. 1 bis 3 BDSG klar definiert, unter welchen Voraussetzungen Videoüberwachung bei der Beobachtung von öffentlich zugänglichen Räumen

zulässig ist. So ist nach § 6bAbs. 1 Nr. 1 BDSG Videoüberwachung nur zulässig, soweit sie zur Aufgabenerfüllung öffentlicher Stellen erforderlich ist, nach § 6bAbs. 1 Nr. 2 BDSG zur Wahrung des Hausrechts und nach § 6bAbs. 1 Nr. 3 BDSG zur Wahrung berechtigter Interessen für konkret festgelegte Zwecke. Bei allen drei Varianten muss die Videoüberwachung erforderlich sein und es dürfen keine Anhaltspunkte bestehen, dass das schutzwürdige Interesse der Betroffenen überwiegt.
Eine Überwachung öffentlich zugänglicher Räume liegt z. B. vor, wenn außer einem privaten Grundstück auch der öffentliche Verkehrsraum in der Umgebung und die dort befindlichen Personen erfasst werden können. Durch die Videoüberwachungsanlage wurde öffentlich zugänglicher Raum im Sinne des § 6b BDSG miterfasst. Nach § 6b Abs. 1 Nr. 2 BDSG beinhaltet das Hausrecht die Befugnis, darüber zu entscheiden, wer bestimmte Gebäude oder befriedetes Besitztum betreten und darin verweilen darf. Der Inhaber des Hausrechts ist daher berechtigt, die zum Schutz des Objekts und der sich darin aufhaltenden Personen sowie die zur Abwehr unbefugten Betretens erforderlichen Maßnahmen zu ergreifen, d. h. Störer zu verweisen und ihnen das Betreten für die Zukunft zu untersagen. Eine Beobachtung zur Wahrnehmung des Hausrechts kann zum einen präventive Zwecke verfolgen, indem Personen davon abgehalten werden sollen, Rechtsverstöße – z. B. Sachbeschädigungen durch Graffiti und Beschädigungen an Garagentüren innerhalb des vom Hausrecht umfassten Bereichs – zu begehen (Störerabwehr), vgl. Scholz, in: Simitis, BDSG, § 6b Rn. 75, 8. Auflage. Dabei reicht aber die Beobachtungsbefugnis des Hausrechtsinhabers nur bis an die Grenzen des Grundstücks und nach der Rechtsprechung einen Meter darüber hinaus, vgl. AG Berlin-Mitte vom 18. Dezember 2003 Az.: 16 C 427/02. Die dargelegten Gründe zur Wahrung des Hausrechts können ein berechtigtes Interesse des Betreibers der Videoüberwachungsanlage sein, demgegenüber stehen jedoch die schutzwürdigen Interessen der Betroffenen. Berechtigte Interessen, beispielsweise der Schutz des Eigentums, stehen in diesen Fällen hinter den schutzwürdigen Interessen der Personen, die in den Erfassungsbereich der Kamera geraten, wie Nachbarn, Passanten und sonstige Verkehrsteilnehmer, in der Regel zurück. Die zur Überwachung und zum Schutz des eigenen Grundstücks zulässig eingesetzte Videoüberwachungstechnik darf daher nicht zur Folge haben, dass – quasi nebenbei – auch anliegende öffentliche Wege und die sich dort auf-

haltenden Personen mit überwacht werden. Aus den vorgelegten Aufnahmen ergab sich, dass der angrenzende Gehweg zur Garagenfassade lediglich einen Meter betrug und weitere Grundstücke gefiltert/geschwärzt wurden. Der Betreiber der Videoüberwachungskameras stützte sich auf sein Hausrecht. Da sich der Kameraaufnahmebereich innerhalb des einen Meters an der Garagenfassade erstreckte und ausreichend Raum zum Ausweichen gegeben war sowie die angrenzenden Grundstücke gefiltert bzw. geschwärzt waren, beurteilte der TLfDI die Videoüberwachungsanlage zur Wahrung des Hausrechts nach § 6b Abs. 1 Nr. 2 BDSG als zulässig. Das Verwaltungsverfahren wurde daher als erledigt angesehen.

In Thüringen tauchen vermehrt im privaten Bereich Videoüberwachungskameras auf. Dabei gelten auch für den privaten Bereich die Regeln des Datenschutzrechts. Werden diese nicht eingehalten, drohen Verwaltungs- und Bußgeldverfahren .

6.45 Insolvenz schützt nicht vor Datenschutz – Videogaga 20

Aufgrund seiner Kontrolltätigkeit wurde dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) bekannt, dass an zwei Wohnblöcken in Ostthüringen eine Videoüberwachung mit jeweils drei Videokameras betrieben wurde. Die Kameras waren auf den Eingangsbereich der Wohngebäude und teilweise auf den öffentlichen Gehweg sowie Straßenbereich gerichtet. Die Eigentümerin wurde mittels Auskunftsersuchen des TLfDI angeschrieben, da diese u. U. verantwortliche Stelle gem. § 3 Abs. 7 Bundesdatenschutzgesetz (BDSG) ist. Das Schreiben kam jedoch als Postrückläufer zurück. Die weiteren Ermittlungen ergaben, dass die Eigentümerin insolvent war. Der für das Vermögen der Eigentümerin bestellte Insolvenzverwalter wurde seitens des TLfDI angeschrieben und um Mitteilung gebeten, ob das Insolvenzverfahren zwischenzeitlich beendet wurde und wer nun Eigentümer der Gebäude ist. Der Insolvenzverwalter teilte sodann mit, dass das Verfahren immer noch andauere. Daraufhin wandte sich der TLfDI mit dem Auskunftsersuchen an den Insolvenzverwalter, da nach § 80 Abs. 1 Insolvenzordnung (InsO) das Recht des Schuldners, das zur Insolvenzmasse gehörende Vermögen zu verwalten, auf den Insolvenzverwalter übergeht. Insofern tritt der Insolvenzverwalter an die Stelle

der Eigentümerin der Gebäude. Das Verfahren dauert beim TLfDI noch an.

Verantwortliche Stelle ist nach § 3 Abs. 7 BDSG jede verantwortliche Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt. Im vorliegenden Fall trat an die Stelle der bisherigen Eigentümerin aufgrund des eröffneten Insolvenzverfahrens deren Insolvenzverwalter. Nach § 80 Abs. 1 InsO geht das Recht des Schuldners, das zur Insolvenzmasse gehörende Vermögen zu verwalten, auf den bestellten Insolvenzverwalter über. Der Betrieb der Videoüberwachungsanlage gehört zur Verwaltung des Eigentums, sodass der Insolvenzverwalter als verantwortliche Stelle i. S. d. BDSG zu betrachten ist.

6.46 Hinweis auf Videoüberwachung, aber wo ist die Kamera?

Aufgrund der Mitteilung einer Polizeiinspektion wurde dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) bekannt, dass an einer Bushaltestelle sowie an einem dort befindlichen Gebäude Hinweisschilder einer dort vermeintlich betriebenen Videoüberwachung angebracht wurden. Videokameras konnten aber auch nach Inaugenscheinnahme durch die Polizei weder im Bereich der Bushaltestelle noch an dem dahinter befindlichen Grundstück festgestellt werden. Der TLfDI wandte sich daher zunächst mit einem Auskunftsverlangen an die mögliche verantwortliche Stelle der Videoüberwachung, den Eigentümer des Grundstücks. Dieser teilte dem TLfDI mit, dass sich auf dem Grundstück und an der Bushaltestelle keine Kameras befinden würden. Und er könne Schilder anbringen wie er wolle. Da die Polizei keine Videokameras feststellen konnte, musste das Verwaltungsverfahren beim TLfDI abgeschlossen werden. Nach § 38 Abs. 5 Satz 1 Bundesdatenschutzgesetz (BDSG) kann der TLfDI nur Maßnahmen zur Beseitigung festgestellter Verstöße bei der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten oder technischer oder organisatorischer Mängel anordnen. Eine Videokamera wurde vorliegend nicht angebracht, sodass kein Datenschutzverstoß festgestellt werden konnte. Jedoch stellen nach Auffassung des TLfDI die angebrachten Hinweisschilder möglicherweise einen Eingriff in das allgemeine Persönlichkeitsrecht der Passanten oder der Wartenden an der Bushaltestelle dar. Die Betroffenen können sich nicht sicher sein, ob sich

in der Nähe eine Kamera befindet, welche Aufnahmen macht, selbst wenn diese nicht zu sehen ist. So wird auch in diesem Fall aufgrund des Hinweisschildes ein gewisser Überwachungsdruck auf die Passanten ausgeübt, was letztendlich zu einem Eingriff in deren allgemeines Persönlichkeitsrecht führen kann. Es können daher möglicherweise zivilrechtliche Ansprüche der Betroffenen gegen den Eigentümer des Grundstücks bestehen.

Die Ermächtigungsbefugnis des TLfDI, Anordnungen zur Beseitigung von festgestellten Mängeln und Verstößen bei der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten oder technischer oder organisatorischer Mängel zu treffen, ergibt sich aus § 38 Abs. 5 Satz 1 BDSG. Sofern kein datenschutzrechtlicher Verstoß seitens des TLfDI festgestellt werden kann, bedeutet dies nicht, dass nicht auch daneben bestehende zivilrechtliche Abwehransprüche im Rahmen der Verletzung des allgemeinen Persönlichkeitsrechts vorliegen können.

6.47 Betreiber einer Videoüberwachung? – Ja Nein Vielleicht; Videogaga 21

Eine Thüringer Stadtverwaltung (SV) bat den Thüringer Landesbeauftragten für den Datenschutz die die Informationsfreiheit (TLfDI) um Unterstützung und Aufklärung zu einer an einem Gebäude angebrachten Videoüberwachung. Nach Mitteilung der SV waren zwei Kameras am Gebäude angebracht. Das Gebäude gehörte wohl einer Privatperson. Außerdem hatte ein Unternehmen Räumlichkeiten im Gebäude angemietet. Die SV belegte dies durch entsprechende Auszüge aus dem Grundbuchamt und durch Fotos.
Der TLfDI wandte sich daraufhin mit einem Auskunftsverlangen gemäß § 38 Bundesdatenschutzgesetz (BDSG) an den Eigentümer, aber auch an das Unternehmen, um in Erfahrung zu bringen, wer letztlich Betreiber – und somit Eigentümer – der Kameras – und damit verantwortliche Stelle i. S. d. § 3 Abs. 7 BDSG – sei.
Das Unternehmen erklärte dem TLfDI, dass es nicht mehr Mieter in diesem Gebäude und damit auch nicht verantwortlich für die Betreibung der Kameras sei. Des Weiteren teilten es mit, dass die Kameras bereits vor seinem Einzug in das Gebäude installiert gewesen waren.

Der Eigentümer des Gebäudes nahm ebenfalls Stellung zum Auskunftsverlangen. Er erklärte, dass er zwar Eigentümer des Gebäudes sei, allerdings nicht Betreiber der Videoüberwachung.
Für den TLfDI war die Rechtslage aufgrund der vorliegenden Fakten undurchsichtig und er recherchierte weiter. Es musste letztlich geklärt werden, ob das Unternehmen nun noch Mieter ist oder nicht und wer die Kameras angebracht hatte. Es stellte sich zwar heraus, dass es ein gerichtliches Verfahren zwischen Vermieter und Mieter gab, in dessen Rahmen auch über die Mietzinsen gestritten wurde. Leider konnte auch hieraus nicht abgeleitet werden, wer die Kameras tatsächlich betreibt. Allerdings wurde vom Vermieter eingeräumt, dass die Kameras bereits vor Übergabe an den Mieter installiert waren. Auch war der Mieter nicht mehr im Objekt und hatte auch keine Möglichkeit mehr, auf die Kameras einzuwirken. Zwar wurde er im Zivilprozess zur Mietzinszahlung verurteilt, jedoch handelte es sich nur um Versäumnisurteile. Solche Urteile kommen dann zustande, wenn eine Partei, hier der Mieter, nicht zum Termin erscheint. Da es sich beim Zivilprozess um einen Parteienprozess handelt, werden somit nur noch die Ausführungen der anderen Partei auf Schlüssigkeit geprüft und auf dieser Grundlage wird der Prozess entschieden. Mit anderen Worten: Aus einem Versäumnisurteil lassen sich auch keine tatsächlichen Umstände ableiten, sondern es handelt sich nur um überprüfte Aussagen einer Partei.
Da der Mieter somit nicht mehr als verantwortliche Stelle in Betracht kam und der Vermieter in einem anderen Bundesland wohnte, gab der TLfDI das Verfahren an die Kollegen des anderen Bundeslandes ab und informierte diese über den Sachstand. Kurz darauf informierten die Kollegen des anderen Bundeslandes darüber, dass die Sache im Sinne des Datenschutzes geklärt wurde, jedoch ohne näher auf weitere Einzelheiten einzugehen.

Gemäß § 42 Abs. 1 Thüringer Datenschutzgesetz i. V. m. § 38 Abs. 6 BDSG ist der TLfDI als sachlich zuständige Behörde zur Kontrolle der Ausführung des BDSG sowie anderer Vorschriften über den Datenschutz ermächtigt, § 38 Abs. 1 Satz 1 BDSG. Allerdings richtet sich die örtliche Zuständigkeit nach den Verwaltungsverfahrensgesetzen der Länder. Befindet sich die verantwortliche Stelle außerhalb von Thüringen, dann sind in der Regel die Kollegen des anderen Landes zuständig. Ausnahmen gibt es nur bei selbstständigen Niederlassungen von Unternehmen. Hier kann der TLfDI

tätig werden, selbst wenn das Unternehmen seinen Hauptsitz in einem anderen Bundesland hat.

6.48 Geschützte Fassaden

Im Rahmen seiner aufsichtsbehördlichen Tätigkeiten ist der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) darauf aufmerksam gemacht worden, dass an der Dachrinne eines Gebäudes eine Kamera installiert sei, die auch die öffentlichen Gehwege und die Straße erfasse.
Der TLfDI hat sich daraufhin mit einem Auskunftsverlangen nach § 38 Abs. 3 Bundesdatenschutzgesetz (BDSG) an die Beschwerdegegnerin gewandt und bat um die Beantwortung eines Fragenkataloges.
Diese äußerte hierauf, dass es sich bei der an ihrem Haus angebrachten Kamera lediglich um eine Attrappe handele. Da sie im Erdgeschoss sehr große Fenster habe und einige ihrer Nachbarn bereits Opfer von Vandalismus geworden seien, habe sie die Kameraattrappe zu ihrem eigenen Schutz angebracht. Sie hoffte, damit gewaltbereite Täter abschrecken zu können. Dafür sei es erforderlich, dass die Dummy-Kamera einer echten Kamera täuschend ähnlich sähe.
Leider hatte sich die Angelegenheit damit noch nicht, wie sie annahm, erledigt.
Der TLfDI geht im Falle der Videoüberwachung davon aus, dass die Vorschriften des BDSG sinngemäß auch auf Kameraattrappen anzuwenden sind, weil der durch diese ausgelöste Überwachungsdruck dem einer funktionsfähigen Kamera entspricht und somit ein ähnlicher Eingriff in das Persönlichkeitsrecht vorgenommen wird wie durch eine tatsächlich funktionierende Kamera.
In einem für den Datenschutz als Meilenstein geltendem Urteil hatte das Bundesverfassungsgericht das Recht auf informationelle Selbstbestimmung als Ausfluss des allgemeinen Persönlichkeitsrechts und der Menschenwürde als Grundrecht anerkannt. Anlass für diese Entscheidung war ein Volkszählungsgesetz, mit welchem Daten von allen Bürgern gesammelt werden sollten.
Kernaussage dieses Urteiles ist Nachfolgendes:
„Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist,

ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. […] Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist. Hieraus folgt: Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. Dieser Schutz ist daher von dem Grundrecht des Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 Grundgesetz umfasst. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.“ (BVerfG, Urteil vom 15. Dezember 1983 Az. 1 BvR 209/83, 1 BvR 484/83, 1 BvR 420/83, 1 BvR 362/83, 1 BvR 269/83, 1 BvR 440/83 [Volkszählungsurteil]).

Diese dort aufgestellten Grundsätze gelten auch für das Installieren von Kameraattrappen, da hier der Eindruck einer echten Kamera erweckt werden soll, sodass der Betroffene nicht weiß, wer was wann und bei welcher Gelegenheit über ihn weiß.

So hat das Landgericht Darmstadt entschieden, dass das Aufstellen einer funktionsfähig aussehenden Videokamera-Attrappe mit der Ausrichtung des Objektivs auf den Hauseingangsbereich eines Mehrparteienhauses und die darin liegende konkludente Androhung einer dauernden Videoüberwachung rechtswidrig das allgemeine Persönlichkeitsrecht der Mieter (und ihrer jeweiligen Besucher) verletzt (LG Darmstadt, Urteil vom 17. März 1999 Az. 8 O 42/99).

Daher bat der TLfDI die Beschwerdegegnerin, ihm mitzuteilen, welche Bereiche die von ihr installierte Kameraattrappe zu erfassen scheint.

Sie erwiderte, die am Haus angebrachte Kameraattrappe sei so ausgerichtet, dass sie den Anschein erwecke, die Fenster im Erdgeschoss zu erfassen. Eine Überwachung im öffentlich zugänglichen Bereich, hier von Fenstern und Fassade, ist nur unter bestimmten Umständen rechtlich zulässig. Insofern ist auch bei der Verwendung von Attrappen zu prüfen, ob die datenschutzrechtlichen Vorgaben zur Beobachtung dieser Bereiche nach § 6b BDSG eingehalten wer-

den. Die Anwendung der vorgenannten Norm setzt voraus, dass ein öffentlich zugänglicher Raum beobachtet wird. Hierbei handelt es sich, wie vorliegend, um Bereiche innerhalb oder außerhalb von Gebäuden, die nach dem erkennbaren Willen des Berechtigten von jedermann genutzt oder betreten werden dürfen.
Nach § 6b Abs. 1 Nr. 2 BDSG ist das Beobachten öffentlich zugänglicher Räume per Videoüberwachung zulässig, soweit es zur Wahrnehmung des Hausrechts für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte für das Vorliegen überwiegender schutzwürdiger Interessen der betroffenen Personen bestehen. Ein berechtigtes Interesse für den Betrieb einer Videoüberwachungsanlage kann ideeller, wirtschaftlicher oder rechtlicher Natur sein. Soll – wie hier – die Videoüberwachung dazu eingesetzt werden, vor Vandalismus zu schützen, ist darin grundsätzlich ein berechtigtes Interesse zu sehen, wenn eine tatsächliche Gefahrenlage nachgewiesen werden kann.
In ihrem Schreiben hatte die Beschwerdegegnerin solche Vorkommnisse genannt. Ziel der von ihr durchgeführten vermeintlichen Videoüberwachung mittels der Kameraattrappe sei die Verhinderung von Beschädigungen durch die abschreckende Wirkung der Kameraattrappe. Dieses Ziel stellt ein berechtigtes Interesse dar, dessen Zweck konkret festgelegt wurde. Die vermeintliche Videoüberwachung der Fassade mittels der Attrappe ist auch als erforderlich anzusehen. Sie ist geeignet, die von ihr genannten Zwecke zu erreichen und es ist kein Mittel ersichtlich, welches bei gleicher Zumutbarkeit weniger stark in die Rechte Dritter eingreifen würde.
Bei der Wahrnehmung des Hausrechts nach § 6b Abs. 1 Nr. 2 BDSG endet die Beobachtungsbefugnis des Hausrechtsinhabers grundsätzlich an den Grundstücksgrenzen. Daneben lässt die Rechtsprechung (vgl. AG Berlin-Mitte vom 18. Dezember 2003 Az.: 16 C 427/02) im Einzelfall zu, dass der öffentliche Verkehrsraum in einer Breite von bis zu einem Meter mitaufgenommen wird.
Dies konnte die Beschwerdegegnerin – bildlich dokumentiert – dadurch gewährleisten, indem sie – nach dem Hinweis des TLfDI – die Kameraattrappe deutlich näher (ein Meter) auf ihre Fassade ausrichtete. Damit war das Verfahren für den TLfDI beendet.

Die Videoüberwachung des eigenen, allein genutzten Grundstücks ist regelmäßig zulässig. Die Beobachtungsbefugnis des Hausrechtsinhabers im Sinne des Datenschutzes endet dabei grundsätzlich an

den Grundstücksgrenzen. Daneben lässt die Rechtsprechung je nach der Ausgestaltung des Einzelfalls zu, dass der öffentliche Raum in einer Breite von bis zu einem Meter aufgenommen wird. Voraussetzung hierfür ist jedoch, dass ausreichend Ausweichfläche verbleibt, um der Videoüberwachung ausweichen zu können. Diese Grundsätze sind auch auf Kameraattrappen anzuwenden, weil der durch diese Kameras ausgelöste Überwachungsdruck denen funktionsfähiger Kameras entspricht und somit ähnliche Eingriffe in das Persönlichkeitsrecht vorgenommen werden wie durch tatsächlich funktionierende Kameras.

6.49 Die überwachte Datsche

Der Pächter einer Parzelle in einer Gartenanlage in Thüringen suchte das Gespräch mit dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Er habe ein Problem mit einem Nachbarn, der glaube, sein Grundstück werde vom Anfragenden überwacht.
Auf dem von ihm näher beschriebenen Grundstück betreibe er eine Videoüberwachungsanlage, bestehend aus vier Kameras. Die Kameras seien zum Teil auch auf benachbarte Grundstücke ausgerichtet. Zwischen seiner Parzelle und der streitbefangenen Nachbarparzelle befinde sich eine etwa zweieinhalb Meter hohe und einen Meter breite Hecke. Dahinter wiederum befinde sich ein blickdichter Zaun. Seine Videoüberwachungsanlage beträfe zwar auch Teile der Nachbargrundstücke, ihr tatsächlicher Sichtbereich beschränke sich – aufgrund technischer Vorkehrungen an den Kameras – ausschließlich aber auf sein Grundstück. Der Himmel über der Hecke zum streitgegenständlichen Nachbargrundstück sei ebenso ausgeschwärzt wie die teilweise seitlich auch noch mit erfassten Nachbarparzellen. Von diesen Grundstücken sei kameratechnisch nicht das Geringste zu erkennen.
Als Beweis dafür legte er Dokumente vor, die dies bestätigen.
Nach der dem TLfDI dargebotenen Sachlage war die Videoüberwachungsanlage datenschutzkonform und von seiner Seite nicht zu beanstanden.

Den nicht im Fokus stehenden Teil des Erfassungsbereiches einer Kamera unkenntlich zu machen, kann auf verschiedenen Wegen erreicht werden. Diese Bereiche können zum einen auf digitaler

Ebene geschwärzt oder unscharf gemacht werden (verpixeln). Zum anderen kann dieser Bereich der Linse mechanisch entsprechend bearbeitet werden.

6.50 Hausrecht – Video

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) wurde darauf aufmerksam gemacht, dass an einem Fenster im ersten Obergeschoss eines Gebäudes eine Videokamera angebracht ist, welche vermutlich auf den öffentlichen Bereich des Gehweges gerichtet ist.
Der TLfDI hat sich daraufhin mit einem Auskunftsverlangen nach § 38 Abs. 3 Bundesdatenschutzgesetz (BDSG) an den Beschwerdegegner gewandt und bat um die Beantwortung eines Fragenkataloges.
In Beantwortung dieser Fragen erläuterte der Betreiber der Anlage, dass er mit der für jedermann sichtbaren, installierten Videokamera die Fassade, sein Schaufenster und den Ladeneingang überwache. Dies belegte auch ein im Anhang beigefügter Screenshot, aufgenommen von der Videokamera. Öffentlich zugängliche Bereiche wie die angrenzende Straße waren geschwärzt. Die Videokamera sei nicht schwenkbar und habe keine Zoomfunktion. Es erfolge eine digitale Aufzeichnung auf einem Server, die nach drei Tagen automatisch überschrieben werde. Eine Auswertung finde nur nach Vorkommnissen statt. Als Zweck für die Installation der Videokamera führte er die Beweissicherung bei Diebstählen und Sachbeschädigungen an seinem Gebäude auf. Er sei in der Vergangenheit bereits mehrfach Opfer von Vandalismus, konkret von Graffiti-Schmierereien, sowie von Einbruchsversuchen gewesen. Ein entsprechendes Hinweisschild auf die Videoüberwachung sei angebracht, was der TLfDI auch den beigefügten Bildern im Anhang zu seinem Schreiben entnehmen konnte.
Nach Sichtung der beigefügten Fotos wurde der angrenzende Gehweg und damit öffentlich zugänglicher Raum im Sinne des § 6b BDSG von der Videoüberwachungsanlage miterfasst. Aus den übersandten Aufnahmen ergab sich, dass der Aufnahmebereich des angrenzenden Gehweges zur Hausfassade lediglich einen Meter betrug und weitere öffentlich zugängliche Bereiche (Straße) vom Betreiber unkenntlich gemacht worden sind. Nach § 6b Abs. 1 Nr. 2 BDSG ist das Beobachten öffentlich zugänglicher Räume per Videoüberwa-

chung zur Wahrnehmung des Hausrechts zulässig. Das Hausrecht beinhaltet die Befugnis, darüber zu entscheiden, wer bestimmte Gebäude oder befriedetes Besitztum betreten und darin verweilen darf. Der Inhaber des Hausrechts ist daher berechtigt, die zum Schutz des Objekts und der sich darin aufhaltenden Personen sowie die zur Abwehr unbefugten Betretens erforderlichen Maßnahmen zu ergreifen, d. h. Störer zu verweisen und ihnen das Betreten für die Zukunft zu untersagen. Eine Beobachtung zur Wahrnehmung des Hausrechts kann repressive oder präventive Zwecke verfolgen, indem Personen beispielsweise davon abgehalten werden sollen, Rechtsverstöße – z. B. Sachbeschädigungen durch Graffiti bzw. Beschädigungen an Gebäuden sowie Einbrüche innerhalb des vom Hausrecht umfassten Bereichs – zu begehen. Dabei reicht aber die Beobachtungsbefugnis des Hausrechtsinhabers nur bis an die Grenzen des Grundstücks und nach der Rechtsprechung einen Meter darüber hinaus. Im Einzelfall muss die Beobachtungsbefugnis jedoch in geringem Umfang über die Grundstücksgrenze hinausgehen dürfen und einen Toleranzbereich mitumfassen, wenn dies einer effektiven Überwachung zum Schutze des Eigentumes dient (Urteil des Amtsgerichts Berlin-Mitte vom 18. Dezember 2003 [Aktenzeichen 16 C 427/02]). In diesem Urteil, welches für die Rechtsprechung in diesem Bereich der Videoüberwachung richtungsweisend war und allgemeine Geltung erfahren hat, hatte das erkennende Gericht einen Toleranzbereich von einem Meter ab der Hauswand als vertretbar erachtet.
Im Ergebnis sah der TLfDI die im Fenster installierte Videokamera, ausgerichtet auf die Fassade und den Ladeneingang, im Sinne des § 6b Abs. 1 Nr. 2 zur Wahrnehmung des Hausrechts als datenschutzrechtlich zulässig an. Sie war erforderlich und es bestanden keine Anhaltspunkte für das Vorliegen überwiegender schutzwürdiger Interessen der betroffenen Personen.
Nach § 6b Abs. 5 BDSG sind die Daten unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen. Dabei wird von einer Löschungsfrist von 48 Stunden ausgegangen. In seiner Stellungnahme führte der Beschwerdegegner aus, dass die Daten erst nach drei Tagen automatisch überschrieben werden.
Nachdem er dem TLfDI mitgeteilt hatte, dass nunmehr eine Löschung binnen 48 Stunden erfolge, sah dieser das Verwaltungsverfahren als erledigt an.

Das Hausrecht umfasst die Befugnis, darüber zu entscheiden, wer bestimmte Gebäude oder befriedetes Besitztum betreten und darin verweilen darf. Die Berufung auf das Hausrecht ist datenschutzkonform, wenn es für dessen Wahrung erforderlich ist und keine Anhaltspunkte für das Vorliegen überwiegender schutzwürdiger Interessen der betroffenen Personen bestehen. Spätestens an Grundstücksgrenzen jedoch endet die Beobachtungsbefugnis des Hausrechtsinhabers in der Regel. Darüber hinaus wurde mit Urteil des Amtsgerichts Berlin-Mitte vom 18. Dezember 2003 (Aktenzeichen 16 C 427/02) entschieden, dass eine Videoüberwachungsanlage einen 1 Meter breiten Streifen entlang der Straßenseite sowie einen 1 Meter breiten Streifen links und rechts der Grundstücksgrenzen einschließlich des darüber befindlichen Luftraums aufzeichnen dürfe.

6.51 Mein schöner Garten!

Ein Betroffener wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), weil die Beschwerdegegner auf ihrem Hausgrundstück eine Videoüberwachungsanlage mit drei Kameras betreiben sollen. Alle drei Kameras seien so ausgerichtet, dass sie auch öffentlich zugängliche Bereiche überwachten.
In ihrer daraufhin vom TLfDI erbetenen Stellungnahme haben die Beschwerdegegner eingeräumt, eine solche Anlage auf ihrem Grundstück installiert zu haben. Sie sei aber ausschließlich auf ihr Grundstück gerichtet, sodass kein öffentlich zugänglicher Bereich, sondern nur ihr Garten von der Anlage betroffen sei. Sie hätten die Anlage angebracht, nachdem es mehrfach zu Verletzungen ihrer Persönlichkeits- und Eigentumsrechte gekommen sei. Nach den Einlassungen der Beschwerdegegner handelt es sich bei den Kameras um solche, die zwar geeignet seien, Bilder zu erzeugen und zu speichern, aber aufgrund fehlender Hard- und Software dazu (noch) nicht fähig seien. Bisher seien die Kameras lediglich Attrappen. Die Beschwerdegegner planten in der Folge jedoch, die Anlage „in Funktion“ zu setzen. Vor der „Scharfschaltung“ der Anlage beabsichtigten die Beschwerdegegner, den TLfDI in die Beratung hinsichtlich der Positionierung der einzelnen Kameras miteinzubeziehen. Das angekündigte Miteinbeziehen war bis zum Erstellen dieses Berichtes noch

nicht erfolgt. Aufgrund des Zeitablaufes wird der TLfDI bei den Beschwerdegegnern abklären, wann die „echte“ Inbetriebnahme der Anlage nunmehr geplant ist.
Unabhängig vom Vorstehenden sollte auch bei Verwendung von Attrappen bedacht werden, dass diese ebenfalls in das Persönlichkeitsrecht Dritter eingreifen.
Insoweit wird der TLfDI die oben angeführte Nachfrage nach dem Zeitpunkt der Inbetriebnahme der Anlage mit dem Begehr um Übersendung von Lichtbildern der Kameras sowie der jeweiligen Erfassungsbereiche verbinden und seine Prüfung sodann fortsetzen.

In allen Bereichen, in denen sich der Einsatz „echter“ Kameras verbietet, sollte auch der Einsatz von Kameraattrappen kritisch besehen werden, da in diesen Fällen eine Verletzung des Persönlichkeitsrechts Dritter ebenso vorliegen kann.

6.52 Video bleibt datenschutzrechtlich schwierig!

Ein Bürger wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und beschwerte sich über eine Videoüberwachungsanlage seines Nachbarn. Die Kameras seien wohl so ausgerichtet, dass das Grundstück des Beschwerdeführers und öffentlicher Bereich miterfasst würde.
Der TLfDI wandte sich daraufhin mit einem Auskunftsersuchen nach § 38 Bundesdatenschutzgesetz (BDSG) an den Nachbarn (im Folgenden „Betreiber“ genannt). Diesem wurde mitgeteilt, dass durch eine Videoüberwachungsanlage personenbezogene Daten erhoben und – im Falle einer gleichzeitigen Speicherung der Aufnahmen – auch verarbeitet werden. Dies sei aber nur dann zulässig, wenn dies durch das BDSG oder eine andere Rechtsvorschrift erlaubt wäre. Eine Möglichkeit zur Zulässigkeit dieser Videoüberwachung wäre die Einwilligung des Betroffenen nach § 4 Absatz 1 BDSG. Bei einer Videoüberwachung ist eine Einwilligung allerdings nur schwer einzuhalten, da nicht absehbar ist, welche Personen zu welchem Zeitpunkt in den Erfassungsbereich der Videoüberwachung gelangen könnten. Bei der Überwachung des eigenen Grund und Bodens ist die Zulässigkeit einer Videoüberwachung unter bestimmten Voraussetzungen zulässig. Dies ist der Fall, wenn die Erhebung, Verarbeitung oder Nutzung der Daten ausschließlich für persönliche oder familiäre Tätigkeiten erfolgt, § 1 Abs. 2 Nr. 3 BDSG und keine Per-

sonen von der Videokamera erfasst werden können, die in keiner persönlichen oder familiären Verbindung zum Videobetreiber stehen. Außerdem hat der Betreiber darauf zu achten, dass sich der Erfassungsbereich der Videoüberwachung ausschließlich auf sein eigenes Grundstück richtet.
Der Betreiber bestätigte die Videoüberwachungsanlage und erklärte, dass dies nur zur Abschreckung von Einbrechern diene. Er möchte sich und sein Grundstück schützen. Der Betreiber kooperierte von Anfang an mit dem TLfDI und übersandte detailliertes Bildmaterial von den angebrachten Kameras.
Anhand der übersandten Unterlagen und des Bildmaterials wurde seitens des TLfDI festgestellt, dass eine der Kameras in einer Höhe angebracht ist, in welcher das Filmen des Nachbargrundstücks möglich war. Der Betreiber wurde daraufhin gebeten, diese Kamera so zu versetzen und dies durch Bilder nachzuweisen, dass eine mögliche Aufnahme des Nachbargrundstücks ausgeschlossen werden kann. Der Betreiber kam dieser Aufforderung auch prompt nach. Somit blieb für den TLfDI noch einzig die Prüfung der Kamera am Hauseingangsbereich. Hierzu wurde dem Betreiber mitgeteilt, dass diese Kamera nur dann zulässig ist, sofern ausgeschlossen wird, dass andere Personen erfasst werden. Denn mithilfe der Videoüberwachungsanlage im Hauseingangsbereich wäre es möglich, andere Personen, wie zum Beispiel den Postboten, zu filmen. Zwar ist der Hauseingangsbereich als öffentlich zugänglicher Raum zu betrachten, allerdings würden die schutzwürdigen Interessen der Betroffenen gemäß § 6b BDSG gegen das ausgeübte Hausrecht grundsätzlich nicht überwiegen, sofern auf die Videoüberwachungsanlage hinreichend hingewiesen wird. Durch die Bildnachweise wurde seitens des TLfDI festgestellt, dass sich der Briefkasten und auch die Klingel am Eingangstor befinden. Somit gelangt kein Postbote zwangsläufig in den Erfassungsbereich der Videoüberwachungsanlage. Ebenso hatte der Betreiber ein entsprechendes Hinweisschild angebracht.
Somit waren die Kameras und deren Ausrichtungen mit dem Datenschutz vereinbar.
Der Betreiber bedankte sich für die Hinweise.

Eine Videoüberwachung des eigenen und allein genutzten Grundstückes ist grundsätzlich zulässig. Jedoch nur dann, wenn gemäß § 1 Absatz 2 Nummer 3 BDSG die Erhebung, Verarbeitung oder Nutzung der Daten ausschließlich für persönliche oder familiäre Tätig-

keiten erfolgt und keine Personen, die nicht in einem persönlichen oder familiären Verhältnis zum Betreiber stehen, von der Videokamera erfasst werden können. Zwar wäre es möglich den Postboten oder Besucher zu filmen, das Hausrecht überwiegt allerdings nach § 6b BDSG an der Stelle.

6.53 Alle Wege führen zum Kindergarten: Videogaga 22

Im Rahmen seiner aufsichtsbehördlichen Tätigkeiten hat der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) erfahren, dass auf dem Grundstück der Beschwerdegegner zwei Kameras mit Blickrichtung auf einen Weg bzw. die Straße angebracht worden seien. Der Weg werde als Zugang für den Gemeindekindergarten genutzt. Er sei zwar im Eigentum der Beschwerdegegner, es bestehe aber ein Wegerecht für den dahinterliegenden Kindergarten.
Der TLfDI hat sich daraufhin mit einem Auskunftsverlangen nach § 38 Abs. 3 Bundesdatenschutzgesetz (BDSG) an die Beschwerdegegner gewandt und um die Beantwortung eines standardisierten Fragenkataloges gebeten.
Auf die Anfrage bestätigten die Beschwerdegegner die Installation der Kameras. Der Gemeinde diene der streitgegenständliche Weg als Zuwegung zu ihrem Kindergarten. In den letzten Jahren sei es mehrfach dazu gekommen, dass Eltern unberechtigterweise mit ihren Fahrzeugen die Einfahrt der Beschwerdeführer genutzt hätten, um zum Kindergarten zu fahren oder ihre Fahrzeuge in der Einfahrt abzustellen. Zudem gäbe es auf dem Grundstück des Kindergartens keine ausreichende Umzäunung, sodass viele Bewohner den Weg wochentags und auch am Wochenende benutzten, um auf den Spielplatz zu gehen. Der Gemeinde sei diese Problematik schon länger bekannt. Der eigentliche Grund zum Betreiben einer Videoüberwachungsanlage sei jedoch der Schutz des Eigentums gegen Vandalismus, Einbruch und Diebstahl .
Die Videoüberwachungsanlage sei noch nicht in Betrieb, solle künftig aber den angesprochenen Bereich überwachen. Die Beschwerdegegner möchten als Eigentümer ihr Eigentum schützen, keinesfalls hätten sie jedoch ein Interesse, Unbeteiligte zu überwachen. Zur Dokumentation der Vorfälle möchten sie eine Festplatte installieren.
In seiner Erwiderung bekräftigte der TLfDI, dass es grundsätzlich einer Rechtsvorschrift bedarf, die eine solche Videoüberwachung

erlaubt, es sei denn, es handele sich bei den Aufnahmen um ausschließlich private oder familiäre Tätigkeiten, dann ist das BDSG nicht anwendbar, vgl. § 1 Abs. 2 Nr. 3 BDSG. Entscheidend ist, ob auch Personen von der Videokamera erfasst werden können, die in keiner persönlichen oder familiären Verbindung zum Videobetreiber stehen.
Eine ausschließlich private oder familiäre Tätigkeit war vorliegend nicht gegeben. Das von den Kameras der Beschwerdeführer erfasste Spektrum umfasst auch öffentliche Bereiche, weswegen das BDSG vorliegend einschlägig und der TLfDI für den oben genannten Sachverhalt damit zuständig ist. Die Richtlinie zum Schutz personenbezogener Daten ist auf die Videoaufzeichnung mit einen Überwachungskamera anwendbar, die von einer Person an ihrem Einfamilienhaus angebracht wurde und auf den öffentlichen Straßenraum gerichtet ist (vgl. EUGH, Urteil C-212/13 vom 11. Dezember 2013).
Das Beobachten öffentlich zugänglicher Räume per Videoüberwachung zur Wahrnehmung des Hausrechts bemisst sich nach § 6b Abs. 1 Nr. 2 BDSG. Das Hausrecht beinhaltet die Befugnis, darüber zu entscheiden, wer bestimmte Gebäude oder befriedetes Besitztum betreten und darin verweilen darf. Dabei reicht aber die Beobachtungsbefugnis des Hausrechtsinhabers nur bis an die Grenzen des Grundstücks bzw. einen Meter jenseits der Grundstücksgrenzen, wenn dies zur Wahrnehmung des Hausrechtes erforderlich ist und keine schutzwürdigen Interessen Dritter überwiegen.
Weder Kamera 1 noch Kamera 2 beobachteten damals nur das im Eigentum der Beschwerdegegner stehende Grundstück, sondern auch den mit einer Nutzungsvereinbarung belasteten Weg zum Kindergarten außerhalb ihres Grundstücks bzw. die öffentliche Straße (mehr als einen Meter). Das Eigentum am Grundstück begründet jedoch kein Recht an einer Videoüberwachung anderer berechtigter Grundstücksnutzer im Hinblick auf die Ausübung ihres Wegerechts.
Nach den Ausführungen der Beschwerdegegner kam es ihnen beim Aufstellen der Kameras entscheidend auch darauf an, den Weg zum Kindergarten mitzuerfassen, sodass ein Verstellen des Betrachtungswinkels oder Schwärzen des Aufnahmebereiches keine Alternativen darstellten.
Das Beobachten öffentlich zugänglicher Räume per Videoüberwachung zur Wahrnehmung des Hausrechts begründet daher vorliegend nicht dessen Zulässigkeit.

Nach § 6b Abs. 1 Nr. 3 BDSG ist das Beobachten öffentlich zugänglicher Räume mit einer Videoüberwachung nur zulässig, soweit es zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Ein berechtigtes Interesse für den Betrieb kann ideeller, wirtschaftlicher oder rechtlicher Natur sein. Sollte die Videoüberwachung, wie vorliegend, dazu eingesetzt werden, vor Einbruch und Vandalismus zu schützen, kann darin grundsätzlich ein berechtigtes Interesse gesehen werden, wenn eine tatsächliche Gefahrenlage nachgewiesen werden kann. Zu fordern sind konkrete Tatsachen, aus denen sich eine Gefährdung ergibt.
Die Gefährdungslage muss substantiiert dargelegt werden. Diesem Erfordernis haben die Beschwerdegegner nicht Rechnung getragen.
Im Ergebnis musste der TLfDI feststellen, dass die von den Beschwerdegegnern betriebenen Kameras unzulässig sind.
Die Beschwerdegegner haben die Ausführungen des TLfDI nachvollziehen können und haben datenschutzrechtlich zulässige Zustände geschaffen.

Nach § 6b Abs. 1 Nr. 3 BDSG ist das Beobachten öffentlich zugänglicher Räume mit einer Videoüberwachung zulässig, soweit es zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Ein berechtigtes Interesse für den Betrieb kann ideeller, wirtschaftlicher oder rechtlicher Natur sein. Soll die Videoüberwachung dazu eingesetzt werden, vor Einbruch, Diebstahl und Vandalismus zu schützen, kann darin grundsätzlich ein berechtigtes Interesse gesehen werden, wenn eine tatsächliche Gefahrenlage nachgewiesen werden kann. Zu fordern sind konkrete Tatsachen, aus denen sich eine Gefährdung ergibt, beispielsweise Beschädigungen in nicht nur geringem Ausmaß oder besondere Vorkommnisse in der Vergangenheit.

6.54 Bewachter Parkplatz

Im Rahmen seiner aufsichtsbehördlichen Tätigkeiten hat der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) davon Kenntnis erlangt, dass ein Anwohner an der

Fassade seines Wohnhauses eine Kamera angebracht hat, die auch den öffentlich zugänglichen Bereich überwache.
Daraufhin hat der TLfDI dem Antragsgegner einen Fragebogen zugesandt, in dem dieser dem TLfDI unter anderem erklären sollte, ob er auf seinem Grundstück eine Kamera installiert habe.
Der Beschwerdegegner teilte dem TLfDI mit, dass er in der Tat eine Kameraattrappe auf seinem Grundstück angebracht habe. Diese Kamera sei aber ausschließlich auf sein Grundstück gerichtet. Die Attrappe sei von ihm angebracht worden, um seine – vor der Toreinfahrt und noch auf seinem Grundstück – geparkten Autos vor Vandalismus zu schützen. Es sei schon mehrfach zu Übergriffen auf diese gekommen und er wisse, wer dafür verantwortlich gewesen sei. Leider hätte er dies nicht beweisen können. Seit der Installation der Kamera habe es keine weiteren Vorfälle dieser Art gegeben.
Aus den dem Schreiben beigefügten Unterlagen, dem Lageplan und den Fotos zur Örtlichkeit und der Kameraattrappe selbst wurde für den TLfDI ersichtlich, dass der Beschwerdegegner – entgegen den Ausführungen des Beschwerdeführers – tatsächlich nur das eigene Grundstück überwachte.
Nach § 6b Abs. 1 Nr. 2 Bundesdatenschutzgesetz (BDSG) ist das Beobachten öffentlich zugänglicher Räume mittels Videoüberwachung zur Wahrnehmung des Hausrechts zulässig. Das Hausrecht beinhaltet die Befugnis, darüber zu entscheiden, wer bestimmte Gebäude oder befriedetes Besitztum betreten und darin verweilen darf. Der Inhaber des Hausrechts ist daher berechtigt, die zum Schutz des Objekts und der sich darin aufhaltenden Personen sowie die zur Abwehr unbefugten Betretens erforderlichen Maßnahmen zu ergreifen, d. h. Störer zu verweisen und ihnen das Betreten für die Zukunft zu untersagen. Eine Beobachtung zur Wahrnehmung des Hausrechts kann repressive oder präventive Zwecke verfolgen, indem Personen beispielsweise davon abgehalten werden sollen, Rechtsverstöße – z. B., wie vorliegend, Sachbeschädigungen an den Fahrzeugen des Beschwerdegegners innerhalb des vom Hausrecht umfassten Bereichs – zu begehen. Dabei reicht aber die Beobachtungsbefugnis des Hausrechtsinhabers nur bis zur Grundstücksgrenze bzw. in Ausnahmefällen einen Meter darüber hinaus (Urteil des Amtsgerichts Berlin-Mitte vom 18. Dezember 2003 – Aktenzeichen 16 C 427/02).
Da die Überwachung lediglich das Grundstück des Beschwerdegegners erfasste und keine Anhaltspunkte ersichtlich waren, dass

schutzwürdige Interessen anderer überwiegen, sah der TLfDI den Vorgang als erledigt an.

Das Videoüberwachen öffentlich zugänglicher Räume kann nach § 6b Abs. 1 Nr. 1 BDSG zulässig sein. Das Hausrecht beinhaltet die Befugnis, darüber zu entscheiden, wer bestimmte Gebäude oder befriedetes Besitztum betreten und darin verweilen darf. Der Inhaber des Hausrechts ist daher berechtigt, die zum Schutz des Objekts und der sich darin aufhaltenden Personen sowie die zur Abwehr unbefugten Betretens erforderlichen Maßnahmen zu ergreifen. Diese Beobachtungsbefugnis reicht jedoch lediglich bis zur Grundstücksgrenze bzw. in Ausnahmefällen einen Meter darüber hinaus.

6.55 Planung einer Videoüberwachung – der TLfDI hilft auch hier

Im Berichtszeitraum wurde der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) wegen der Anbringung von Kameraattrappen an einem Gebäude, welches aufgrund der Lage an einem Weltkulturerbe touristisch hochfrequentiert war, angefragt. Das Haus wurde vom Eigentümer gerade frisch saniert. Es kam kurz nach der Sanierung zu Graffitischmierereien an dem Gebäude. Diese konnten zwar wieder entfernt werden, jedoch befürchtete der Eigentümer eine Verwahrlosung der Umgebung um das Gebäude, da in dem Treppenaufgang neben dem Haus Schäden durch das Urinieren von Personen entstanden waren. Der TLfDI machte sich im Rahmen eines Vor-Ort-Termins ein Bild von der Umgebung, um eine entsprechende Beratung durchzuführen. Es sollten insgesamt drei Kameraattrappen an der Hausfassade angebracht werden, um eine abschreckende Wirkung hinsichtlich der eingetretenen Beschädigungen zu erzielen.
Dabei sollten zum einen eine Kameraattrappe an der Rückseite des Gebäudes und zwei an der Hauswand zum Treppenaufgang installiert werden. Dieser Treppenaufgang befand sich zwischen den Gebäuden und war lediglich einen Meter breit.
Nach Auffassung des TLfDI stellen auch Attrappen einen Eingriff in das vom Bundeverfassungsgericht entwickelte Grundrecht auf informationelle Selbstbestimmung dar. Daher sind die Vorgaben des Bundesdatenschutzgesetzes (BDSG) einzuhalten.

Ferner wurde der Eigentümer des Gebäudes darauf hingewiesen, dass auch bei Kameraattrappen, welche, wie in diesem Fall, öffentlich zugängliche Räume erfassen, ein Hinweisschild auf die Videoüberwachung anzubringen ist. Entsprechend § 6b Abs. 2 BDSG ist dieses Hinweisschild in Augenhöhe anzubringen. Der Betroffene muss einschätzen können, welcher Bereich von einer Kamera erfasst wird, damit er in die Lage versetzt wird, gegebenenfalls der Überwachung auszuweichen oder sein Verhalten anzupassen. Außerdem muss die verantwortliche Stelle, welche die Videokameras angebracht hat, erkennbar sein. Daher ist sie grundsätzlich mit ihren Kontaktdaten explizit auf dem Hinweisschild zu nennen. Der Eigentümer des Hauses wurde durch den TLfDI umfassend zu allen Voraussetzungen für eine Installation von Kameras beraten. Bei einem Vor-Ort-Termin mit dem Eigentümer wurden nochmals die möglichen Kamerastandorte in Augenschein genommen und ihre möglichen Erfassungsbereiche sowie die mögliche Beeinträchtigung der Passanten abgeklärt. Der Eigentümer hat sich am Ende aber doch nicht für die Installation von Kameras an dem Gebäude entschieden.

Nach Auffassung des TLfDI stellt auch eine Kameraattrappe einen Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen dar. Diese können nicht wissen, ob die Kamera tatsächlich Aufnahmen macht oder ob es sich lediglich um ein Kameragehäuse handelt. Daher löst auch eine solche Kameraattrappe einen Überwachungsdruck bei den Betroffenen aus.

6.56 Nette Familie

Die Beschwerdeführer wandten sich gegen eine von einem männlichen Familienmitglied installierte Kamera, mittels derer er das von ihnen gemeinsam genutzte und bewohnte Grundstück beobachte.
Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) bat den Betreiber der Anlage u. a. um Auskünfte, welche Bereiche zu welchen Zwecken und seit wann videoüberwacht, auf welche Art und Weise die erhobenen Daten gespeichert und wie lange die Überwachungsdaten aufbewahrt werden.
Daraufhin teilte der Beschwerdegegner mit, dass es sich bei dieser Kamera um eine Attrappe handele, die weder aufzeichnen noch spei-

chern könne. Aufgestellt sei diese nur zur Abschreckung wegen einiger Diebstähle auf seinem Grundstück.
Nach der Auffassung des TLfDI ist der von einer Attrappe ausgelöste Überwachungsdruck dem einer funktionsfähigen Kamera ähnlich, weil damit auch ein Eingriff in die Persönlichkeitsrechte der Betroffenen vorgenommen wird.
Datenschutzrechtlich war die Kamera durch den TLfDI allerdings nicht zu beurteilen. Da der scheinbare Aufnahmebereich der hier streitgegenständlichen Kameraattrappe ausschließlich auf das im Eigentum des Beschwerdegegners befindliche Grundstück gerichtet war und die Aufnahmen ausschließlich zu privaten oder familiären Zwecken diente, war das BDSG nicht anwendbar, § 1 Abs. 2 Nr. 3 BDSG.
Damit musste der TLfDI die Angelegenheit als erledigt ansehen.

Handelt es sich bei den Aufnahmen um ausschließlich private oder familiäre Tätigkeiten, dann ist das BDSG nicht anwendbar, vgl. § 1 Abs. 2 Nr. 3 BDSG Danach findet das Gesetz keine Anwendung auf die Verarbeitung personenbezogener Daten, die eine natürliche Person zur ausschließlich persönlichen Verwendung vornimmt. Die Videoüberwachung des eigenen, allein genutzten Grundstücks ist daher oftmals nicht nach dem BDSG zu beurteilen.

6.57 Kamerainstallation oder nicht, das ist hier die Frage

Im Berichtszeitraum hat der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) Kenntnis davon erlangt, dass ein Bürger auf einem in der Anzeige näher benannten Grundstück auch öffentliche Flächen mit seinen Videokameras überwache.
Im Zuge der Ermittlungen übersandte der TLfDI dem Beschwerdegegner als verantwortlicher Stelle einen Fragebogen zur Beantwortung der genauere Angaben über die (vermeintliche) Videoüberwachung des Beschwerdegegners verlangte.
In seiner Rückantwort wies der Beschwerdegegner die Behauptung, auf seinem Grundstück eine Videoüberwachung durchzuführen, zurück. Auf diesem Grundstück seien weder Kameras noch Kameraattrappen installiert.
Bei der Wahrnehmung seiner aufsichtsbehördlichen Tätigkeit ist der TLfDI mitunter darauf angewiesen, fremde Hilfe in Anspruch zu

nehmen. § 5 Thüringer Verwaltungsverfahrensgesetz (ThürVwVfG) regelt die Voraussetzungen und Grenzen der Amtshilfe auf Behördenebene. Die dort an die Amtshilfe gestellten Voraussetzungen waren vorliegend gegeben.
Gemäß § 38 Thüringer Datenschutzgesetz haben öffentliche Stellen die Pflicht, den Landesbeauftragten für den Datenschutz bei der Erfüllung seiner Aufgaben zu unterstützen. Deshalb wandte sich der TLfDI nochmals an das Ordnungsamt, das ihn seinerzeit auf die Existenz der Kameras hingewiesen hatte, und bat es, die gerügten Kameras zu fotografieren und ihm die entsprechenden Bilder zu übersenden.
Zum Zeitpunkt der Erstellung dieses Berichts war die erbetene Fotodokumentation von den strittigen Kameras noch nicht zur Akte gelangt.
Das weitere Vorgehen des TLfDI hängt von dem Befund ab, der sich aus den noch zu überreichenden Aufnahmen ergibt.

Eine Behörde – vorliegend der TLfDI – kann um Amtshilfe insbesondere dann ersuchen, wenn sie aus rechtlichen Gründen die Amtshandlung nicht selbst vornehmen kann, aus tatsächlichen Gründen, wenn die zur Vornahme der Amtshandlung erforderlichen Dienstkräfte oder Einrichtungen fehlen, sie die Amtshandlung nicht selbst vornehmen kann, sie zur Durchführung ihrer Aufgaben auf die Kenntnisse von Tatsachen angewiesen ist, die ihr unbekannt sind und die sie selbst nicht ermitteln kann, sie zur Durchführung ihrer Aufgaben Urkunden oder sonstige Beweismittel benötigt, die sich im Besitz der ersuchten Behörde befinden, sie die Amtshandlung nur mit wesentlich größerem Aufwand vornehmen könnte als die ersuchte Behörde.
Weiterhin ist gemäß dem Thüringer Datenschutzgesetz die Unterstützung durch die öffentlichen Stellen verpflichtend.

6.58 Ich glaub, ich steh im Wald

Ein Bürger wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), da er beabsichtige, eine Wildkamera zum Filmen und Fotografieren von Tieren auf dem eigenen Grundstück zu installieren. Abhängig davon, an welcher Stelle er die Kamera anbringe, sei es möglich, dass auch eine Teilfläche des Nachbargrundstücks miterfasst werde. Außerdem

fragte er sich, ob der Sachverhalt anders zu beurteilen sei, wenn er sicherstelle, dass ausschließlich das eigene Grundstück betroffen ist. Er sei sich über die geltende Rechtslage unsicher.
Der TLfDI ist auch für die Einhaltung der datenschutzrechtlichen Gesichtspunkte bei der Videoüberwachung zuständig, weswegen er sich der Fragen annahm.
Bei einer Videoüberwachung handelt es sich immer um einen Umgang mit personenbezogenen Daten. Diese ist nur zulässig, soweit das Bundesdatenschutzgesetz (BDSG) oder eine andere Rechtsvorschrift dies erlaubt, anordnet oder die Betroffenen eingewilligt haben, § 4 Abs. 1 BDSG. Das Erheben, Verarbeiten oder Nutzen der mit einer Wildkamera erstellten Aufnahmen stellen automatisierte Verarbeitungen dar, sofern hiervon personenbezogene Daten betroffen sind.
Die Zulässigkeit des Einsatzes von Wildkameras durch nichtöffentliche Stellen, worunter Privatpersonen (z. B. Jäger) fallen, beurteilt sich grundsätzlich nach § 6b BDSG, wenn öffentlich zugänglicher Raum erfasst wird.
Der vorgeschilderte Sachverhalt ist den Fällen ähnlich, in denen Wildkameras im „klassischen“ Wald aufgestellt werden, mit dem Unterschied, dass hier der Fokus auf der Beobachtung des eigenen Grundstückes liegt.
Bei der Beurteilung der Zulässigkeit von Videokameras, die auf Grundstücken angebracht sind, ist nach dem Erfassungsbereich der Kamera zu unterscheiden. Es bedarf einer Rechtsvorschrift, die eine solche Videoüberwachung erlaubt, es sei denn es handelt sich bei den Aufnahmen um ausschließlich private oder familiäre Tätigkeiten, dann ist das BDSG nicht anwendbar, vgl. § 1 Abs. 2 Nr. 3 BDSG (Urteil des Europäischen Gerichtshofs vom 11. Dezember 2014 mit dem Aktenzeichen C-212/13). Entscheidend ist hierbei, ob auch Personen von der Videokamera erfasst werden können, die in keiner persönlichen oder familiären Verbindung zum Videobetreiber stehen. Der Anwendungsbereich der vorgenannten Entscheidung ist eng auszulegen. Daher kann eine Videoüberwachung, die sich auf den öffentlichen Raum erstreckt und dadurch auf einen Bereich außerhalb der privaten Sphäre desjenigen gerichtet ist, der die Daten verarbeitet, nicht als eine „ausschließlich persönliche oder familiäre Tätigkeit“ angesehen werden.

Die Überwachung des allein genutzten Grundstücks jedoch ist regelmäßig zulässig. Die sich daraus ergebende Beobachtungsbefugnis endet allerdings an der Grundstücksgrenze.
In der ersten Fallgestaltung, in der der Fragensteller nicht ausschließen konnte, dass neben seinem Grundstück auch das Nachbargrundstück von der Beobachtung betroffen werde, kommt eine ausschließlich private oder familiäre Tätigkeit nach der vorgenannten Rechtsprechung nicht in Betracht.
Nach § 6b Abs. 1 BDSG kann eine Videoüberwachung zulässig sein, soweit sie der Wahrnehmung des Hausrechts oder der Wahrnehmung berechtigter Interessen dient.
Nach § 6b Abs. 1 Nr. 2 BDSG ist das Beobachten öffentlich zugänglicher Räume per Videoüberwachung zur Wahrnehmung des Hausrechts unter Berücksichtigung der Erforderlichkeit und der Interessenabwägung zulässig, sofern sie nur an die Grenzen des Grundstücks bzw. je nach Einzelfall maximal einen Meter darüber hinaus erfolgt. Diese Grenze ist bei der ersten Fallgestaltung überschritten.
Die vom Anfragenden betriebene Videoüberwachung ist daher im Falle der Mitüberwachung des Nachbargrundstücks von § 6b Abs. 1 Nr. 2 BDSG nicht gedeckt.
Deshalb kommt in diesem Falle eine Zulässigkeit nach § 6b Abs. 1 Nr. 3 BDSG in Betracht. Danach ist eine Videoüberwachung öffentlich zugänglicher Räume zulässig, soweit sie zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Ein berechtigtes Interesse für den Betrieb kann ideeller, wirtschaftlicher oder rechtlicher Natur sein. Daneben muss die Videoüberwachung auch erforderlich sein, um diesen Zweck zu erreichen. Die Erforderlichkeit einer Videoüberwachung kann nur dann bejaht werden, wenn der beabsichtigte Zweck nicht genauso gut mit einem anderen zumutbaren, in die Rechte des Betroffenen weniger eingreifenden Mittel erreicht werden kann. Deswegen muss man sich mit zumutbaren Alternativen auseinandersetzen, die in das informationelle Selbstbestimmungsrecht des Einzelnen weniger eingreifen. Eine reine Aufzeichnung ist für präventive Zwecke nicht geeignet, da keine direkte Interventionsmöglichkeit besteht. Diese ist nur bei einem Live-Monitoring gegeben, da der Betreiber dort unmittelbar eingreifen kann.
Soweit eine Erforderlichkeit für die Videoüberwachung zur Wahrung eines berechtigten Interesses vorliegt, darf sie nur in Betrieb

genommen werden, wenn keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. An dieser Stelle ist eine Abwägung zwischen den berechtigten Interessen des Betreibers und den von der Überwachung Betroffenen vorzunehmen. Die permanente Überwachung stellt einen gravierenden Eingriff dar und führt häufig dazu, dass deutliche Anhaltspunkte dafür vorliegen, dass schutzwürdige Interessen der betroffenen Personen gegenüber den berechtigten Interessen des Betreibers überwiegen.
Sowohl die erste als auch die zweite Sachverhaltsschilderung sind zu wenig konkret, um eine abschließende Beurteilung zu ermöglichen. Um belastbare Aussagen über die Zulässigkeit der Kameras treffen zu können, wären weitere Angaben notwendig gewesen, die aufgrund der Abstraktheit der Anfrage nicht vorgelegen haben.

Sofern sich die Videoüberwachung ausschließlich auf das eigene Grundstück bezieht und nur Bereiche erfasst, die nicht zum Betreten durch Dritte vorgesehen sind, ist eine Videoüberwachung aus datenschutzrechtlicher Sicht regelmäßig zulässig, da dort das BDSG überhaupt keine Anwendung findet.

6.59 Problemzonen im Autohaus – Fortsetzung

Bereits im 1. Tätigkeitsbericht im nicht-öffentlichen Bereich wurde unter Punkt 3.17 ausführlich über eine datenschutzrechtliche Kontrolle eines Autohauses berichtet; ein Ergebnis dazu gab es leider in dem Berichtszeitraum 2012/2013 nicht.
Zum Hintergrund: Gegenstand einer datenschutzrechtlichen Kontrolle des TLfDI war ein Autohaus. Im Nachgang der Kontrolle gab es einige Punkte, die datenschutzrechtlich bewertet werden mussten. Unter anderem betrieb das Autohaus umfangreich eine Videoüberwachungsanlage im öffentlich zugänglichen Außenbereich des Autohauses. Da nach § 4 Abs. 1 BDSG das Erheben, Nutzen und Verarbeiten von personenbezogenen Daten nur zulässig ist, wenn es hierzu einen Norm gibt, die dies anordnet oder erlaubt oder der Betroffene eingewilligt hat, waren die Voraussetzungen des § 6b BDSG zu prüfen, der abschließend die Überwachung von öffentlich zugänglichen Räumen regelt. Nur wenn eine Videoüberwachung diesen Anforderungen entspricht, ist sie aus datenschutzrechtlicher Sicht zulässig.

Das Autohaus betrieb die Videoüberwachungsanlage, da es in der Vergangenheit bereits zu mehreren Diebstählen, Einbrüchen und Sachbeschädigungen gekommen war. Die Vorkommnisse wurden auch bei der Polizei gemeldet und konnten als Nachweis für ein berechtigtes Interesse der Videoüberwachung nach § 6bAbs. 1 Nr. 3 BDSG gewertet werden. Der TLfDI sah allerdings die Videoüberwachung nicht als erforderliches Mittel zur Vermeidung der Delikte an und verlangte vom Autohaus, dass ein milderes Mittel eingesetzt wird, mit dem die genannten Vorkommnisse (Diebstahl, Einbrüche, Sachbeschädigungen) vermieden werden können. Hierzu wäre der Einsatz von Monitoring möglich gewesen. Ein zuständiger Mitarbeiter könnte – bei einer oben dargestellten Situation – somit dann gleich eingreifen. Das Autohaus argumentierte, dass es nicht in der Lage sei, sein Personal mit der zusätzlichen Aufgabe des Monitorings zu beschäftigen. Zu umfangreich seien die Bereiche, die auf dem Gelände des Autohauses videoüberwacht werden. Hinzu komme der Kostenfaktor für die Variante. Außerdem sei es auch ein berechtigtes Interesse, Schadensersatzforderungen im Nachhinein durchsetzen zu können.
Im Ergebnis sah der TLfDI deswegen die Videoüberwachungsanlage unter den dargestellten Gründen als zulässig an, legte dem Autohaus allerdings nahe, über den Einsatz von Monitoring nachzudenken und Sicherheitspersonal für die Überwachung des Monitoring zu beauftragen. Das Sicherheitspersonal könnte sofort eingreifen, wenn etwas passiert. So würden Beschädigungen verhindert.

Jede datenschutzrechtliche Würdigung ist eine Einzelfallentscheidung. In diesem Fall ist man nach zwei Tätigkeitsberichtszeiträumen zu einem Ergebnis gekommen. Im Fokus der datenschutzrechtlichen Prüfung war der § 6b BDSG, von dem eine Voraussetzung nach § 6bAbs. 1 Nr. 1 bis 3 BDSG hätte erfüllt sein müssen, damit die Videoüberwachung im öffentlich zugänglichen Bereich zulässig ist. Sollte von Unternehmen Videoüberwachungsanlagen installiert werden, ist dringend erforderlich, dass die gesetzlichen Grenzen der Zulässigkeit solcher Maßnahmen geprüft und nicht überschritten werden. Bei allgemeinen Anfragen verweist der TLfDI immer auf die „Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen“ des Düsseldorfer Kreises, in der die Grundsätze zulässiger Videoüberwachung aufgeführt sind. Diese Orientierungshilfe stellt der TLfDI auf seiner Website

(https://www.tlfdi.de/mam/tlfdi/datenschutz/video/oh-v -durch-nicht- ffentliche-stellen.pdf) zur Verfügung.



6.60 Ob der Lkw richtig steht, sieht man, wenn die Kamera angeht – Videogaga 23

Bei einer datenschutzrechtlichen Kontrolle wurde eine durch eine Firma betriebene Videoüberwachung seitens des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) überprüft. Auf dem Firmengelände konnten zwei Videokameras festgestellt werden. Beide Kameras waren auf die Lkw-Waage gerichtet und dienten der Kontrolle, ob der Lkw richtig auf der Waage platziert war. Der Monitor war im Waagenraum angebracht. Die Kameras zeichneten nicht auf und waren nur zu den Geschäftszeiten eingeschaltet. Sie waren nicht schwenk- und zoomfähig. Es gab jedoch kein Hinweisschild, welches auf die Videoüberwachung in diesem Bereich hingewiesen hat.
Die Zulässigkeit der betreffenden Videoüberwachung richtete sich in diesem Fall nach § 6b Abs. 1 Bundesdatenschutzgesetz (BDSG). Danach ist das Beobachten öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) nur zulässig, soweit es zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Ein berechtigtes Interesse für den Betrieb einer Videoüberwachungsanlage kann ideeller, wirtschaftlicher oder rechtlicher Natur sein. Der von der verantwortlichen Stelle vorgetragene Zweck, zu kontrollieren, ob der Lkw richtig auf der Waage platziert wurde, war als konkret festgelegter Zweck im Rahmen des berechtigten Interesses zu berücksichtigen. Hinsichtlich der Erforderlichkeit der Videoüberwachung ergaben sich ebenfalls keine Bedenken. Darüber hinaus gab es keine Anhaltspunkte, dass schutzwürdige Interessen Betroffener, in diesem Fall die be-

rechtigten Interessen der Firma, überwiegen. Zu bemängeln war jedoch, dass nicht auf die Videoüberwachung im Bereich der Lkw-Waage hingewiesen wurde. Nach § 6b Abs. 2 BDSG sind der Umstand der Beobachtung und die verantwortliche Stelle durch geeignete Maßnahmen erkennbar zu machen. Der Hinweis kann mithilfe entsprechender Schilder oder grafischer Symbole (z. B. Piktogramm nach DIN 33450) erfolgen. Er ist so (etwa in Augenhöhe) anzubringen, dass der Betroffene vor dem Betreten des überwachten Bereichs den Umstand der Beobachtung erkennen kann. Der Betroffene muss einschätzen können, welcher Bereich von einer Kamera erfasst wird, damit er in die Lage versetzt wird, gegebenenfalls der Überwachung auszuweichen oder sein Verhalten anzupassen. Außerdem muss die für die Datenverarbeitung verantwortliche Stelle erkennbar sein, das heißt, wer genau die Videodaten erhebt, verarbeitet oder nutzt. Entscheidend ist dabei, dass für den Betroffenen problemlos feststellbar ist, an wen er sich bezüglich der Wahrung seiner Rechte ggf. wenden kann. Daher ist die verantwortliche Stelle grds. mit ihren Kontaktdaten explizit auf dem Hinweisschild zu nennen. Der Mangel wurde seitens der verantwortlichen Stelle umgehend behoben und ein den Vorgaben des § 6b Abs. 2 BDSG entsprechendes Hinweisschild im Bereich der Videoüberwachung wurde angebracht. Die Videoüberwachung wird nach Einschreiten des TLfDI nunmehr datenschutzkonform betrieben.

Die gebotene Hinweispflicht gem. § 6b Abs. 2 BDSG im Rahmen der Videoüberwachung in öffentlich zugänglichen Bereichen dient insbesondere dazu, den Betroffenen die Möglichkeit zu geben, dass diese selbst entscheiden können, der Überwachung auszuweichen oder ihr Verhalten entsprechend anpassen zu können. Deswegen ist es wichtig, dass die verantwortlichen Stellen diese Hinweispflicht ernst nehmen und auch erfüllen. Der Hinweis kann mithilfe entsprechender Schilder oder grafischer Symbole (z. B. Piktogramm nach DIN 33450) erfolgen. Er ist etwa in Augenhöhe anzubringen. Die für die Datenverarbeitung verantwortliche Stelle muss erkennbar sein, das heißt, wer genau die Videodaten erhebt, verarbeitet oder nutzt. Entscheidend ist dabei, dass für den Betroffenen problemlos feststellbar ist, an wen er sich bezüglich der Wahrung seiner Rechte ggf. wenden kann. Daher ist die verantwortliche Stelle grds. mit ihren Kontaktdaten explizit auf dem Hinweisschild zu nennen.

Achtung: Bisher führte ein fehlender Hinweis weder zu einem Bußgeld, noch zu einer Rechtswidrigkeit der Videoüberwachung selbst. Dies wird sich mit Geltung der Datenschutz-Grundverordnung (DS-GVO) ab Ende Mai 2018 ändern. Verstöße gegen die dort genannten Informationspflichten können zu empfindlichen Geldbußen (bis zu 20 Mio. Euro) führen. Im Rahmen der Bestimmung der Höhe dieser Geldbußen sind jedoch z. B. Art, Schwere und Dauer des Verstoßes sowie weitere in Art. 83 Abs. 1 DS-GVO aufgeführte Vorgaben zu berücksichtigen. Darüber hinaus führt ein Mangel bei diesen Informationspflichten zur Rechtswidrigkeit der Videoüberwachung.

6.61 Streetview outsourced – davon wird's nicht besser; Videogaga 24

Ein Bürger wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und wollte wissen, ob er „Probleme" bekommen würde, wenn er Fotos vom öffentlichen Straßenverkehr ins Internet hochladen würde. Die Kamera würde in sehr kurzen Zeitintervallen auslösen. Er gibt an, dass die von ihm bevorzugte Seite zwar Personen und Autokennzeichen verpixeln würde, es aber wohl bei Automatismen dieser Art üblich sei, dass dies nur selten zu 100 Prozent passiert. Dies würde bedeuten, dass ein Gesicht oder Autokennzeichen eventuell sichtbar bzw. leserlich sein könnte. Weiterhin erklärte er, dass die Fotos zum Zwecke der geografischen sowie straßenverkehrstechnischen Datenermittlung genutzt werden würden, um eben das Programm als freie und offene Geodatenbank verbessern zu können.
Der TLfDI teilte dem Bürger daraufhin mit, dass er tatsächlich „Probleme" bekommen könnte, wenn er solche Fotos hochladen würde, nämlich dann, wenn er dabei erwischt wird und der TLfDI davon Kenntnis bekäme. Eine bezweckte Dauerbeobachtung öffentlich zugänglicher Räume ist mit dem Bundesdatenschutzgesetz (BDSG) nicht vereinbar. Die Beobachtung, worunter auch die digitale Fotografie, sofern eine gewisse zeitliche Dauer zugrunde liegt, von öffentlich zugänglichen Räumen fällt, wozu der öffentliche Straßenverkehr gehört, hat der Gesetzgeber in § 6b BDSG abschließend geregelt. Danach ist eine Beobachtung von öffentlich zugänglichen Räumen nur dann zulässig, wenn dies zur Aufgabenerfüllung durch öffentliche Stellen, zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwe-

cke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Bei der Videoüberwachung von öffentlich zugänglichen großflächigen Anlagen, wie insbesondere Sport-, Versammlungs- und Vergnügungsstätten, Einkaufszentren oder Parkplätzen, Fahrzeugen und öffentlich zugänglichen großflächigen Einrichtungen des öffentlichen Schienen-, Schiffs- und Busverkehrs gilt der Schutz von Leben, Gesundheit oder Freiheit von sich dort aufhaltenden Personen als ein besonders wichtiges Interesse. Nur unter diesen genannten Voraussetzungen sind solche Videoüberwachungen zulässig. Diese waren in dem vorgenannten Fall nicht gegeben. Wird eine solche Datenerhebung durchgeführt, ohne dass die Voraussetzungen von § 6b BDSG vorliegen, erfüllt dies den Ordnungswidrigkeitentatbestand des § 43 Abs. 2 Nr. 1 BDSG. Dieser kann mit einem Bußgeld geahndet werden.

Eine bezweckte Dauerbeobachtung öffentlich zugänglicher Räume ist mit dem Bundesdatenschutzgesetz (BDSG) nicht vereinbar. Eine Beobachtung durch Dritte von öffentlich zugänglichen Räumen, wozu auch der Straßenverkehr gehört, hat der Gesetzgeber in § 6b BDSG abschließend geregelt.

6.62 Die (Un)zulässigkeit von Dashcams oder Die Leiden des (jungen) Hobbyfilmers

Die Zulässigkeit von sogenannten Dashboardcams bzw. Dashcams, dies sind in Fahrzeugen installierte Kameras, mit denen das Verkehrsgeschehen aufgenommen wird und die so gewonnenen Bilder gespeichert werden können, ist umstritten. Bei den auch als „Armaturenbrett-Kameras“ bezeichneten Aufnahmegeräten steht ein Aufklärungsinteresse, zumeist von Unfallbeteiligten, dem Persönlichkeitsrecht der anderen Verkehrsteilnehmer gegenüber. Während in verschiedenen Ländern deren Einsatz rechtlich zulässig oder verboten ist, ist in Deutschland die Rechtslage noch unklar. Während die Datenschützer deren Einsatz mehrheitlich als datenschutzwidrig ansehen, gibt es in Deutschland zu deren Zulässigkeit bzw. Unzulässigkeit noch keine gefestigte Rechtsprechung. Da sich der Einsatz solcher Kameras stetig größerer Beliebtheit erfreut, ist auch der Kreis der Urteile, die sich mit der Rechtmäßigkeit dieser Kameras befassen, deutlich gestiegen.

Die nach hiesiger Meinung bekanntesten Urteile, die sich mit diesem Thema beschäftigen sind:

- Amtsgericht München, Urteil vom 9. August 2017 Az. 1112 OWi Js 121012/17
- Amtsgericht München, Urteil vom 6. Juni 2013 Az. 343 C 4445/13
- Amtsgericht Nienburg, Urteil vom 20. Januar 2015, Az. 4 Ds 520 Js 39473/14
- Landgericht Landshut, Hinweisbeschluss vom 1. Dezember 2015, Az.12 S 2603/15
- Oberlandesgericht Stuttgart, Beschluss vom 4. Mai 2016, Az. 4 SS 543/15
- LG München I, Beschluss vom 14. Oktober 2016, Az.: 17 S 6473/16
- Verwaltungsgericht Ansbach, Urteil vom 12. August 014, Az. AN 4 K 13.01634
- Amtsgericht München, Hinweisbeschluss vom 13. August 2014, Az. 345 C 5551/14
- Landgericht Heilbronn Urteil vom 17. Februar 2015 Az. I 3 S 19/14
- Landgericht Memmingen Urteil vom 14. Januar 2016 Az. 22 O 1983/13.
- Verwaltungsgericht Göttingen Urteil vom 31. Mai 2017 Az.1 A 170/16

Während sich die ersten fünf Entscheidungen für die (partielle) Zulässigkeit von Dashcams im Sinne einer gerichtlichen Verwertbarkeit aussprechen, negieren die übrigen Entscheidungen deren grundsätzliche Zulässigkeit. Mit dem Volkzählungsurteil des Bundesverfassungsgerichts vom 15. Dezember 1983, in dem Datenschutz, dem sog. Recht auf informationelle Selbstbestimmung, Verfassungsrang zuerkannt wurde, hat sich das bis dahin geltende Datenschutzrecht grundlegend geändert. Als Bundesgesetz ist das Bundesdatenschutzgesetz allseits, d. h. auch im Zivilrecht, im Strafrecht und im Ordnungswidrigkeitsrecht, zu beachten.

Die zitierten Entscheidungen, die den Einsatz partiell als legitim ansehen, begründen dies teilweise auch damit, dass der Gesetzgeber lediglich die fest installierten Kameras in den Geltungsbereich von § 6b Bundesdatenschutzgesetz (BGSG) einbezogen habe.

Diese Entscheidungen, die die Rechtmäßigkeit der Videoüberwachung mittels Dashcams befürworten, sehen dies unter dem Blickwinkel der Beweisverwertung gegebenenfalls auch rechtswidrig erlangter Beweise im Zivil-/Strafprozess bzw. Ordnungswidrigkeitsverfahren.
Besonders das Urteil des Amtsgerichtes München, Urteil vom 6. Juni 2013 (Az. 343 C 4445/13) wurde als Anerkennung für den Einsatz von Dashcams gewertet, weil dort erstmals ein deutsches Zivilgericht die Frage der Verwertung der mithilfe einer Dashcam gefertigten Aufnahmen positiv entschieden hat. Die Frage der Zulässigkeit bei der Verwertung derartiger Aufnahmen bestimme sich nach Interessen beider Parteien, die gegeneinander abzuwägen wären. Im dort entschiedenen Fall war ein Autofahrer in einen Verkehrsunfall verwickelt. Zum Zeitpunkt der Aufnahme sei noch keine Zweckbestimmung erfolgt. Die Personen, die auf Video aufgenommen worden waren, seien rein zufällig ins Bild geraten. Eine Beeinträchtigung von Grundrechten läge nur dann vor, wenn eine derartige, zufällig gewonnene Aufnahme im Nachgang gegen den Willen der abgebildeten Person veröffentlicht werde. Wegen der (nachträglichen) Beweiserheblichkeit könnten solche Aufnahmen im anschließenden Prozess durchaus Verwendung finden.
Nach dem Urteil des Amtsgerichtes Nienburg sei die Vorschrift § 6b BDSG nicht anwendbar, da diese Norm nur für den ortsfesten Betrieb einer Kamera gelte. Dieser Schluss ergebe sich bereits aus der Hinweispflicht nach § 6b Abs. 2 dieser Vorschrift. Beim Betrieb einer beweglichen Kamera sei es schlicht unmöglich, die betroffenen Personen auf bevorstehende Aufzeichnungen hinzuweisen. Dies wiederum sei Voraussetzung für die Anwendung dieser Vorschrift. Im konkreten Falle sei die hier erfüllte spezialgesetzliche Ermächtigung, die dem Zeugen das Videoaufzeichnen ermögliche, die entsprechende Anwendung des § 28 Abs. 1 Nummer 1 BDSG. Bei der Kommentierung dieses Urteils wird oftmals übersehen, dass das erkennende Gericht die Verwertbarkeit als Beweis im Strafverfahren nur in sehr engen Grenzen gebilligt hat. Der Zeuge, der das Unfallgeschehen dort aufgenommen hat, hatte die Kamera nicht dauernd im Einsatz sondern nur als Beweismittel in der konkreten strafrechtlich relevanten Situation. In dieser kurzen, anlassbezogenen Aufnahme waren zudem auch keine Personen, sondern nur das Auto des Täters zu sehen.

Nach Ansicht des Landgerichts Landshut seien Videoaufnahmen mit Dashcams grundsätzlich verwertbar. Das Anfertigen der Aufnahmen sei nicht verboten, weswegen auch kein Beweisverwertungsverbot bestehe. Das Kunsturhebergesetz (KUG), welches unter anderem das Recht am eigenen Bild schütze, sei nach Auffassung des Landgerichtes nicht einschlägig. Abgesehen davon, dass die von der Aufnahme Betroffene selbst nicht videografiert worden sei, verbiete § 22 KUG nur das Verbreiten und Präsentieren von Aufnahmen, nicht aber das Aufnehmen selbst. Auch das Bundesdatenschutzgesetz hielt das erkennende Gericht für unanwendbar. Diese Norm gelte lediglich für fest installierte Kameras. Zwar habe das Verwaltungsgericht Ansbach das anders gesehen, aber der Fall dort habe anders gelegen. In diesem oben angeführten Urteil des Verwaltungsgerichtes Ansbach habe der Kläger systematisch den Verkehrsraum überwacht, um dann Anzeigen wegen Ordnungswidrigkeiten zu erstatten.
Selbst ein Verstoß gegen das Bundesdatenschutzgesetz hätte aus Sicht des Gerichtes nicht zu einem Beweisverwertungsverbot geführt. Das laufende Filmen des Verkehrsgeschehens durch eine Onboard-Kamera stelle keinen gravierenden Grundrechtseingriff dar. Eventuell abgebildete Personen blieben anonym. Ohnehin müsse jeder Autofahrer zwingend damit rechnen, dass seine Fahrweise von anderen beobachtet werde. Zwar komme den Filmaufnahmen nach einem Unfall eine größere Bedeutsamkeit zu. Aber nach einem Unfall würden ständig die Fahrzeuge, die Unfallspuren und auch umstehende Beteiligte zwecks Beweissicherung fotografiert werden.
Die oben angeführte Entscheidung des Oberlandesgerichtes Stuttgart hat es, zumindest für den Bereich der Verfolgung schwerwiegender Ordnungswidrigkeitenverfahren, für zulässig erachtet, mit einer Dashcam aufzunehmen. Bei dieser Entscheidung hat das Gericht offen gelassen, ob bzw. unter welchen Voraussetzungen der Einsatz einer Dashcam durch einen anderen Verkehrsteilnehmer gegen § 6b BDSG verstoße. Jedenfalls enthalte § 6b Abs. 3 Satz 2 dieser Norm kein Beweisverwertungsverbot für das Straf- und Bußgeldverfahren. Ein für das Gericht möglicher Verstoß gegen das Datenschutzgesetz sei nicht zwingend ein Grund, die Aufnahmen nicht zu verwerten. Über deren Verwertbarkeit sei vielmehr im Einzelfall unter Abwägung der widerstreitenden Interessen zu entscheiden.
Auch das Landgericht München I sah in der oben aufgeführten Entscheidung eine Verwertung der Aufnahmen im Zivilprozess – unter umfassender Abwägung der Interessen des Abgebildeten an einer

selbstbestimmten Verwendung personenbezogener Datensätze einerseits und dem Beweissicherungsinteresse des Beweisführers andererseits – als möglich an, wenn diese Aufnahmen nur anlassbezogen erstellt würden und sichergestellt sei, dass diese Aufnahmen nach einer bestimmten Zeit gelöscht oder überschrieben würden.

Zu einem anderen Ergebnis kommt das Landgericht Heilbronn in seinem oben angesprochen Urteil. Aufzeichnungen einer in einem Pkw installierten Dashcam könnten im Zivilprozess wegen eines Beweismittelverbotes nicht als Beweismittel zum Hergang eines Unfalls verwertet werden. Eine solche großflächige Beobachtung von öffentlichen Straßen stelle schon deshalb einen schwerwiegenden Eingriff in die Persönlichkeitsrechte der Betroffenen dar, weil durch die hier vorgenommene, permanente Aufzeichnung mit der Videokamera eine Vielzahl von Personen in kurzer Zeit in ihrem allgemeinen Persönlichkeitsrecht betroffen wird.

Das Landgericht Memmingen hat in seinem Urteil das Anfertigen von Videoaufnahmen von Personen im öffentlichen Straßenraum als rechtswidrig angesehen, wenn dies durch eine an der Windschutzscheibe eines Pkw installierte betriebsbereite Dashcam geschähe. Dies gelte auch dann, wenn diese über einen Bewegungsmelder verfüge, soweit die Aufzeichnungen nicht ausnahmsweise erforderlich wären und das schutzwürdige Interesse des Verwenders der Kamera überwöge. Soweit die Befürworter der Zulässigkeit von Dashcams im Straßenverkehr ins Feld führten, die Vorschrift des § 6b BDSG sei nur auf stationäre Kameras anzuwenden, sei dem nicht zu folgen. Diese Auslegung sei dem Gesetzeswortlaut nicht zu entnehmen. Zudem werde die Beobachtung entgegen § 6b Abs. 2 BDSG auch nicht in geeigneter Weise deutlich gemacht. Ein kleines Warnschild im Pkw genüge insoweit nicht, da es nicht ins Auge steche und erst aus großer Nähe sichtbar sei.

Einen ganz besonderen Fall hatte das Verwaltungsgericht Göttingen zu entscheiden. Dort hatte ein Rentner seine Dashcam dazu benutzt, seine privaten „Ordnungsfantasien“ auszuleben. Der als „Knöllchen-Horst“ in die Geschichte eingegangene Ordnungshüter hatte mehr als 15.000 Verkehrsverstöße dokumentiert und bei den Verfolgungsbehörden angezeigt. Das Gericht kam zu dem Schluss, dass der Einsatz von Dashcams im öffentlichen Verkehrsraum sowohl die Persönlichkeitsrechte der Verkehrsteilnehmer wie auch den Datenschutz verletze. § 6b BGSG verbiete es, ohne dort genannte Gründe personenbezogene Aufnahmen zu fertigen. Ein Verstoß gegen diese Norm

läge schon deshalb vor, weil der Anzeigenerstatter den Umstand der Beobachtung nicht erkennbar gemacht habe. Die permanente Überwachung des Verkehrs sei darüber hinaus auch nicht gerechtfertigt gewesen, da er mit seinem Verhalten keine schützenswerten Eigeninteressen verfolgt habe, sondern Sachwalter öffentlicher Interessen sei.
In Polizeikreisen wird die Zulässigkeit von Dashcams durchaus befürwortet. Sie könnten zum Nachweis von Verkehrsstraftaten dienen, bei denen bisher als Beweismittel allenfalls Aussagen und Erinnerungen vorlägen. Die Gewerkschaft der Polizei plädiert deswegen für eine verbindliche Einführung eines sogenannten Unfalldatenspeichers.
Im Sinne der Rechtsklarheit ist es zwingend geboten, eine verbindliche Regelung zu schaffen, die die widerstreitenden Interessen der Beteiligten berücksichtigt. Es ist nicht von der Hand zu weisen, dass das Beweisinteresse der die Kameras nutzenden Verkehrsteilnehmer einerseits und ein Interesse der übrigen Verkehrsteilnehmer zur Wahrung der Persönlichkeitsrechte andererseits im Widerstreit stehen. Dieser Widerstreit muss schnellstens aus Gründen der Rechtssicherheit aller Beteiligter gelöst werden.

In Deutschland fehlt es bisher an einer verbindlichen Regelung dazu, ob und bejahendenfalls in welchem Maße Dashcams für den Straßenverkehr genutzt werden können.

6.63 Nicht alle Wege führen zum Friedhof

Ein Beschwerdeführer wandte sich wegen einer am Waldesrand installierten Kamera an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI).
Der Besitzer eines Waldstückes und der umliegenden Grundstücke verweigere anderen mittels dieser Kamera faktisch die Nutzung des sich auf diesem Areal befindlichen Weges zum Friedhof, weil diese sich – zutreffend – beobachtet fühlten. Dieser streitgegenständliche Weg sei in der Katasterkarte eingetragen und erfreue sich großer Beliebtheit. Wahrscheinlich, um seinen Wunsch nach dessen Nichtgebrauch zu überwachen und zu sehen, wer diesen Weg gleichwohl nutze, habe er eine Beobachtungskamera an einem dort befindlichen Baum in ca. 3,50 Meter Höhe installiert.

Der TLfDI hat daraufhin dem Besitzer des streitbefangenen Grundstückes ein Auskunftsverlangen nach § 38 Abs. 3 Bundesdatenschutzgesetz (BDSG) zugesandt und um die Beantwortung eines Fragenkataloges gebeten.
Darauf erwiderte der Beschwerdegegner, dass er auf dem vom TLfDI genannten Grundstück keine funktionstüchtige Videoüberwachungsanlage betreibe. Auch werde von ihm nicht der Eindruck erweckt, dort eine Videoüberwachungsanlage zu betreiben.
Das zuständige Landratsamt hat den TLfDI inzwischen darüber informiert, dass die streitbefangene Kamera zwischenzeitlich deinstalliert wurde.
Damit hat sich die Angelegenheit für den TLfDI erledigt.

Der Betreiber einer Videoüberwachungsanlage ist nach § 38 Abs. 3 BDSG verpflichtet, unverzüglich, vollständig und wahrheitsgemäß seiner Auskunftspflicht nachzukommen. Wenn der Auskunftspflichtige dieser Verpflichtung vorsätzlich oder fahrlässig nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig nachkommt, handelt er nach § 43 Abs. 1 Nummer 10 BDSG ordnungswidrig. Die Ordnungswidrigkeit kann nach § 43 Abs. 3 Satz 1 BDSG mit einer Geldbuße bis zu 50.000 € geahndet werden.

6.64 Rundumüberwachung durch den Nachbarbetrieb?

Im Berichtszeitraum erreichte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) eine Beschwerde über drei installierte Videokameras an einem Privat- und Firmengelände. Eine der Kameras erfasste wohl ausschließlich das Privatgrundstück. Die beiden anderen waren auf den öffentlichen Verkehrsraum ausgerichtet, womit auch teilweise das Haus der Beschwerdeführerin mit Zufahrtsweg sowie das Grundstück eines weiteren Nachbarn erfasst waren. Der TLfDI wandte sich mit einem Auskunftsersuchen an den Betreiber der Kameras. Dieser teilte mit, dass keine Aufzeichnung über die Videokamera erfolgte, sondern nur eine Beobachtung mittels Bildübertragung auf einen Monitor stattfand. Die Kameras dienten der Kontrolle der Zufahrt zum Grundstück (Wohnbereich und Betrieb) als auch der Überwachung des Betriebsgeländes, da dort Gefahrgut gelagert war.
Durch die „reine“ Beobachtung mit optisch-elektronischen Einrichtungen werden ebenfalls personenbezogene Daten erhoben. Nach § 4

Bundesdatenschutzgesetz (BDSG) ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit dieses Gesetz oder eine Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.
Vorliegend kamen hier entweder § 6b BDSG oder § 28 Abs. 1 Nr. 2 BDSG in Betracht, um die Zulässigkeit der Videobeobachtung zu beurteilen, abhängig davon, welche Bereiche erfasst wurden.
§ 28 Abs. 1 Nr. 2 BDSG gilt für nicht-öffentlich zugängliche Bereiche. Nicht-öffentlich zugänglich sind Räume, die nur von einem bestimmten und abschließend definierten Personenkreis betreten werden können oder dürfen. Entscheidend ist hierbei, dass die Nicht-Öffentlichkeit durch Verbotsschilder oder den Kontext der Umgebung erkennbar ist. Danach ist das Erheben von personenbezogenen Daten als Mittel zur Erfüllung eigener Geschäftszwecke zulässig, soweit es zur Wahrung berechtigter Interessen erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegen. Anhand der im Auskunftsverfahren erteilten Informationen und Bilder und der Aufnahmewinkel der Kameras war erkennbar, dass das gesamte Grundstück eingezäunt und ohne Einverständnis des Besitzers nicht betreten werden konnte. Kamera 1 war nur auf das eigene Grundstück ausgerichtet und diente der Wahrnehmung des Hausrechts des Betreibers mittels Kontrolle unbefugten Betretens des Grundstücks. Ein berechtigtes Interesse zum Betreiben der Kameras lag daher vor. Auch konnten die Erforderlichkeit bejaht und das Überwiegen schutzwürdiger Interessen ausgeschlossen werden. Somit wurde diese Kamera vom TLfDI als zulässig betrachtet.
Allerdings erfassten die beiden anderen Kameras auch weite Bereiche des öffentlichen Verkehrsraums sowie Grundstücksbereiche der umliegenden Nachbarn.
§ 6b BDSG regelt die Videoüberwachung von öffentlich zugänglichen Räumen. Hierbei handelt es sich um Bereiche innerhalb oder außerhalb von Gebäuden, die nach dem erkennbaren Willen des Berechtigten (z. B. des Grundstückseigentümers) von jedermann genutzt oder betreten werden dürfen. Ebenso handelt es sich um eine Überwachung von öffentlich zugänglichen Räumen, wenn außer einem privaten Grundstück auch der öffentliche Verkehrsraum in der Umgebung und die dort befindlichen Personen erfasst werden.
Gem. § 6b Abs. 1 Nr. 2 bis 3 BDSG ist die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Vi-

deoüberwachung) durch nicht-öffentliche Stellen nur zulässig, soweit sie entweder zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Die Kameras dienten wie bei Kamera 1 der Kontrolle des Zutritts zum Grundstück, also zur Wahrnehmung des eigenen Hausrechts. Allerdings muss die Videobeobachtung auch für den festgelegten Zweck geeignet und erforderlich sein. Bewertet wird hier auch, wie die Videotechnik eingesetzt wird (insbesondere der räumliche Umfang). Beide Kameras beobachteten einen umfangreichen Bereich außerhalb des Grundstückes. Das ist für den festgelegten Zweck, Wahrnehmung des Hausrechts, nicht erforderlich. Darüber hinaus bestanden Anhaltspunkte, dass schutzwürdige Interessen der Betroffenen überwiegen. Durch die eingestellten Kamerawinkel werden unter Umständen eine Vielzahl von Fußgängern und auch Nachbarn beobachtet. Dies bedeutet einen erheblichen Eingriff in deren informationelles Selbstbestimmungsrecht. Bei einer Abwägung der Interessen des Überwachenden und der Beobachteten musste der Zweck der Wahrnehmung des Hausrechts insoweit zurückstehen.

Die Kameras müssen im Rahmen der Erforderlichkeit so positioniert sein, dass lediglich ein Bereich bis einen Meter hinter der Grundstücksgrenze aufgenommen wird. Selbst dies ist nur dann zulässig, wenn ausreichender Platz zum Ausweichen verbleibt. Zur Wahrnehmung des Hausrechts darf der öffentliche Verkehrsraum grundsätzlich nicht mit Videokameras überwacht werden.

Der Betreiber der Kameras folgte den Anweisungen des TLfDI. Er beschränkte den Aufnahmebereich einer Kamera mit einem Sichtschutz, sodass der öffentliche Verkehrsraum und das Nachbarhaus nicht mehr erfasst wurden. Die andere Kamera deinstallierte der Betreiber, da er eine Beobachtung dieses Bereichs auch durch ein Fenster vornehmen konnte. Die verbleibenden Kameras werden durch Einschreiten des TLfDI datenschutzkonform betrieben.

Auch mit einer reinen Videobeobachtung, also keiner Speicherung der Daten, werden personenbezogene Daten erhoben. Demnach benötigt eine solche Anlage gem. § 4 BDSG eine Berechtigung zum Betreiben dieser Kameras. Die Zulässigkeitsprüfung wird dann anhand von § 28 BDSG für nicht-öffentliche Bereiche oder § 6b BDSG für öffentlich zugängliche Bereiche vorgenommen.

6.65 Wertvoller Schrott im Fokus – Fortsetzung

Bereits im 1. Tätigkeitsbericht zum Datenschutz im nicht-öffentlichen Bereich wurde über eine Kontrolle eines Recycling-Unternehmens in Thüringen berichtet (Beitrag 3.12 im 1. Tätigkeitsbericht nicht-öffentlicher Bereich). Schwerpunkt der Kontrolle war, dass dieses Unternehmen eine Videoüberwachungsanlage an jeweils vier Standorten im Unternehmen betreibt. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) hat bereits ausführlich die gesetzliche datenschutzrechtliche Sicht dargelegt, insbesondere, dass die Einhaltung des § 6b Bundesdatenschutzgesetz (BDSG) beim Einsatz von Videoüberwachungsanlagen in öffentlich zugänglichen Bereichen maßgeblich ist. Ein endgültiges Ergebnis konnte im genannten Berichtszeitraum nicht mitgeteilt werden, da das Verwaltungsverfahren beim TLfDI noch nicht abgeschlossen war.
Für Unternehmen, die Videoüberwachungsanlagen betreiben wollen, sind die Voraussetzungen nach § 6b Abs. 1 Nr. 2 bis 3 BDSG maßgebend. Nach § 6b Abs. 1 Nr. 2 BDSG ist eine Videoüberwachung zulässig, wenn sie zur Wahrnehmung des Hausrechts erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Gleiches gilt für § 6bAbs. 1 Nr. 3 BDSG. Hiernach ist eine Videoüberwachung nur zulässig, wenn sie zur Wahrung eines berechtigten Interesses für einen konkreten Zweck erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.
Der TLfDI hielt drei der vier Kameras für datenschutzrechtlich zulässig. Die vierte Kamera war allerdings so ausgerichtet, dass im Kassenbereich nicht nur personengezogene Daten von Kunden erhoben wurden, sondern auch die sich an der Kamera aufhaltenden Mitarbeiter (u. a. der Kassierer) sowie zwei Arbeitsplätze gesehen werden konnten. Wie bereits im zweiten Absatz erwähnt, ist eine Videoüberwachung nach § 6b BDSG nur zulässig, wenn das berechtigte Interesse für konkret festgelegte Zwecke erforderlich ist und das schutzwürdige Interesse des Betroffenen nicht überwiegt. Die Videoüberwachung wurde vom Betroffenen als verantwortliche Stelle zu Sicherheitszwecken und zur Abschreckung eingesetzt. Dies kann grundsätzlich ein berechtigtes Interesse für einen konkret festgelegten Zweck darstellen. Zulässig wäre die Videoüberwachung aber nur

dann, wenn sie dafür auch erforderlich wäre und keine Anhaltspunkte dafür bestehen, dass die schutzwürdigen Interessen der Betroffenen überwiegen. Zunächst entfaltet eine reine Videoüberwachung mittels aufzeichnender Kamera keine präventive Wirkung. Zwar können möglicherweise Vorkommnisse aufgeklärt werden, jedoch handelt es sich dabei um eine repressive Wirkung. Die wirksame Verhinderung z. B. von Diebstählen kann damit nicht bewerkstelligt werden. Die Art der Videoüberwachung ist daher nicht erforderlich. Demgegenüber steht das schutzwürdige Interesse der Kunden und der Mitarbeiter. Der Kunde hält sich im Kassenbereich auf, um seine Rechnung zu bezahlen. Er ist zudem gezwungen, diesen Bereich auch zu betreten. Auch der Kassierer läuft aus dienstlichen Gründen an der Kamera vorbei. Die Videoüberwachung im Kassenbereich stellt einen erheblichen Eingriff in die Privatsphäre des Kunden und der Mitarbeiter dar. Daraufhin forderte der TLfDI den Betreiber auf, dass die Videoüberwachungsanlage im Kassenbereich nur während der Schließzeiten aufzeichnet und dass während der Geschäftszeiten nur Live-Monitoring mit Verpixelung der Arbeitsplätze erfolgt. Das Unternehmen ist den Forderungen des TLfDI nachgekommen, indem es die Kamera im Kassenbereich außer Betrieb genommen hat.

Sollten von Unternehmen Videoüberwachungsanlagen installiert werden, ist dringend erforderlich, dass die gesetzlichen Grenzen der Zulässigkeit solcher Maßnahmen geprüft und nicht überschritten werden. Gern steht der TLfDI in solchen Fragen beratend zur Seite. Zur Rechtsgrundlage des § 6b BDSG gibt es auch eine „Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen“, die auf der Internetseite des TLfDI zur Verfügung steht: (https://www.tlfdi.de/mam/tlfdi/datenschutz/video/oh-v__-durch-nicht-__ffentliche-stellen.pdf).

6.66 Videoüberwachung als Auszugsgrund?

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) ist durch die Beschwerdeführerin darauf aufmerksam gemacht worden, dass der Beschwerdegegner in einem Bürofenster eines Grundstückes eine Kamera installiert habe. Diese Kamera observiere sowohl den Eingangsbereich des dort vom Beschwerdegegner unterhaltenen Büros wie auch die im selben Objekt befindliche Wohnung der Beschwerdeführerin.
Auf Nachfrage des TLfDI äußerte der Beschwerdegegner, im streitbefangenen Objekt tatsächlich eine Kamera positioniert zu haben. Er habe sie installiert, weil in der Gegend vermehrt eingebrochen worden sei. Die Kamera sei lediglich auf sein Grundstück, den Büroeingang, Teile des Innenhofes und die Garagenzufahrt gerichtet. Die Kamera sei nicht funktionstüchtig, da eine Speicherkarte derzeit noch nicht eingesetzt sei. Zukünftig aber sei eine Inbetriebnahme der Anlage angestrebt.
Nach weiterem Schriftverkehr stellte sich heraus, dass die streitgegenständliche Kamera lediglich auf sein – komplett von einer Mauer umgebenes – Grundstück ausgerichtet war. Dieses konnte zudem nach seinen Angaben nur nach manueller Betätigung des Eingangstores betreten werden. Eine gewerbliche Nutzung des Objektes sei zwischenzeitlich aufgegeben worden.
Die Videoüberwachung in solchen Bereichen ist nur im Rahmen einer Erforderlichkeit des abschließenden Zweckkatalogs des § 6b Abs. 1 Nr. 1 bis 3 Bundesdatenschutzgesetz (BDSG) zulässig. Danach ist die Videoüberwachung nur statthaft, soweit sie zur Aufgabenerfüllung öffentlicher Stellen, zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und außerdem keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.
Im vorliegenden Fall war – zumindest bei Einreichen der Beschwerde – die Beobachtungsbefugnis zur Wahrnehmung des Hausrechts nach § 6b Abs. 1 Nr. 2 BDSG einschlägig.
Als berechtigtes Interesse hatte der Beschwerdegegner vorgetragen, die Überwachung seines Grundstücks sei notwendig, da es in der Umgebung zu Einbrüchen gekommen sei. Hierin ist die Wahrnehmung des eigenen Hausrechts zu sehen, welches die Befugnis beinhaltet, darüber zu entscheiden, wer bestimmte Gebäude oder befriedetes Besitztum betreten und darin verweilen darf. Der Inhaber des

Hausrechts ist daher berechtigt, die zum Schutz des Objekts und der sich darin aufhaltenden Personen sowie die zur Abwehr unbefugten Betretens erforderlichen Maßnahmen zu ergreifen. Eine Beobachtung zur Wahrnehmung des Hausrechts dient sowohl einem präventiven als auch einem repressiven Zweck, indem zum einen Straftaten durch Abschreckung verhindert und zum anderen die Strafverfolgung durch die Beweissicherung ermöglicht werden soll. Auf den vom Beschwerdegegner übersandten Fotos ist zu erkennen, dass lediglich sein eigener Grundstücksbereich überwacht wird, sodass der räumliche Umfang der Überwachung für den Zweck der Wahrnehmung des Hausrechts nicht zu beanstanden ist.
Wenn bei der Videoüberwachung Anhaltspunkte bestehen, dass schutzwürdige Interessen von betroffenen Personen überwiegen, ist sie als unzulässig einzustufen. Dies könnte vorliegend der Fall sein, wenn – nicht mit dem Betreiber der Anlage in persönlicher oder familiärer Tätigkeit verbundene Dritte – das Grundstück nutzen, da deren schutzwürdige Interessen das berechtigte Interesse an der Wahrnehmung des Hausrechts häufig verdrängen.
Da die Beschwerdeführerin zum Zeitpunkt ihrer Beschwerde ebenfalls in dem Streitobjekt gewohnt hatte, sah sie sich in ihrem Persönlichkeitsrecht verletzt. Ob im vorliegenden Fall das Hausrecht zur Statthaftigkeit der Anlage geführt hätte, war nicht mehr zu entscheiden, nachdem die Beschwerdeführerin ihrerseits ausgezogen war. Daher bestanden keine Anhaltspunkte mehr dafür, dass schutzwürdige Interessen anderer von der Kamera verletzt würden.

Wenn bei der Videoüberwachung Anhaltspunkte bestehen, dass die schutzwürdigen Interessen von betroffenen Personen überwiegen, ist sie als unzulässig einzustufen. Dies ist beispielsweise der Fall, wenn auch nicht mit dem Betreiber der Anlage in persönlicher oder familiärer Tätigkeit verbundene Dritte ein Grundstück nutzen, da deren schutzwürdigen Interessen die berechtigten Interessen des Hausrechtsinhabers an der Wahrnehmung dieses Hausrechtes häufig verdrängen.

6.67 Videoüberwachungskamera auf der anderen Straßenseite

Das Ordnungsamt einer Stadtverwaltung meldete dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) eine Videoüberwachungsanlage an einem gemischt genutz-

ten Gebäude. Eine Videokamera war im 2. Stock des Hauses angebracht, sodass nicht ausgeschlossen werden konnte, dass die öffentliche Straße und Gehwege sowie die gegenüberliegenden Grundstücke vom Kamerabereich miterfasst wurden.
Der Hausbesitzer und gleichzeitige Geschäftsführer der dort ansässigen Firma wurde vom TLfDI angeschrieben und um Auskunft gebeten. Er teilte mit, dass es sich bei den drei angebrachten Kameras um Kameragehäuse (sog. Attrappen) handelte. Auf die „vermeintliche" Kameraüberwachung wurde mit einem Schild hingewiesen. Weiter führte er aus, dass die Attrappen zur Verhinderung von weiteren Diebstählen, Einbrüchen und Vandalismus dienen würden. Zusätzlich hatte er ebenfalls eine akustische Alarmanlage installiert. Auf der gegenüberliegenden Straßenseite befand sich das Lager der Firma. Die Kameraattrappe im 2. Stock sollte dazu dienen, dieses Grundstück zu erfassen, da eine Attrappe an der Lagerhalle in den Augen des Betreibers nicht zielführend gewesen wäre und potenziellee Straftäter diese entfernt oder zugeklebt hätten.
Nach Auffassung des TLfDI stellen auch Attrappen einen Eingriff in das vom Bundeverfassungsgericht entwickelte Grundrecht auf informationelle Selbstbestimmung dar. Daher sind die Vorgaben des Bundesdatenschutzgesetzes (BDSG) einzuhalten.
Bezüglich einer der Kameraattrappen, die auf den Vorgartenbereich gerichtet war, äußerte der TLfDI keine Bedenken. Der Kamerawinkel war so ausgerichtet, dass lediglich das eigene Grundstück erfasst wurde und sie konnte daher auch bei einer nicht mehr konkret vorliegenden Gefahrensituation, im Rahmen der Wahrnehmung des eigenen Hausrechts, weiterhin genutzt werden.
Die anderen Kameraattrappen waren so ausgerichtet, dass sie letztendlich öffentlich zugängliche Bereiche miterfassten. Bei der im Erdgeschoss befindlichen Kameraattrappe bestanden Anhaltspunkte, dass die schutzwürdigen Interessen von Betroffenen überwiegen, da diese auf den Eingangsbereich der Büroräume gerichtet war. Kunden, Brief- und Paketzusteller mussten sich somit zwangsweise in den beobachteten Bereich begeben und hatten keine Ausweichmöglichkeiten hinsichtlich des Erfassungsbereichs der Kameraattrappe. Die andere Attrappe im 2. Stock des Gebäudes war für den von dem Betreiber genannten Zweck, mögliche Einbrecher abzuschrecken, nicht geeignet. Aufgrund der Position ist diese für potenziellee Täter nicht erkennbar, da diese meist nur die nähere Umgebung absuchen. Außerdem wurde an dem Gebäude eine akustische Alarmanlage

angebracht. Die Ausführungen des Hausbesitzers belegen, dass die vorgefallenen versuchten Einbrüche durch die Alarmanlage verhindert wurden und nicht durch die angebrachte Kameraattrappe auf der anderen Straßenseite.
Daraufhin entfernte der Hausbesitzer alle drei Kameraattrappen.

Auch eine Videoattrappe stellt einen Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen dar, da diese nicht wissen, ob die Kamera tatsächlich Aufnahmen macht oder es sich lediglich um ein Kameragehäuse handelt. Daher löst auch eine Kameraattrappe einen Überwachungsdruck bei den Betroffenen aus.

6.68 Apotheken-Video – Videogaga 25

Im Berichtzeitraum erreichte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) eine Beschwerde bezüglich einer Videoüberwachung in den Verkaufsräumen einer Apotheke.
Der TLfDI ist nach § 42 Abs. 1 Thüringer Datenschutzgesetz i. V. m. § 38 Abs. 6 Bundesdatenschutzgesetz (BDSG) die nach § 38 Abs. 1 BDSG zuständige Aufsichtsbehörde für die Kontrolle der Einhaltung des BDSG sowie sonstiger datenschutzrechtlicher Vorschriften bei nicht-öffentlichen Stellen.
Im Rahmen dieser Zuständigkeit wandte sich der TLfDI mit einem Auskunftsersuchen nach § 38 Abs. 3 BDSG, das einen Fragenkatalog zu der Videoüberwachungsanlage enthielt, an den Apotheker. Zudem sollten der Beantwortung auch Nachweise beigefügt werden, wie zum Beispiel ein Lageplan des Ladens mit den eingezeichneten Standorten der Kameras und Screenshots, aus denen sich der Aufnahmebereich der Kameras erkennen lässt.
Daraufhin teilte der Apothekenbesitzer dem TLfDI mit, dass es sich bei den zwei Kameras nur um Attrappen handele, die zur Abschreckung von potenziellen Ladendieben dienten. Diese seien auf beiden Seiten der Verkaufstheke befestigt, mit Ausrichtung zu den Kassenplätzen.
Da auch Attrappen einen Eingriff in das Persönlichkeitsrecht seiner Kunden begründen können, wies der TLfDI den Apotheker auf diese Rechtslage hin.
Der Apotheker entfernte daraufhin die Attrappen in seiner Apotheke.

Der TLfDI ist die zuständige Aufsichtsbehörde für den Datenschutz (§ 42 Abs. 1 S. 1 ThürDSG i. V. m. § 38 Abs. 6 BDSG). Um seiner Kontrollaufgabe nachgehen zu können, wurden dem TLfDI Kompetenzen verliehen. Hierzu gehört unter anderem, dass gem. § 38 Abs. 3 BDSG die der Kontrolle unterliegenden Stellen sowie die mit deren Leitung beauftragten Personen der Aufsichtsbehörde auf Verlangen die für die Erfüllung ihrer Aufgaben erforderlichen Auskünfte unverzüglich zu erteilen haben. Wenn mit Vorsatz oder aus Fahrlässigkeit eine Auskunft unvollständig oder nicht rechtzeitig erteilt wird, kann dies mit einer Geldbuße geahndet werden.

6.69 Wenn der Thermenbesuch beobachtet wird – Videogaga 26

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) erfuhr durch einen Hinweis von Kameraaufnahmen in einer Therme. Im Umkleidebereich der Sauna würden die Besucher gefilmt.
Der TLfDI wandte sich mit einem Auskunftsersuchen an die Geschäftsführung der Therme. Der externe Datenschutzbeauftragte des Unternehmens antwortete und reichte die benötigten Nachweise ein. In der Therme war eine Videoüberwachungsanlage mit fünf Kameras installiert. Sie erfasste den Wert- und Kleiderspindbereich mit den dazwischenliegenden Gängen zum Zwecke der Prävention bzw. Aufklärung von Straftaten wie Schrankaufbrüchen und Vandalismus.
Durch eine Videoüberwachung werden personenbezogene Daten erhoben, Aufnahmerekorder speichern diese und führen damit eine Verarbeitung der Daten durch. Gemäß § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG) ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet.
Vorliegend wurden keine schriftlichen Einverständniserklärungen der Besucher eingeholt, was bei einer unbestimmten Anzahl an Besuchern auch praktisch nicht umsetzbar ist. Ebenso wurden von den betroffenen Mitarbeitern keine Einwilligungserklärungen abgegeben. Allerdings wären letztere auch nur unter äußerst engen Voraussetzungen möglich. Dem Arbeitnehmer müssen Wahlmöglichkeiten gegeben werden, sodass er auch ohne Betreten des überwachten Bereichs seiner Arbeit nachkommen kann. Erst dann kann eine Freiwilligkeit bei der Einverständniserklärung angenommen werden. Im vorliegenden Fall mussten die Mitarbeiter, insbesondere das Reini-

gungspersonal, den videoüberwachten Bereich zwangsläufig betreten, um ihre Tätigkeit ausüben zu können.
Somit verbleibt zur Beurteilung der Zulässigkeit der Videoüberwachungsanlage nur noch § 6b BDSG. Diese Norm regelt die Videoüberwachung von öffentlich zugänglichen Räumen durch nicht-öffentliche Stellen. Hierbei handelt es sich um Bereiche innerhalb oder außerhalb von Gebäuden, die nach dem erkennbaren Willen des Berechtigten (z. B. des Grundstückseigentümers) von jedermann genutzt oder betreten werden dürfen. Die Therme ist einem unbestimmten Personenkreis zugänglich, womit es sich um einen öffentlich zugänglichen Raum handelt.
Gem. § 6b Abs. 1. Nr. 2 bis 3 BDSG ist die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) durch nicht-öffentliche Stellen nur zulässig, soweit sie entweder zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Hier soll die Videoüberwachungsanlage zur Gewährleistung der Prävention bzw. Aufklärung von Straftaten wie Schrankaufbrüchen und Vandalismus dienen. Solange eine tatsächliche Gefahrenlage nachgewiesen werden kann, ist darin grundsätzlich ein berechtigtes Interesse zu erkennen. Jedoch muss dieser Umstand mit konkreten Nachweisen aus der Vergangenheit belegt werden. Dies erfolgte nach erneutem Nachfragen. Jedoch muss die Videoüberwachung auch erforderlich sein.
Dafür muss die Kameraüberwachung zur Erreichung dieses Zwecks geeignet sein und kein milderes Mittel darf zur Verfügung stehen, um den angestrebten Zweck bei gleicher Effektivität zu erreichen. Für den festgelegten Zweck sind jedoch einige Alternativen ersichtlich. Zunächst könnte ein besseres Schlosssystem in die Spinde eingebaut werden oder das Badepersonal könnte Kontrollgänge durchführen. Auch möglich wäre das Bereitstellen von Wertschließfächern im Kassenbereich, sodass diese sich unter ständiger Kontrolle des Kassenpersonals befinden. Ebenso sind Anhaltspunkte ersichtlich, dass schutzwürdige Interessen von Betroffenen überwiegen. Dabei ist eine Abwägung zwischen den berechtigten Interessen des Überwachenden und dem von der Überwachung Betroffenen vorzunehmen. Eine Videoüberwachung im Umkleide- und Spindbereich stellt einen erheblichen Eingriff in das informationelle Selbstbestimmungsrecht dar.

In diesem Bereich sind Menschen typischerweise spärlich bekleidet, und selbst wenn die Umkleidekabinen von dem Spindbereich getrennt sind, kann nicht automatisch davon ausgegangen werden, dass sich Besucher nicht doch in diesem Bereich entkleiden. Vor allem bei einem erhöhten Besucherandrang, wenn alle Umkleidekabinen belegt sind, werden manche Besucher den Spindbereich zum Umziehen nutzen. Eine Beobachtung der Intimsphäre durch eine Videoüberwachung stellt grundsätzlich keine verhältnismäßige und datenschutzrechtlich zulässige Maßnahme dar.
Somit überwiegen die schutzwürdigen Interessen der Besucher (Wahrung der Intimsphäre) gegenüber einer Überwachung zur Sicherung des Eigentums.
Der TLfDI ordnete das Entfernen der Kameras an. Dieser Aufforderung kam die verantwortliche Stelle auch nach. Das Verfahren konnte beim TLfDI daraufhin abgeschlossen werden. Die Einleitung eines Bußgeldverfahrens seitens des TLfDI gegen die verantwortliche Stelle wird derzeit geprüft.

Die Videoüberwachung im öffentlichen Bereich durch nicht-öffentliche Stellen ist nur in engen Grenzen zulässig. Der Gesetzgeber hat dies ausdrücklich und abschließend in § 6b BDSG geregelt. Gem. § 6b Abs. 1. Nr. 2 bis 3 BDSG ist die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) durch nicht-öffentliche Stellen nur zulässig, soweit sie entweder zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

6.70 Wildtierkameras

Im Berichtszeitraum wurde der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) seitens einer Polizeibehörde, welche sich mit immer wiederkehrenden Anfragen von Bürgern auseinandersetzen musste, befragt, ob ein privater Jagdpächter im Wald Wildtierkameras an Bäumen anbringen kann. Zunächst ist darauf hinzuweisen, dass seit dem Urteil des *Verwaltungsgerichts Saarland vom 18. Mai 2016, Az.: 1 K 63/15 (siehe Pressemitteilung des TLfDI vom 19. Mai 2017 Anlage 4*), welches durch Urteil des Oberverwaltungsgerichts Saarlouis vom

14. September 2017 bestätigt wurde, feststeht, dass auch Wildtierkameras der Meldepflicht des § 4d Abs. 1 BDSG unterliegen, da auch auf diese das Bundesdatenschutzgesetz anwendbar ist. Die Zulässigkeit des Einsatzes von Wildkameras durch nicht-öffentliche Stellen, wozu auch Privatpersonen (auch als Jäger) gehören, beurteilt sich nach § 6b Bundesdatenschutzgesetz (BDSG), da nach dem Thüringer Waldgesetz das Betreten des Waldes jedem gestattet ist und es sich somit um einen öffentlich zugänglichen Raum handelt. Nach § 6b Abs. 1 Nr. 3 BDSG ist der Betrieb von Wildkameras dann zulässig, wenn dies zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Ein berechtigtes Interesse der Jäger ist anzunehmen, soweit die Verwendung der Kameras den Bestand und den Wechsel des Wildes im Jagdbezirk feststellen soll. Jedoch überwiegen die schutzwürdigen Interessen der Betroffenen (z. B. Spaziergänger, Sporttreibende, Pilz- und Kräutersammler), sich im Wald unbeobachtet von technisch elektronischen Einrichtungen aufzuhalten. Im Ergebnis hält der TLfDI den Einsatz von Wildkameras in öffentlich zugänglichen Waldgebieten regelmäßig für unzulässig. Ausnahmen ergeben sich für die Bereiche, die ausschließlich und erkennbar vom Jagdrevierinhaber betreten werden dürfen, oder dann, wenn die Kameras so aufgestellt sind, dass eine Beobachtung von Personen unwahrscheinlich ist, etwa in entlegenen Waldgebieten oder durch das Anbringen der Kameras in entsprechend niedriger Höhe.
Zudem müssen in allen Fällen, in denen die Installation einer Wildkamera in einem öffentlich zugänglichen Raum datenschutzrechtlich zulässig ist, gemäß § 6b Abs. 2 BDSG der Umstand der Beobachtung und die verantwortliche Stelle durch geeignete Maßnahmen erkennbar gemacht werden.

Das Betreiben von Wildtierkameras durch die private Jägerschaft unterfällt seit dem Urteil des Verwaltungsgerichts Saarland vom 18. Mai 2016, Az. 1 K 63/15 (Pressemitteilung des TLfDI vom 19. Mai 2016) der sog. Meldepflicht des § 4d Abs. 1 BDSG. Durch das Oberverwaltungsgericht des Saarlands wurde dieses Urteil am 14. September 2017 bestätigt. Das Anbringen von Wildtierkameras in öffentlich zugänglichen Waldgebieten ist regelmäßig unzulässig, jedoch bestehen Ausnahmen, wenn in entlegenen Waldgebieten oder

durch das Anbringen der Kameras in entsprechend niedriger Höhe kein Personenbezug hergestellt werden kann.

6.71 Spielhalle: Videogaga 27

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichte eine Beschwerde über eine Videoüberwachungsanlage in einer Spielhalle. Der TLfDI wandte sich mit einem Auskunftsverlangen nach § 38 Abs. 3 Bundesdatenschutzgesetz (BDSG) an den Spielhallenbetreiber. Dieser teilte mit, dass die Videoüberwachungsanlage aus 16 Kameras bestehe, die folgende Bereiche erfasse:
Eingangsbereiche der Halle, beide Thekenbereiche, alle Geldspielgeräte sowie alle nicht von der Theke aus einsehbaren Bereiche. Die Aufnehmen werden elektronisch auf einer Festplatte für zehn Werktage gespeichert. Die Überwachung bestehe aufgrund der Unfallverhütungsverordnung (UVV) für Spielhallen, Spielcasinos und Automatensäle (§ 6 UVV), die sie verpflichtet, eine optische Raumüberwachung zu gewährleisten. Als Zweck der Überwachung wurden der Schutz des Personals, die Prävention und Abschreckung gegen potenziellee Straftäter und zum anderen die Erleichterung der Strafverfolgung angegeben. Die Mitarbeiter seien über die Videoüberwachung informiert worden und hätten alle mit einer schriftlichen Einverständniserklärung zugestimmt.
Nach § 4 Abs. 1 des Bundesdatenschutzgesetzes (BDSG) ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit eine Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Die Einwilligung bedarf gem. § 4a BDSG der Schriftform. Vorliegend wurden keine schriftlichen Einverständniserklärungen von den Besuchern eingeholt, was bei einer unbestimmten Anzahl an Besuchern auch praktisch nicht umsetzbar ist. Zudem muss die Einwilligung vor der Datenerhebung erfolgen. Allerdings werden bereits mit Betreten der Spielhalle (Kamera im Eingangsbereich) Daten der Besucher erhoben.
Zwar wurde von den Mitarbeitern eine schriftliche Einwilligung abgegeben, jedoch ist eine solche Einwilligung nur unter äußerst engen Voraussetzungen möglich. Dem Arbeitnehmer müssen Wahlmöglichkeiten gegeben werden, sodass er auch ohne Betreten des überwachten Bereichs seiner Arbeit nachkommen kann. Erst dann kann eine Freiwilligkeit bei der Einverständniserklärung angenom-

men werden. Vorliegend war dies nicht möglich, da die Spielhalle flächendeckend überwacht wurde.
§ 6 Abs. 2 der Unfallverhütungsvorschrift für Spielhallen, Spielcasinos und Automatensäle von Spielbanken (UVV BGV C3) fordert, dass optische Raumüberwachungsanlagen so installiert sind, dass wesentliche Phasen eines Überfalles optisch wiedergegeben werden können. Da eine Einwilligung also nicht infrage kommt, bedarf es einer Rechtsgrundlage, die die Videoüberwachung erlaubt. Die UVV stellt jedoch keine Rechtsgrundlage i. S. d. § 4 BDSG dar. Vielmehr ist die Zulässigkeit der Videoüberwachungsanlage anhand des § 6b BDSG, welcher die Videoüberwachung in öffentlich zugänglichen Bereichen regelt, zu prüfen. Demnach ist die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) nur zulässig, soweit sie entweder zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und außerdem keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.
Vorliegend wurde die Videoüberwachung zum Schutz vor Straftaten installiert. Darin ist grundsätzlich ein berechtigtes Interesse zu sehen, wenn eine tatsächliche Gefahrenlage nachgewiesen werden kann. Jedoch ist es in bestimmten Fällen auch möglich, eine abstrakte Gefährdungslage anzunehmen, wenn eine Situation vorliegt, die nach der Lebenserfahrung typischerweise gefährlich ist, z. B. in Geschäften, die im Hinblick auf Vermögens- und Eigentumsdelikte potenziell besonders gefährdet sind. Diese potenziellee Gefährdung kann bei einer Spielhalle unterstellt werden.
Das Videoüberwachungssystem muss allerdings auch erforderlich, also zur Erreichung des festgelegten Zwecks vor allem geeignet sein. Es darf kein milderes Mittel zur Verfügung stehen, das weniger in die Rechte der Betroffenen eingreift, um den angestrebten Zweck bei gleicher Effektivität zu erreichen. Zudem dürfen keine schutzwürdigen Interessen der Betroffenen überwiegen.
Aufgrund dieser Beschränkungen sah der TLfDI einige Aufnahmebereiche kritisch. Der Zeitvertreib in Spielhallen und das Spielen von Glücksspielen zählt zur Freizeitbeschäftigung der Betroffenen. Das dem Freizeitbereich zuzurechnende Verhalten untersteht einem besonders hohen Schutzbedarf des Persönlichkeitsrechts des Betroffenen. Im Normalfall überwiegt hier das schutzwürdige Interesse der Betroffenen gegenüber einer Überwachung. Deswegen ist eine Vi-

deoüberwachung nur in den Bereichen gerechtfertigt, in denen eine erhöhte Gefahr der Kriminalität besteht (z. B. Geldautomaten, die aufgebrochen oder manipuliert werden können). Gemäß § 3 Abs. 5 des Thüringer Spielhallengesetzes (ThürSpielhallenG) muss die Aufsicht des Spielhallenbetreibers von ihrem regelmäßigen Aufenthaltsort aus, auch unter Zuhilfenahme technischer Einrichtungen, alle Spielgeräte einsehen und Spieler beobachten können. Daher sind die Videokameras mit dem Aufnahmebereich der Geldspielgeräte zulässig. Die Videokameras, welche die Sitzgruppen und die Snookertische erfassen, sind jedoch nicht zulässig.
Auch bemängelte der TLfDI die Aufnahmen im Thekenbereich, wo sich Mitarbeiter dauerhaft aufhalten. Die Überwachung öffentlich zugänglicher Räume mit Publikumsverkehr, die gleichzeitig Arbeitsplätze erfasst, unterliegt strengen Anforderungen. Möglich ist eine Videoüberwachung insbesondere zur Erfüllung der Schutzpflicht des Arbeitgebers gegenüber den Beschäftigten, wenn eine Videoüberwachung in besonders gefahrträchtigen Arbeitsbereichen erforderlich ist. Dabei ist allerdings zu beachten, dass der Erfassungsbereich der Kamera auf den sicherheitsrelevanten Bereich beschränkt wird und die Beschäftigten soweit wie möglich ausgeblendet werden (Schwärzung des Aufnahmebereiches).
Außerdem beanstandete der TLfDI die lange Speicherfrist von zehn Tagen. Gemäß § 6b Abs. 5 BDSG sind die Daten unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen. Videoaufnahmen werden nicht mehr benötigt, wenn eine Gefahr nicht weiter abgewendet werden muss oder eine Beweissicherung nicht notwendig ist. Es sollte prinzipiell möglich sein, innerhalb von ein bis zwei Tagen zu klären, ob die Sicherung des Materials notwendig ist. Folglich hat die Löschung grundsätzlich spätestens nach 48 Stunden zu erfolgen. In begründeten Einzelfällen kann eine längere Speicherfrist akzeptiert werden.
Hierzu führte die verantwortliche Stelle aus: Die Manipulation an Spielautomaten ist nur beim elektronischen Auslesen der Geräte erkennbar. Dieses Auslesen kann jedoch nur alle 10 bis 14 Tage erfolgen, da es sonst zu Problemen bei der Erklärung der Vergnügungssteuer kommt. Diese Einwände können aber nur bei Kameraaufnahmen berücksichtigt werden, die Geldspielgeräte überwachen.
Bereits während des Schriftverkehrs demontierte die verantwortliche Stelle zwei Kameras, die vom TLfDI beanstandet wurden.

Da die Mitarbeiterüberwachung im Bereich der Theke und die lange Speicherung für alle Videokameras weiterhin vonstattengingen, erließ der TLfDI einen Anordnungsbescheid. In diesem gab er der verantwortlichen Stelle auf, die Kamera, die einen Snookertisch erfasste, innerhalb von zwei Wochen nach Bestandkraft des Bescheids zu entfernen. Außerdem soll die Speicherfrist aller Kameras, die keine Geldspielgeräte bewachen, auf 48 Stunden verkürzt werden. Weiterhin waren die Aufnahmebereiche der Kameras mit Blick auf die Thekenbereiche zu schwärzen, sodass die Mitarbeiter nicht mehr erkennbar waren. Wahlweise können die Kameras auch an einen Alarmknopf gekoppelt werden, sodass die Aufnahme erst durch eine Betätigung dieses Knopfes ausgelöst wird. Diesen Aufforderungen kam die verantwortliche Stelle nach. Daraufhin konnte das Verwaltungsverfahren abgeschlossen werden.

Gem. § 6b BDSG ist die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) nur zulässig, soweit sie entweder zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und außerdem keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. In Fällen der Mitarbeiterüberwachung und Freizeitgestaltung der Betroffenen überwiegt zumeist das schutzwürdige Interesse des Betroffenen (Überwachten) gegenüber dem Interesse des Bewachers. Nach § 6b Abs. 5 BDSG sind die Daten unverzüglich zu löschen, sobald feststeht, dass das Videomaterial nicht mehr benötigt wird. Grundsätzlich sollte nach 48 Stunden zu klären sein, ob eine Straftat vorgefallen ist. In begründeten Einzelfällen kann eine längere Speicherfrist akzeptiert werden.

6.72 Fahrgäste im Visier – Videogaga 28

Seit einigen Jahren steht der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) nun schon in Kontakt mit einem öffentlichen Nahverkehrsbetrieb (3.10 Busfahrer im Visier Videogaga 3 TB 2012/13) wegen der Installation von Kameras in dssen Bussen. Nachdem dort bereits eine datenschutzrechtliche Kontrolle erfolgt war, ruhte das Verfahren zunächst, da eine Einigung der Datenschutzaufsichtsbehörden im Düsseldorfer Kreis zu dieser Problematik abgewartet werden sollte. Dort wurde eine „Ori-

entierungshilfe in öffentlichen Verkehrsmitteln“ erstellt, welche auf der Website des TLfDI https://www.tlfdi.de/mam/tlfdi/datenschutz/video/oh_v_____pnv_stand_09_2015_dk.pdf zum Abruf zur Verfügung steht. Aufgrund der am 25. Mai 2018 Geltung erlangenden Europäischen Datenschutz-Grundverordnung (DS-GVO) wird diese Orientierungshilfe an die rechtlichen Neuerungen im Zusammenhang mit Videoüberwachungen angepasst werden. Die aktualisierte Orientierungshilfe wird dann ebenfalls auf der Website des TLfDI abrufbar sein.



Das Verfahren wurde nach Erstellung der Orientierungshilfe wieder aufgegriffen. Der TLfDI wollte zunächst von dem Betrieb erfahren, ob seit der Kontrolle Änderungen in Bezug auf die Videoüberwachung erfolgt sind. In den 26 Bussen wurden weiterhin jeweils 4 Kameras betrieben, welche den gesamten Fahrgastraum überwachten. Zudem konnten durch die Kameras teilweise Außenaufnahmen gefertigt werden. Ferner war auch zum Teil der Fahrerbereich zu erkennen.

Die Videoaufnahmen wurden in den Bussen ohne Vorfall 72 Stunden gespeichert. Diese Aufnahmen konnten mittels Auslösen eines Notfallschalters im Rahmen eines Vorfalls durch den Busfahrer dauerhaft gespeichert werden. Aufgrund der Aufnahmen und der anschließenden Speicherung werden personenbezogene Daten erhoben und verarbeitet. Nach § 4 Abs. 1 des Bundesdatenschutzgesetzes (BDSG) ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit eine Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.

Weder eine gesetzliche Grundlage außerhalb des BDSG war für den TLfDI ersichtlich, noch kam eine Einwilligung für die Videoüberwachung in Betracht. Die Zulässigkeit der Videoüberwachung in den Bussen richtete sich nach § 6b BDSG, da es sich hierbei um öffentlich zugängliche Räume handelt, welche von jedermann betreten werden können. Nach § 6b Abs. 1 Nr. 2 und 3 BDSG ist eine Überwachung mit optisch-elektronischen Einrichtungen zulässig, soweit sie entweder zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Zudem ist mit dem seit dem

4. Mai 2017 in Kraft getretenen Videoüberwachungsverbesserungsgesetz der neue Satz 2 zu berücksichtigen, wonach bei der Videoüberwachung von Fahrzeugen des öffentlichen Busverkehrs der Schutz von Leben, Gesundheit oder Freiheit von dort aufhältigen Personen als ein besonders wichtiges Interesse gilt. In den angeführten Zielen für die Videoüberwachung in der Datenschutzvereinbarung des Betriebes wurde u. a. angeführt: präventive Wirkung und Verringerung von strafbaren Handlungen wie z. B. Sachbeschädigungen, Eigentumsdelikte, Körperverletzungen und gefährliche Eingriffe in den Busverkehr sowie die verbesserte Strafverfolgung dieser einzelnen Delikte. Da vorliegend der Schutz von Leben und Gesundheit ein vordergründiges Ziel des Unternehmens zum Betreiben der Videoüberwachung war, musste dies bei den berechtigten Interessen und im Rahmen der Interessenabwägung berücksichtigt werden. Zudem war seitens des Unternehmens eine konkrete Gefahrenlage nachzuweisen, was durch die Nennung entsprechender Vorkommnisse mit den polizeilichen Tagebuchnummern ohne Probleme erfolgte. Ferner musste die Videoüberwachung für den festgelegten Zweck geeignet und erforderlich sein. Im Rahmen der Erforderlichkeitsprüfung ist nicht nur das „Ob“ der Videoüberwachung zu überprüfen, sondern auch das „Wie“. Dabei ist insbesondere der räumliche und zeitliche Umfang der Überwachung zu berücksichtigen. Vorliegend bestanden Bedenken hinsichtlich der durchgehenden Speicherung, obwohl es möglich war, mittels Notfallschalter im Rahmen eines Vorkommnisses die Aufnahme auszulösen. Zudem bestanden datenschutzrechtliche Bedenken betreffend der Außenaufnahmen durch die Videokameras. Hier waren auf den einzelnen Screenshots parkende Pkw zu erkennen, wenn auch nicht mit deren Kennzeichen, sowie die an den Haltestellen wartenden Personen. Eine Schwärzung der Aufnahmen war technisch nachweisbar nicht möglich, jedoch ist die Ausrichtung der Kameras so vorzunehmen, dass entweder keine Außenaufnahmen oder nur solche ohne Personenbezug stattfinden. Diese sind für die von dem Unternehmen genannten Zwecke nämlich nicht erforderlich. Zudem bestanden vorliegend Anhaltspunkte, dass schutzwürdige Interessen der betroffenen Fahrgäste überwiegen. Entscheidend ist hierbei die Eingriffsintensität der jeweiligen Maßnahme. Diese wird durch Art und Umfang der erfassten Informationen (Informationsgehalt und Informationsdichte), durch Anlass und Umstände der Erhebung (zeitliches und räumliches Ausmaß des Videoeinsatzes) durch den betroffenen Per-

sonenkreis und die Art und den Umfang der Verwertung der erhobenen Daten bestimmt. Das Unternehmen überwachte vorliegend während der gesamten Fahrtzeit auf jeder Linie den kompletten Fahrgastraum. Das informationelle Selbstbestimmungsrecht der Fahrgäste in diesen Bereichen ist besonders intensiv betroffen, da Menschen dort typischerweise miteinander kommunizieren, sich aber jedenfalls längere Zeit aufhalten. Hinzu tritt, dass die Fahrgäste häufig auf die Nutzung der öffentlichen Verkehrsmittel angewiesen sind und nur bedingt auf andere Verkehrsmittel und damit der Videoüberwachung ausweichen können. Ferner ist dort eine Vielzahl von Personen betroffen, die durch ihr Verhalten keinerlei Anlass für eine Beobachtung geben. Ein solch intensiver Eingriff in das Recht auf informationelle Selbstbestimmung ist nur zum Schutz von Rechtsgütern erheblichen Gewichts (z. B. Schutz vor Gewalt von Personen) gerechtfertigt. Mit dem Urteil des Oberverwaltungsgerichts Niedersachsen vom 07.09.2017, Az.: 11 LC 59/16 ergaben sich erhebliche Änderungen bei der Beurteilung der Zulässigkeit von Videoüberwachungen im Personennahverkehr. Eine Differenzierung des Einsatzes der Videoüberwachung nach Strecken, Tageszeiten und Fahrzeugbereichen, wie bisher durch die Aufsichtsbehörden gefordert, wurde seitens des Gerichts abgelehnt, da das Unternehmen vortragen konnte, dass Störungen und Vorkommnisse auf sämtlichen Strecken und zu jeder Tag- und Nachtzeit vorgefallen sind. Auch bei dem hier geprüften Busunternehmen konnte dieser Sachverhalt festgestellt werden. Jedoch wurde durch das Gericht auch in der Interessenabwägung berücksichtigt, dass bestimmte technische organisatorische Maßnahmen seitens der Unternehmen zu treffen sind, um dadurch die schutzwürdigen Interessen der Betroffenen umfassend zu berücksichtigen. Insbesondere sind hier zu nennen: eine kurze Speicherfrist (24 Stunden), bei der Auswertung der Datenträger müssen Zugriffsbeschränkungen bestehen, die Daten müssen in einem gesonderten abschließbaren Raum gesichert werden zu dem nur ein schriftlich festgelegter Personenkreis Zugriff hat und diese Daten dürfen nur auf einen nicht vernetzten Computer abgelegt werden. Der TLfDI schloss sich im vorliegenden Fall der Auffassung des Oberverwaltungsgerichts an. Dem Unternehmen wurde die geänderte Rechtsauffassung mitgeteilt. Jedoch sind weiterhin die Außenaufnahmen aus den Bussen heraus unzulässig. Auch sind seitens des Unternehmens entsprechende technische organisatorische Maßnahmen, wie in dem Urteil aufgeführt, zu treffen und schriftlich festzulegen. Das Verfah-

ren ist beim TLfDI daher noch nicht abgeschlossen. Über den Ausgang des Verfahrens wird voraussichtlich in dem nächsten Tätigkeitsbericht abschließend informiert werden.



Bisher wurde seitens der Aufsichtsbehörden bei der Videoüberwachung in öffentlichen Verkehrsmitteln von den verantwortlichen Stellen eine Differenzierung der Überwachung gefordert. Die entsprechende Orientierungshilfe zur Videoüberwachung in öffentlichen Verkehrsmitteln wird auf der Website des TLfDI bereitgestellt (https://www.tlfdi.de/mam/tlfdi/datenschutz/video/oh_v_____pnv_stand_09_2015_dk.pdf). Eine generelle, zeitlich und räumlich durchgängige Videoüberwachung des gesamten Fahrgastbereiches nach § 6b BDSG ist danach unverhältnismäßig und daher unzulässig. Die Erwägungen des Urteils des Oberverwaltungsgerichts Niedersachsen, sowie das Videoüberwachungsverbesserungsgesetz führen jedoch aus Sicht des TLfDI dazu, dass eine Videoüberwachung in Bussen und sonstigem öffentlichen Verkehr zukünftig eher als zulässig zu betrachten sein wird. Jedoch verbleibt es dabei, dass jede eingesetzte Videoüberwachung auch im Personennahverkehr eine Einzelfallentscheidung bleibt und keine generelle Zulässigkeit von Videoüberwachungen in Bussen und Bahnen angenommen werden kann.

6.73 Kameras im Imbiss – Videogaga 29

Dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) wurde aufgrund einer Beschwerde eine Videoüberwachung in einem Imbiss bekannt. Der TLfDI ermittelte zunächst die Eigentümer des Imbisses und wandte sich mit einem Auskunftsersuchen an die Inhaber. Diese teilten mit, dass zwei Videokameras installiert wurden. Die erste Kamera war auf den Eingangsbereich gerichtet, welche jedoch auch den Bereich der Stehti-

sche erfasste. Eine weitere war auf die Kasse ausgerichtet. Diese Kamera wurde jedoch nur eingeschaltet, wenn die Betreiber des Imbisses allein im Geschäft waren und einer von beiden in den Keller gehen musste. Die Kamerabilder wurden dann auf einen kleinen Monitor übertragen, um die Kasse im Blick zu behalten. Es erfolgte keine Aufzeichnung, sondern eine Echt-Zeit-Beobachtung (Monitoring) mittels der Kameras.

Maßgebliche Vorschrift für die Beurteilung der Zulässigkeit der hier betriebenen Videokameras ist § 6b Abs. 1 Bundesdatenschutzgesetz (BDSG), da es sich bei dem Gastraum während der Öffnungszeiten um einen öffentlich zugänglichen Raum handelt. Danach ist das Beobachten öffentlich zugänglicher Räume per Videoüberwachung zulässig, soweit es zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Problematisch war hier insbesondere die Kamera, welche auf den Stehtischbereich ausgerichtet war. Die Videoüberwachung des Gastraums einer Gaststätte ist nach § 6b BDSG im Regelfall datenschutzrechtlich unzulässig. Gemeint ist die Gaststätte i. S. d. § 1 Gaststättengesetzes (GastG), d. h. ein Betrieb, in welchem Getränke und/oder Speisen zum Verzehr an Ort und Stelle verabreicht werden und der jedermann oder bestimmten Personenkreisen zugänglich ist. Darunter fallen insofern auch Imbisslokale und Schnellrestaurants. Die mit Tischen und Sitzgelegenheiten ausgestatteten Gastronomiebereiche sind die Bereiche, die zum längeren Verweilen, Entspannen und Kommunizieren einladen und somit nicht mit Videokameras überwacht werden dürfen (siehe hierzu Urteil des Amtsgerichts Hamburg vom 22. April 2008 – 4 C 134/08). Das dem Freizeitbereich zuzurechnende Verhalten als Gast einer Gaststätte geht mit einem besonders hohen Schutzbedarf des Persönlichkeitsrechts des Betroffenen einher. Eine Videoüberwachung stört die unbeeinträchtigte Kommunikation und den unbeobachteten Aufenthalt der Gaststättenbesucher und greift damit besonders intensiv in das Persönlichkeitsrecht des Gastes ein. Das schutzwürdige Interesse des Besuchers überwiegt im Normalfall das berechtigte Interesse des Gastronomieinhabers an einer Überwachung, weshalb sich dessen Interesse nur in seltenen Ausnahmefällen durchsetzen kann. Im vorliegenden Fall wurde seitens der Imbissinhaber auch kein berechtigtes Interesse zum Betreiben der Kamera benannt, sodass in jedem Fall die schutzwürdigen Interessen über-

wiegen. Hinsichtlich der anderen Kamera, welche auf die Kasse ausgerichtet war, bestanden keine Bedenken, da diese nur für den Fall eingeschaltet wurde, dass die Betreiber allein im Lokal waren und Mitarbeiter- sowie Kundeninteressen nicht betroffen waren.
Der TLfDI teilte den Betreibern der Videokameras seine Rechtsauffassung mit, woraufhin diese die problematische Kamera deinstallierten. Ein weiteres Einschreiten des TLfDI war daher nicht erforderlich.

Im Berichtszeitraum wurde der TLfDI mehrmals auf Videoüberwachungen in Gasträumen von Gaststätten aufmerksam gemacht. Die Videoüberwachung von Gasträumen, welche mit Tischen und Sitzgelegenheiten ausgestattet sind, ist während der üblichen Geschäftszeiten oder wenn sich sonstiges Personal darin aufhält, im Regelfall datenschutzrechtlich aufgrund des intensiven Eingriffs in das informationelle Selbstbestimmungsrecht der Gäste oder des Personals unzulässig. Gerade in diesem Freizeitbereich, wo die ungestörte und unbeeinträchtigte Kommunikation im Vordergrund steht, ist der Schutz der Betroffenen vor Beobachtung in diesem Bereich besonders wichtig.

6.74 Mieter unter Beobachtung – Videogaga 30

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) wurde seitens eines Bürgers auf eine Videoüberwachung aufmerksam gemacht, welche auf die öffentliche Straße und den Gehweg gerichtet war. Im Wege der Amtshilfe durch eine thüringische Stadtverwaltung konnte tatsächlich eine Kamera an der Einfahrt zum Hinterhof festgestellt werden. Gleichzeitig wurde der Eigentümer des Gebäudes hinsichtlich der betriebenen Videoüberwachung mittels Auskunftsersuchens angeschrieben, um den Sachverhalt zu ermitteln.
Der Eigentümer teilte daraufhin mit, dass er zwei Videokameras an dem Gebäude installiert hatte. Eine Kamera war an der Toreinfahrt angebracht und so ausgerichtet, dass sie den Eingang zum Haus, sowie die Briefkästen und den Fahrradständer erfasste. Der Gehweg und die öffentliche Straße wurden ausgepixelt und waren nicht zu erkennen. Eine weitere Kamera befand sich im hinteren Hausbereich, welche ebenfalls den Fahrradständer und den Sitz- und Bankbereich im Garten abbildete. Das Gebäude bewohnte zum einen der Eigen-

tümer selbst, zum anderen lebten dort mehrere Mietparteien. Als Zweck zum Betreiben der Kameras gab der Eigentümer an, dass die Abschreckung von Vorfällen wie das Stehlen von Fahrrädern, Graffitiverschmutzungen und Beschädigungen am Fahrzeug im Vordergrund steht.
Nach § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG) sind die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Zwar wurde seitens des Eigentümers eine Liste von Einwilligungserklärungen seitens der Mieter eingereicht, jedoch wurde die Einwilligung entgegen § 4a Abs. 1 BDSG erst nach Datenerhebung erteilt und war daher nicht mehr zu berücksichtigen. Hinzu kommt, dass auch die Besucher, sowie sonstige von der Videoüberwachung Betroffene vor der Erhebung der personenbezogenen Daten, also vor Betreten des videoüberwachten Bereichs eine schriftliche Einwilligung erteilen müssten, was praktisch nicht umsetzbar ist. Daher scheidet eine Einwilligung für die in diesem Fall betriebene Videoüberwachung aus.
Bei den beiden Kameras ist zu unterscheiden, welche Bereiche durch die Aufnahmen erfasst werden. Bei der Kamera, welche den Eingangsbereich überwacht, beurteilt sich die Zulässigkeit der betriebenen Videoüberwachung nach § 6b Abs. 1, 3 BDSG. Danach ist eine Beobachtung mittels optisch-elektronischen Einrichtungen zulässig, soweit sie zur Wahrnehmung des Hausrechts oder zur Wahrnehmung des berechtigten Interesses für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Bei dem mit der ersten Kamera überwachten Hauseingangsbereich handelt es sich um die Überwachung eines öffentlich zugänglichen Raums, da dieser von jedermann betreten werden kann. Der von dem Betreiber genannte Zweck kann dann ein berechtigtes Interesse zum Betreiben der Videoüberwachung darstellen, wenn eine tatsächliche Gefahrenlage nachgewiesen werden kann. Hierfür trug der Eigentümer im weiteren Verfahren vor, dass es in der Vergangenheit zu Strafanzeigen wegen Fahrraddiebstählen, Sachbeschädigungen an der Gebäudewand und am privaten Pkw gekommen sei. Die Aufzählung der Vorkommnisse reichte in diesem Fall aus, um ein berechtigtes Interesse bejahen zu können.

Es bestanden jedoch Anhaltspunkte, dass schutzwürdige Interessen von Betroffenen, in diesem Fall der Mieter und der Besucher des Hauses, die berechtigten Interessen am Betreiben der Videoüberwachung überwiegen. Die dauerhafte Überwachung von Eingängen zu Wohngebäuden lässt Rückschlüsse auf den Tagesablauf und die sonstige Lebensführung der Mieter zu. Die Bilder dokumentieren einen nicht unerheblichen Bereich des Privatlebens. Auch werden Besucher der Mieter miterfasst. Hinzu kommt, dass die Mieter und Besucher des Gebäudes auf die Nutzung des Eingangs angewiesen sind, sodass hier ein erheblicher Eingriff in deren informationelles Selbstbestimmungsrecht vorliegt. Eine Überwachung in diesem Bereich kann nur dann zulässig sein, wenn schwerwiegenden Beeinträchtigungen der Rechte des Betreibers nicht in zumutbarer anderer Weise begegnet werden könnte (LG Berlin, Urteil vom 23. Mai 2005, Az. 62 S 37/05). Hierzu wurde seitens des Betreibers nichts vorgetragen. Die genannten Vorkommnisse waren nicht so schwerwiegend, dass eine Videoüberwachung in diesem Bereich gerechtfertigt wäre.

Die zweite Kamera war in einem nicht-öffentlich zugänglichen Bereich angebracht, da hier nur die Bewohner und Eigentümer des Hauses Zutritt zum Hinterhof und Gartenbereich hatten. Hier richtet sich die Beurteilung der Zulässigkeit nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG, wonach das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten für die Erfüllung eigener Geschäftszwecke zulässig ist, soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass schutzwürdige Interessen an dem Ausschluss der Verarbeitung überwiegen. Hier gelten ähnliche Voraussetzungen für eine Videoüberwachung wie bei § 6b BDSG, sodass insbesondere auf die oben gemachten Ausführungen zum berechtigten Interesse verwiesen wird. Vorliegend bestanden bei der Kamera Bedenken hinsichtlich der Erforderlichkeit. Ausreichend für den genannten Zweck war eine Ausrichtung nur auf den Fahrradständer. Zudem gab es Anhaltspunkte für das Überwiegen schutzwürdiger Interessen von Betroffenen, also den Mietern des Hauses. Da der Sitzbereich, als Ruhe- und Kommunikationsmöglichkeit der freien Entfaltung der Persönlichkeit dient, stellt eine dauerhafte Überwachung einen erheblichen Eingriff in das Freizeitverhalten der Nutzer dieses Bereichs dar. Beide Kameras sah der TLfDI im Hinblick auf die Ausrichtung für unzulässig an. Diese Auffassung wurde dem Eigentümer mitgeteilt.

Das Verfahren ist noch nicht abgeschlossen, da eine weitere Verpixelung der nunmehr eingereichten Videobilder erfolgen muss.

Bei der Videoüberwachung von Hauseingangsbereichen handelt es sich um die Überwachung von öffentlich zugänglichen Räumen, unabhängig davon, ob sich diese auf dem eigenen Grundstück befinden. Insbesondere in Mehrfamilienhäusern mit Mietparteien ist dieser Bereich als datenschutzrechtlich sehr empfindlich einzustufen. Hier überwiegen die schutzwürdigen Interessen der Betroffenen zumeist die berechtigten Interessen der Betreiber der Videoüberwachung. Die Mieter und deren Besucher sind auf die Nutzung des überwachten Bereichs angewiesen. Die Form der Überwachung lässt zudem Rückschlüsse auf deren Tagesablauf und die sonstige Lebensführung zu und liefert neben der hohen Informationsdichte einen besonderen Informationsgehalt. Dabei dokumentieren die Bilder einen nicht unerheblichen Bereich des Privatlebens. Eine Überwachung in diesem Bereich kann nur dann zulässig sein, wenn schwerwiegenden Beeinträchtigungen der Rechte des Betreibers nicht in zumutbarer anderer Weise begegnet werden könnte (LG Berlin, Urteil vom 23. Mai 2005, Az. 62 S 37/05).

6.75 Videokameras als Türsteherersatz? – Videogaga 31

Im Berichtszeitraum hat eine Stadtverwaltung dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) eine Videoüberwachung im Außenbereich einer Diskothek gemeldet, welche auch die öffentliche Straße und Gehwege miterfassen sollte. Der TLfDI wandte sich daraufhin an die Betreiber der Diskothek, um mithilfe eines Auskunftsersuchens den Sachverhalt aufzuklären.
Der Diskothekenbetreiber teilte mit, dass vier Videokameras installiert waren. Eine Kamera befand sich im inneren Eingangsbereich der Diskothek, zwei waren außen seitlich zum Eingang gerichtet angebracht. Diese bildeten die Straßenkreuzung sowie einen Großteil des Gehweges mit ab. Eine weitere Kamera war an der Eingangstür Richtung Straße ausgerichtet. Die Kameras zeichneten nicht auf und wurden während der Öffnungszeiten der Diskothek eingeschaltet. Die Kameras sollten zur Gefahrenabwehr eingesetzt werden.
Die Zulässigkeit der betriebenen Videoüberwachung richtet sich während der Öffnungszeiten vorliegend nach § 6b Abs. 1 Bundesda-

tenschutzgesetz (BDSG), wonach das Beobachten öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) nur zulässig ist, soweit es zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist. Der angegebene Zweck Gefahrenabwehr war im vorliegenden Fall zu unkonkret, da nicht deutlich wurde, welche Gefahren genau abgewehrt werden sollten. Hierzu ist es auch erforderlich, eine tatsächliche Gefahrenlage nachzuweisen, d. h. etwaige Vorkommnisse aus der Vergangenheit mit Datum, Art und Schadenshöhe zu dokumentieren oder polizeiliche Tagebuchnummern oder staatsanwaltschaftliche Aktenzeichen zu nennen. Im Verwaltungsverfahren hatte der Betreiber der Videoüberwachung hierzu nichts vorgetragen. Insofern lag kein berechtigtes Interesse zum Betreiben der Videokameras vor. Zudem bestanden Bedenken hinsichtlich der Erforderlichkeit der Videoüberwachungsanlage. Es darf kein gleich geeignetes milderes Mittel zum Erreichen des Zwecks vorhanden sein. Es wäre möglich, entsprechendes Sicherheitspersonal während des Einlasses zu positionieren, um ein Eingreifen bei entsprechenden Delikten vor der Tür zu ermöglichen. Dies ist eine gängige Praxis bei Diskotheken. Aber nicht nur das „Ob“ des Einsatzes der Videoüberwachung ist Gegenstand der Erforderlichkeitsprüfung, sondern auch das „Wie“, also der zeitliche und räumliche Umfang der eingesetzten Videotechnik. Insbesondere die Kameras im Außenbereich, welche die öffentliche Straße und einen Großteil des Gehwegs überwachten, waren für den Zweck nicht erforderlich. Die Kameras waren hier so auszurichten, dass die Straße außerhalb des Erfassungsbereichs lag. Da kein berechtigtes Interesse zum Betreiben der Kameras bejaht werden konnte, musste die Erforderlichkeit im Rahmen der Wahrnehmung des eigenen Hausrechts überprüft werden. Die Ausrichtung ist hier lediglich bis einen Meter von der Hauswand entfernt in den öffentlichen Raum zulässig, was in diesem Fall ebenfalls nicht erfüllt war.
Der TLfDI teilte dem Betreiber der Videokameras seine Rechtsauffassung mit. Der Diskothekenbetreiber stellte daraufhin die komplette Videoüberwachung in seiner Diskothek ein, sodass ein weiteres Einschreiten des TLfDI nicht erforderlich war.

Der Einsatz einer Videoüberwachung sollte seitens der verantwortlichen Stelle genau überlegt werden. Insbesondere die mit der Videoüberwachung verfolgten Zwecke sind so konkret wie möglich zu

bezeichnen. Eine pauschale Angabe von Sicherheitsgründen oder zur Gefahrenabwehr reicht hierfür nicht aus. Die Erforderlichkeit jeder einzelnen Kamera ist an dem genannten Zweck zu überprüfen. Es scheitert hier sehr oft bereits an der Geeignetheit der Kamera zu diesem Zweck. Auch existieren oft mildere Mittel, deren Einsatz die verantwortlichen Stellen aufgrund des höheren Aufwandes scheuen.



Personal - ©Wolfilser / Fotolia.com

7 Beschäftigtendatenschutz

7.1 Videoüberwachung im Freizeitpark

Ein Besucher eines Freizeitparks nahm neben den dargebotenen Attraktionen auch immer wieder Videokameras wahr, während er vergeblich den vorgeschriebenen Hinweis darauf suchte. Er wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) als zuständige Datenschutzaufsichtsbehörde nach § 42 Abs. 1 Satz 1 Thüringer Datenschutzgesetz (ThürDSG) in Verbindung mit § 38 Abs. 6 Bundesdatenschutzgesetz (BDSG), der nach § 38 Abs. 1 BDSG die Einhaltung datenschutzrechtlicher Bestimmungen kontrolliert, die den Einzelnen davor schützen sollen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.
Auf das an den Freizeitpark betreibende Unternehmen gerichtete Auskunftsersuchen nach § 38 BDSG teilte dieses mit, es habe bereits vor Jahren 13 Kameras installiert, um den reibungslosen Betriebsablauf zu gewährleisten. Aufzeichnungen würden nicht angefertigt, es erfolge eine reine Beobachtung der erfassten Bereiche.
Nach § 6b Abs. 1 BDSG ist das Beobachten öffentlich zugänglicher Räume per Videoüberwachung nur zulässig, soweit es zur Wahr-

nehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte für das Vorliegen überwiegender schutzwürdiger Interessen der betroffenen Personen bestehen. Um die Zulässigkeit der Videoüberwachung prüfen zu können, wurde das Unternehmen gebeten, zu jeder einzelnen Kamera die Angabe des Zwecks der Videoüberwachung darzulegen. Es ist im Vorhinein konkret festzulegen und schriftlich zu dokumentieren, welchem Zweck die Videoüberwachung im Einzelfall dienen soll. Dabei ist der Überwachungszweck jeder einzelnen Kamera gesondert und konkret schriftlich festzulegen, § 6b Abs. 1 Nr. 3 BDSG. Weiterhin wurde erfragt, ob die verfolgten Zwecke tatsächlich mit der Videoüberwachung erreicht werden können. Ferner wurde das Unternehmen darauf hingewiesen, nach § 6b Abs. 2 BDSG den Umstand der Beobachtung und die verantwortliche Stelle durch geeignete Maßnahmen erkennbar zu machen. Der Hinweis kann mit Hilfe entsprechender Schilder oder grafischer Symbole (z. B. Piktogramm nach DIN 33450) erfolgen. Er ist so (etwa in Augenhöhe) anzubringen, dass der Betroffene vor dem Betreten des überwachten Bereichs den Umstand der Beobachtung erkennen kann. Der Betroffene muss einschätzen können, welcher Bereich von einer Kamera erfasst wird, damit er in die Lage versetzt wird, gegebenenfalls der Überwachung auszuweichen oder sein Verhalten anzupassen. Außerdem muss die für die Datenverarbeitung verantwortliche Stelle erkennbar sein, das heißt, wer genau die Videodaten erhebt, verarbeitet oder nutzt. Entscheidend ist dabei, dass für den Betroffenen problemlos feststellbar ist, an wen er sich bezüglich der Wahrung seiner Rechte ggf. wenden kann. Daher ist die verantwortliche Stelle grundsätzlich mit ihren Kontaktdaten explizit auf dem Hinweisschild zu nennen.

Gegen die Mehrzahl der Kameras bestanden keine datenschutzrechtlichen Bedenken. Sie beobachteten lediglich den Besucherstrom und ermöglichten dem Personal so, den Eintritt zu bestimmten Bereichen zu steuern. So wurde verhindert, dass sich zu viele Personen dort aufhielten. Problematisch war, dass neben den dargebotenen Attraktionen im Freizeitpark auch der Eingangsbereich mit Kassenhäuschen, das Restaurant im Innenbereich und der Andenken-Verkaufsraum überwacht wurden. Dies schloss eine Erfassung der Mitarbeiter in diesen Bereichen ein und konnte eine unzulässige Leistungs- und Verhaltenskontrolle ermöglichen. Daher kam der Abwägung mit den Interessen der Betroffenen im Sinne von § 6b

Abs. 1 BDSG besondere Bedeutung zu. Als zulässig sah der TLfDI an, den Zugang des Besucherstroms an den Kassenhäuschen gegebenenfalls zu koordinieren, wobei allerdings ausgeschlossen sein musste, dass der dort tätige Mitarbeiter einer ständigen Beobachtung ausgesetzt war. Andererseits konnte die Beobachtung der Gäste und Mitarbeiter im Restaurant nicht mit der Sicherstellung eines geordneten Betriebsablaufs begründet werden. Sollte dort weiteres Personal erforderlich sein, um das hohe Besucheraufkommen bewältigen zu können, kann man dies auf andere Weise, wie etwa eine telefonische Anforderung weiteren Personals, bewerkstelligen. Eine ständige Beobachtung des Bedienpersonals und der sich dort aufhaltenden Gäste war nicht erforderlich. Im Verkaufsraum musste ebenfalls nicht das Personal beobachtet werden. Ob letztendlich Diebstähle durch Besucher dort durch eine Beobachtung per Videokamera verhindert oder aufgeklärt werden konnten, erschien mehr als fraglich. Um im Falle eines vom Verkaufspersonal bemerkten Diebstahls oder gar Überfalls Hilfe anzufordern, hätte auch ein Notrufknopf ausreichen können. Daraufhin stellte das Unternehmen klar, dass es alle Kameras in eine Wechselschleife eingebunden hatte, sodass nur noch Einzelbilder in bestimmten Zeitabständen auf den Monitoren erschienen. Diese Einzelbilder seien aber unverzichtbar, um mit wenig Personal die komplexen Betriebsabläufe sicherzustellen. Im Übrigen habe man die Kameras im Restaurant so ausgerichtet, dass das Essverhalten der Besucher nicht mehr beobachtet werden konnte.
Weiterhin hatte man Hinweisschilder angebracht, die auf die Kameraüberwachung aufmerksam machten. Daher war kein weiteres Vorgehen erforderlich.

Werden öffentlich zugängliche Räume mittels einer Videoanlage überwacht, ist der konkrete Zweck für jede einzelne Kamera vorab schriftlich festzulegen. Die Videobeobachtung muss für den angegebenen Zweck geeignet sein. Weiterhin muss mit den schutzwürdigen Interessen der von der Überwachung Betroffenen abgewogen werden. Eine ständige Beobachtung von Beschäftigten ist grundsätzlich nicht zulässig.

7.2 Frau am Facebook-Pranger

Eine Beschwerde einer zwischenzeitlich ausgeschiedenen Mitarbeiterin eines Unternehmens erreichte den Thüringer Landesbeauftrag-

ten für den Datenschutz und die Informationsfreiheit (TLfDI). Die Arbeitnehmerin musste feststellen, dass ihr ehemaliger Arbeitgeber über das soziale Netzwerk „Facebook“ alle Welt wissen ließ, er habe gegen sie wegen Verdachts des gewerbs- und bandenmäßigen Betrugs in mindestens 50 Fällen Strafanzeige erstattet. Sie solle sich durch Verbuchung von Scheinlieferungen persönlich bereichert und einen Schaden in sechsstelliger Höhe verursacht haben.
Eine entsprechende Schadensersatzklage gegen die Mitarbeiterin war vom zuständigen Arbeitsgericht abgewiesen worden. Angefragt erklärte das Unternehmen, man sei gegen das Urteil in Berufung gegangen, aber von der Schuld der Betroffenen überzeugt. Weil eine gütliche Einigung nicht möglich war, habe man sich unter Inanspruchnahme des Grundrechts auf Meinungsfreiheit zu der Veröffentlichung auf der vorrangig firmeninternen Plattform entschlossen. Das sei man im Übrigen auch den anderen Mitarbeitern schuldig gewesen, denn der Vorgang habe innerhalb der Belegschaft für Beunruhigung gesorgt. Man habe ja auch nur von einem „Verdacht“ gesprochen.
Dass die Veröffentlichung auf https://www.facebook.com zweifellos nicht nur auf einer firmeninternen, sondern einer weltweit öffentlich zugänglichen Plattform erfolgt, hätte dem Unternehmen klar sein müssen. Verkannt wurde darüber hinaus auch, dass das Grundrecht auf Meinungsfreiheit seine Schranken in den Vorschriften der allgemeinen Gesetze findet und dass eine solche Schranke auch § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG) darstellt. Danach ist eine Veröffentlichung personenbezogener Daten nur erlaubt, wenn dies eine Rechtsvorschrift zulässt oder die Einwilligung des Betroffenen vorliegt. Beides war in keiner Weise ersichtlich. Dass es sich bei der unzulässigen Veröffentlichung auf Facebook nicht um eine Lappalie handelt, zeigt schon, dass dies mit einem Bußgeld bis zu dreihunderttausend Euro geahndet werden kann (§ 43 Abs. 2 Nr. 1 und 2, Abs. 3 Satz 1 2. Halbsatz BDSG). Der TLfDI leitete daher auch ein Bußgeldverfahren ein.



Immerhin hatte das Unternehmen den Facebook-Eintrag nach kurzer Zeit gelöscht. Der weiteren Forderung, schriftliche Festlegungen durch das Unternehmen zur Nutzung von Facebook zu treffen, kam das Unternehmen letztendlich auf massives Drängen des TLfDI

nach. Danach dürfen grundsätzlich keine personenbezogenen Daten Beschäftigter auf dieser Plattform veröffentlicht werden, sofern keine wirksame Einwilligung der Betroffenen vorliegt. Wirksam ist eine Einwilligung allerdings nur, wenn sie freiwillig erteilt wurde. Im Beschäftigtenverhältnis ist dies nur dann der Fall, wenn der Beschäftigte unter keinerlei Zwang steht. Da man im Beschäftigtenverhältnis aber fast immer von einem gewissen Druck ausgehen kann, unter dem die Betroffenen stehen, die „gewünschte“ Einwilligung abzugeben, ist nur in sehr seltenen Fällen von Freiwilligkeit auszugehen. Festgelegt wurden auch die Verantwortlichkeiten für die Veröffentlichung und Modalitäten der Überwachung der Einträge.

Egal wie ärgerlich es ist, wenn man zu seinem vermeintlichen Recht nicht kommt. Eine Rechtfertigung, einen ehemaligen Mitarbeiter in sozialen Medien anzuprangern, gibt es nicht. Zum Betrieb von Facebook-Fanpages für Unternehmenszwecke sind entsprechende Festlegungen zu treffen.

7.3 (K)ein Kraftaufwand: Videoüberwachung im Fitnessstudio

Ein Bürger informierte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) darüber, dass in einem Fitnessstudio im Eingangs- und Bürobereich Kameras installiert seien, um die Mitarbeiter hinsichtlich Verhalten, Tätigkeit und Leistung zu überwachen. Der Beschwerdeführer bat den TLfDI um datenschutzrechtliche Bewertung dieses Sachverhalts.
Für die Erstellung von Videoaufnahmen ist gemäß § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG) eine gesetzliche Ermächtigung oder die Einwilligung des Betroffenen erforderlich. Als zuständige Aufsichtsbehörde kontrolliert der TLfDI gemäß § 38 Abs. 1 BDSG, ob bzw. dass Videoaufzeichnungen nach den datenschutzrechtlichen Bestimmungen erfolgen.
Auf Nachfrage teilte der Inhaber des Fitnessstudios dem TLfDI mit, dass er seit mehr als 2 Jahren eine Videoüberwachungsanlage mit zwei Kameras betreibe – eine im Eingangsbereich des Studios und eine im Büro. Der Inhaber legte dar, dass die Versicherung Schutzmaßnahmen gefordert hatte, nachdem zuvor wiederholt in das Fitnessstudio eingebrochen worden war. Andernfalls habe die Versicherung über eine Vertragskündigung nachdenken wollen. Daher habe

sich der Inhaber verpflichtet gesehen, das Fitnessstudio besser zu sichern.
Weiterhin gab der Inhaber an, dass die Kameraaufzeichnungen an einem sicheren Ort erfolgten und nicht während der Geschäftszeit angeschaut werden könnten. Die Daten würden acht Tage gespeichert, die Festplatte sei passwortgeschützt und müsse zur Einsichtnahme abgebaut und an einen Monitor angeschlossen werden. Zugriff hätten nur die Inhaber des Fitnessstudios, die Aufnahmen würden nicht an Dritte weitergegeben. Im Eingangsbereich des Studios, am Nebenausgang und an den Parkplätzen seien außerdem Hinweisschilder zu den Kameras angebracht. Einen Datenschutzbeauftragten gab es nach Angabe der Inhaber im Fitnessstudio nicht.
Nachdem der TLfDI um ergänzende Angaben zu den genauen Kameraeinstellungen und deren technischen Nutzung gebeten hatte, teilte der Inhaber des Fitnessstudios mit, dass er aufgrund der zeitaufwendigen Stellungnahmen die Videokameras abschalte. Der TLfDI forderte die Löschung der gesamten Videoaufnahmen und behielt sich eine Vor-Ort-Kontrolle vor.

Nach § 4 Abs. 1 BDSG bedarf die Erhebung von Videoaufnahmen einer gesetzlichen Ermächtigung oder persönlichen Einwilligung der bzw. des Betroffenen. Der TLfDI ist die zuständige Aufsichtsbehörde für den Datenschutz nach § 42 Abs. 1 Satz 1 Thüringer Datenschutzgesetz (ThürDSG). Er kontrolliert nach § 38 Abs. 1 Bundesdatenschutzgesetz (BDSG) die Einhaltung entsprechender datenschutzrechtlicher Bestimmungen.

7.4 Mit GPS immer ein Auge auf die Mitarbeiter?

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) bekam einen anonymen Hinweis darauf, dass ein Dienstleistungsunternehmen sämtliche Fahrzeuge des Fuhrparks mit GPS-Systemen aufgerüstet habe. Die Mitarbeiter befürchteten, über die Nutzung ihrer Dienstfahrzeuge rund um die Uhr überwacht zu werden. Der TLfDI wandte sich mit einem Auskunftsverlangen nach § 38 Abs. 3 Bundesdatenschutzgesetz (BDSG) an den Unternehmer und bat um nähere Informationen zur Ausstattung der Firmenwagen mit dem GPS-System, insbesondere zu den schriftlichen Festlegungen, der Speicherdauer und um Angabe des Zwecks der Datenverarbeitung.

Das Unternehmen, das einen externen Datenschutzbeauftragten bestellt hatte, teilte mit, man habe das GPS-System zunächst testweise erprobt und nutze es aktiv erst seit wenigen Tagen. Mit einem Informationsblatt war den Mitarbeitern zur Testphase nur die Tatsache des Einbaus von GPS-Technik zum Zweck der Schutzfunktion vor Diebstahl der Fahrzeuge mit teurer Messtechnik, zu Zwecken der Abrechnung mit Kunden und zur Optimierung des Einsatzes und der Tourenplanung zur Kenntnis gegeben worden. Gegen die Nutzung von GPS für diese Zwecke bestehen grundsätzlich keine datenschutzrechtlichen Bedenken, denn sie dienen der Wahrung berechtigter Interessen des Arbeitgebers nach § 28 Abs. 1 Nr. 2 BDSG, wobei das Interesse des Betroffenen in diesem Zusammenhang nicht überwiegt. Aus der Information ließ sich jedoch für die Betroffenen in keiner Weise ableiten, ob eine auf sie bezogene Auswertung oder eine Nutzung der erfassten Daten auch für arbeitsrechtliche Zwecke erfolgen sollte. In der zwischenzeitlich durch die Geschäftsleitung erstellten und mit dem Aktiveinsatz des GPS-Systems geltenden „Anweisung zur Nutzung GPS“ wurden die erforderlichen Festlegungen für die Verarbeitung der personenbezogenen Daten der Beschäftigten getroffen. Danach gelten geeignete Maßnahmen zum Schutz der Beschäftigten und namentlich restriktive Zugriffsbeschränkungen. Die Daten werden nach Erreichung der Zwecke, insbesondere die Abrechnung mit den Kunden, gelöscht. Es wurde festgelegt, dass eine permanente oder allgemeine Leistungs- und Verhaltenskontrolle nicht durchgeführt wird. Das System darf auch nicht in Fahrzeuge eingebaut werden, bei denen eine Privatnutzung für die Mitarbeiter zugelassen ist. Darüber hinaus erhalten die Mitarbeiter die Hinweise, um dem Gebot der Transparenz für die Betroffenen Rechnung zu tragen. Nachzulesen sind die Vorgaben auch unter den Hinweisen des LfD NRW https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Datenschutzrecht/Inhalt/Personalwesen/Inhalt/4_Ortungssysteme_und_Beschaeftigtendatenschutz/Ortungssysteme.pdf „Einsatz von Ortungssystemen und Beschäftigtendatenschutz“.

Nicht zu bemängeln war, dass auch Stichproben sowie bei begründetem Verdacht auf Pflichtverletzungen weitere Kontrollen vorgesehen werden. Dabei war vorgesehen, dass

der betriebliche Datenschutzbeauftragte nur jährlich hierüber informiert wird. Der TLfDI hielt es in diesem Zusammenhang jedoch für angebracht, den Beauftragten für den Datenschutz über Stichprobenkontrollen entweder vorab zu informieren oder ihn einzubinden, um die Einhaltung der datenschutzrechtlichen Festlegungen transparent machen zu können.
Die Geschäftsleitung nahm die Anregungen des TLfDI auf und passte die Arbeitsanweisung in dem Punkt an. Vor einer geplanten Kontrolle von Beschäftigten ist der Beauftragte für den Datenschutz nunmehr mit einem Vorlauf von mindestens zwei Werktagen zu informieren. Nach Abschluss der Kontrollmaßnahmen ist dem Beauftragten für den Datenschutz ein Protokoll der Durchführung und Ergebnisse auszuhändigen. Die Beschäftigten sind innerhalb von vierzehn Tagen über die durchgeführte Überprüfung und den Umfang der dabei erhobenen Daten zu informieren.

Der Einsatz von GPS ist zum Schutz bei Diebstahl des Fahrzeugs, zu Abrechnungszwecken gegenüber den Kunden und zur Optimierung des Einsatzes bzw. für die Routenplanung zulässig. Eine Dauerüberwachung von Mitarbeitern ist aufgrund des permanenten Kontrolldrucks unzulässig. Für die Fahrzeugführer muss erkennbar sein, ob und in welchem Umfang ihre personenbezogenen Daten verarbeitet oder genutzt werden. Stichproben oder Kontrollen bei konkretem Verdacht sind zulässig.

7.5 Was ist vor der Inbetriebnahme einer Kamerainstallation zu beachten?

Ein anonymes Schreiben erreichte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Darin wird von einem Betrieb berichtet, der seine Produktionshallen von innen und außen mit Videokameras überwacht. Die Mitarbeiter beschwerten sich zwar darüber, seien aber zu einer Einverständniserklärung genötigt worden. Seitens der Geschäftsführung werde die Videoüberwachung als versicherungstechnisch erforderlich gerechtfertigt. Zudem wurden dort elektronische Schlüssel eingeführt, welche auch für den Zugang zu den Umkleideräumen und den Toiletten zu benutzen sind. Mittels dieser Schlüssel könne laut Geschäftsleitung ausgelesen und gespeichert werden, welcher Mitarbeiter welche

Tür wie oft benutzt. Der Beschwerdeführer wandte sich deshalb mit der Bitte, die Rechtmäßigkeit der Überwachungsmaßnahme der Geschäftsleitung zu prüfen, an den TLfDI.
Aufgrund dieser Informationen beschloss der TLfDI, eine Kontrolle nach § 38 Abs. 1 Bundesdatenschutzgesetz (BDSG) bei dem Betrieb durchzuführen. Dabei stellte der TLfDI fest, dass an dem Standort über 20 Kameras betrieben wurden.
Nach § 4 Abs. 1 BDSG ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.
In Bereichen, die nicht-öffentlich zugänglich sind, sich aber Mitarbeiter aufhalten, ist die Videoüberwachung nach § 28 BDSG zu beurteilen. Dabei muss der Einsatz von Videotechnik zur Wahrung berechtigter Interessen des Arbeitsgebers erforderlich sein und schutzwürdige Interessen des Beschäftigten dürfen nicht überwiegen. So können ausnahmsweise Eigentümerinteressen des Arbeitgebers eine Videoüberwachung rechtfertigen, wenn Beschäftigte nicht im Fokus der Überwachung stehen und nicht permanent überwacht werden. In diesem Fall befanden sich aber einige Kameras an den Arbeitsplätzen der Beschäftigten, sodass sich diese hauptsächlich im Aufnahmebereich befanden und damit die Voraussetzungen für die Verarbeitung von Beschäftigtendaten nach § 32 BDSG hätten vorliegen müssen, was nicht der Fall war. Um die Eigentümerinteressen zu begründen, führte der Geschäftsführer an, dass es in den letzten zwei Jahren fünf Einbrüche in die Firma gegeben hätte.
Außerdem haben nach § 4f Abs. 1 BDSG nicht-öffentliche Stellen, die eine automatisierte Verarbeitung vornehmen, einen betrieblichen Datenschutzbeauftragten zu bestellen, es sei denn, es sind in der Regel höchstens neun Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt, § 4f Abs. 1 Satz 4 BDSG. Diese Ausnahme griff aber im vorliegenden Fall nicht, weil mit dem Betrieb der Videoüberwachung besondere Risiken für die Rechte und Freiheiten der Betroffenen verbunden sind, § 4f Abs. 1 Satz 6 BDSG i. V. m. § 4d Abs. 5 BDSG.
Einen betrieblichen Datenschutzbeauftragten gab es in dem Betrieb nicht. Zum Beauftragten für den Datenschutz darf nach § 4d Abs. 2 Satz 1 BDSG nur bestellt werden, wer die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzt. Neben der fachlichen Qualifikation ist daher wichtig, dass der betriebliche

Datenschutzbeauftragte aufgrund seiner persönlichen Eigenschaften sowie seines Verhaltens geeignet ist, seine Aufgaben ordnungsgemäß zu erfüllen. Die Firma bestellte die Leiterin der Datenverarbeitung als betriebliche Datenschutzbeauftragte. Diese kommt jedoch aufgrund ihres beruflichen Aufgabengebiets in einen Interessenkonflikt. Der TLfDI forderte daher, eine andere Person zum betrieblichen Datenschutzbeauftragten zu bestellen.

Außerdem ist gemäß § 4d Abs. 5 BDSG eine Vorabkontrolle erforderlich, wenn die automatisierte Verarbeitung besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweist. Nach der Gesetzesbegründung bestehen besondere Risiken, wenn Überwachungskameras „in größerer Zahl und zentral kontrolliert eingesetzt werden“ (BT-Drs. 14/5793, S. 62). Hiervon ist nach den bei der Kontrolle gemachten Feststellungen auszugehen. Diese Vorabkontrolle wäre durch den betrieblichen Datenschutzbeauftragten durchzuführen gewesen. Hier war zur Zeit der Inbetriebnahme kein Datenschutzbeauftragter bestellt, deshalb hätte dem TLfDI eine Meldung nach § 4d Abs. 1 BDSG gemacht werden müssen, auch dies ist nicht erfolgt.

Des Weiteren ist durch den betrieblichen Datenschutzbeauftragten eine Verfahrensübersicht, gemäß § 4g Abs. 2 und 2a BDSG, zu erstellen, die darin aufzunehmenden Angaben zählt der § 4e Satz 1 BDSG auf. Eine solche Verfahrensübersicht ist auch für das Schließsystem an zu fertigen. Um eine solche Verfahrensübersicht zu erstellen, wurden dem Betrieb vom TLfDI entsprechende Formulare zum Ausfüllen übersandt.

In diesen Formularen gab der Betrieb an, dass eine Löschung der Daten alle sieben Tage geschehe. Jedoch sind gemäß § 6b Abs. 5 BDSG die Daten der Videoüberwachung unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen. Das ist der Fall, wenn eine Gefahr nicht weiter abgewendet werden muss oder eine Beweissicherung nicht notwendig ist. Der TLfDI hielt im vorliegenden Fall eine Speicherdauer von 72 Stunden für angemessen, weil sich während des Wochenendes keine Personen im Betrieb aufhielten. Während der Betriebsferien könne die Speicherdauer erhöht werden.

Der TLfDI steht noch mit dem Betrieb in Kontakt, es wurden noch weitere und konkretere Auskünfte vom Betrieb verlangt, um die Zulässigkeit der Maßnahme der Videoüberwachung datenschutz-

rechtlich beurteilen zu können. Die Prüfung der Unterlagen war zum Ende des Berichtszeitraums noch nicht abgeschlossen.
Ein Bußgeldverfahren wird sich anschließen.

Nach § 4f Abs. 1 BDSG haben Betriebe einen Beauftragten für den Datenschutz zu bestellen. Durch diesen ist gemäß § 4d Abs. 5 BDSG eine Prüfung der automatischen Verarbeitung vor Beginn der Verarbeitung durchzuführen, wenn die Verarbeitung besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweist. Sollte kein betrieblicher Datenschutzbeauftragter bestellt worden sein, ist der Aufsichtsbehörde nach § 4d Abs. 1 BDSG eine Meldung zu machen.

7.6 Datenschutz in der Altenhilfe: Wer hat wo- wann- wem geholfen?

Im Januar 2015 wandte sich eine Einrichtung der Altenhilfe an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und bat um datenschutzrechtliche Informationen zum Umgang mit Aufbewahrungsfristen für Dienstpläne, Tourenpläne und Stundenabrechnungen insbesondere im Hinblick auf haftungsrechtliche Konsequenzen. In der Anfrage wurde dargelegt, dass sich in den einschlägigen Gesetzen für diese Dokumente keine speziellen Regelungen fänden.
Der TLfDI beantwortete die Anfragte folgendermaßen:
Tatsächlich gibt es hinsichtlich der Aufbewahrungsfristen für Dienstpläne, Tourenpläne und Stundenabrechnungen in den Einrichtungen der Altenhilfe keine speziellen gesetzlichen Regelungen. Da diese Dokumente jedoch allesamt personenbezogene Daten enthalten, ist hierfür das Bundesdatenschutzgesetz (BDSG) anwendbar. Nach § 20 Abs. 2 BDSG müssen personenbezogene Daten, die automatisiert verarbeitet oder in nicht automatisierten Dateien gespeichert sind, gelöscht werden, wenn ihre Speicherung unzulässig ist oder wenn die verantwortliche Stelle diese Daten für die Erledigung ihrer Aufgaben nicht mehr benötigt. Gemäß § 20 Abs. 3 BDSG ist in folgenden Fällen anstelle der Löschung eine Sperrung der Daten vorgesehen:

- wenn einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen,
- wenn Grund zur Annahme besteht, dass durch eine Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt werden,

- wenn eine Löschung wegen der besonderen Speicherart nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist.

Bei den angegebenen Dokumenten handelt es sich um nicht automatisierte Dateien. Grundsätzlich sind diese Dokumente zu löschen, wenn sie für den Zweck, für den sie erhoben wurden, nicht mehr benötigt werden. Stundenabrechnungen können solange aufbewahrt werden, bis die entsprechenden Beträge bezahlt sind. Auch danach ist eine Aufbewahrung möglich, um eventuell bestehende Meinungsverschiedenheiten zu klären, sofern Verjährungs- bzw. Rechtsmittelfristen noch nicht abgelaufen sind. Dies gilt ebenso für Dienst- und Tourenpläne. Dabei ist jedoch zu beachten, ob allgemeine gesetzliche Aufbewahrungsfristen nach dem Handels- oder Steuerrecht zu beachten sind und die Akten dann nach § 20 Abs. 3 BDSG gesperrt werden müssen. Nach § 3 Abs. 4 Nr. 4 BDSG bedeutet „Sperrung“, dass die gespeicherten personenbezogenen Daten entsprechend gekennzeichnet werden müssen, um ihre Weiterverarbeitung oder -nutzung einzuschränken. Es sind nach § 9 BDSG organisatorische Maßnahmen zu treffen, dass diese Akten dem Zugriff der Mitarbeiter im Rahmen der normalen Bearbeitung entzogen werden. Dies kann beispielsweise durch die Einlagerung in einen Archivraum geschehen, zu dem nur ein begrenzter Mitarbeiterkreis Zugang hat.

Hinsichtlich der Aufbewahrungsfristen für Dienstpläne, Tourenpläne und Stundenabrechnungen in der Altenhilfe gilt das Bundesdatenschutzgesetz (BDSG). Nach § 20 Abs. 2 BDSG müssen diese Daten gelöscht werden, wenn die verantwortliche Stelle die Daten zur ordnungsgemäßen Erledigung ihrer Aufgaben nicht mehr benötigt. In Einzelfällen können einer Löschung der Daten gesetzlich geregelte Aufbewahrungsfristen entgegenstehen (beispielsweise nach dem HGB). In diesen Fällen sind die Daten gemäß § 20 Abs. 3 BDSG zu sperren und in ein gesichertes Archiv zu überführen.

7.7 Bewerbungsverfahren abgeschlossen – Bewerberdaten gelöscht?

Ein Bürger beschwerte sich beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) darüber, dass ein Unternehmen der Bitte, seine personenbezogenen Daten zu löschen, nicht nachgekommen sei. Der Beschwerdeführer hatte sich bei dem Unternehmen beworben und ein Absageschreiben erhalten.

Daraufhin bat er das Unternehmen wiederholt per E-Mail darum, seine personenbezogenen Daten, auch die intern an den Geschäftsführer weitergeleiteten Daten und entsprechende Ausdrucke, zu löschen bzw. zu vernichten und ihm die Löschung zu bestätigen. Eine derartige Bestätigung hatte er aber nicht erhalten.

Der TLfDI ist gemäß § 42 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) in Verbindung mit § 38 Abs. 6 Bundesdatenschutzgesetz (BDSG) dazu ermächtigt, die Ausführung des BDSG und anderer Vorschriften über den Datenschutz zu kontrollieren (§ 38 Abs. 1 Satz 1 BDSG). Der Zweck dieser Kontrolle ist es, den Betroffenen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.

Nach § 24 Abs. 1 BDSG hat die verantwortliche Stelle dem Betroffenen auf Verlangen Auskunft über die zu seiner Person gespeicherten Daten zu erteilen. Personenbezogene Daten sind zu löschen, wenn die Voraussetzungen des § 35 Abs. 2 BDSG vorliegen. Unter anderem ist danach eine Löschung erforderlich, wenn die Kenntnis der Daten für die Erfüllung der Zwecke, für die sie erhoben wurden, nicht mehr erforderlich ist (Nummer 3).

In Ausübung seiner Kontrollfunktion bat der TLfDI das Unternehmen um eine detaillierte Auskunft zum vorgetragenen Sachverhalt des Beschwerdeführers gemäß § 38 Abs. 3 BDSG. Ergänzend wies der TLfDI in diesem Zusammenhang darauf hin, dass es sich auch bei den Anfragen des Beschwerdeführers um personenbezogene Daten handelt, die gegebenenfalls nach Bearbeitung seiner Beschwerde zu löschen sind. Sollten im Unternehmen schriftliche Festlegungen zum Umgang mit Bewerberdaten nach Abschluss des Verfahrens vorliegen, bat der TLfDI um Übersendung einer Kopie.

Auf seine Anfrage teilte das Unternehmen dem TLfDI mit, dass alle personenbezogenen Daten und Anfragen des Beschwerdeführers nach Abschluss des Bewerbungsverfahrens gelöscht worden seien. Das Unternehmen habe den Beschwerdeführer nicht über die Löschung informiert, da es von dessen Seite nach eigener Darlegung keine entsprechende Aufforderung erhalten habe. Der TLfDI informierte den Beschwerdeführer über die durch das Unternehmen bestätigte Löschung seiner gesamten personenbezogenen Daten und Anfragen und legte dar, dass insofern keine Anhaltspunkte für datenschutzrechtliche Verstöße bestehen. Da der Beschwerdeführer sich nicht mehr meldete, konnte der Vorgang abgeschlossen werden.

Nach § 24 Abs. 1 BDSG hat die verantwortliche Stelle dem Betroffenen auf Verlangen Auskunft über die zu seiner Person gespeicherten Daten zu erteilen. Personenbezogene Daten sind nach § 35 Abs. 2 Nr. 3 BDSG zu löschen, wenn die Kenntnis der Daten für die Erfüllung der Zwecke, für die sie erhoben wurden nicht mehr erforderlich ist. Dies ist in der Regel bei einer erfolglosen Bewerbung der Fall.

7.8 Wenn der Chef weiß, dass der Mitarbeiter zur Konkurrenz will

Im September 2015 wandte sich eine Arbeitnehmerin an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und bat um Auskunft, inwiefern ein fremdes Unternehmen, bei dem sie sich beworben hatte, dazu befugt ist, über diese Bewerbung das Unternehmen, bei dem sie angestellt ist, in Kenntnis zu setzen. Die Geschäftsführung des Unternehmens, bei dem die Beschwerdeführerin angestellt war, hatte ihr in einem persönlichen Gespräch vorgeworfen, auf der Suche nach einem neuen Tätigkeitsfeld als Immobilienverwalterin zu sein. Hierüber hatte sich der Geschäftsführer geärgert und der Arbeitnehmerin einen Aufhebungsvertrag angeboten. Auf Nachfrage bei dem Geschäftsführer, woher er die Informationen erhalten habe, erhielt die Beschwerdeführerin keine Auskunft. Bei diesem Gespräch waren zwei weitere Personen anwesend.

Die Beschwerdeführerin hatte sich bei einem Personaldienstleister auf eine ausgeschriebene Stelle beworben. Was sie nicht wusste: Diese Stelle war für die Firma, in der die Beschwerdeführerin aktuell beschäftigt war, ausgeschrieben. Die Beschwerdeführerin vermutete, dass der Personaldienstleister die entsprechenden Informationen weitergegeben hatte, zumal ihre Firma wohl ausschließlich mit diesem Personaldienstleister zusammenarbeitete. Die Beschwerdeführerin hatte nach eigener Aussage bereits einen Anwalt kontaktiert und dargelegt, dass der Personaldienstleister ihre Daten nicht an den Geschäftsführer hätte weitergeben dürfen.

Die Arbeitnehmerin erbat vom TLfDI Auskunft darüber, ob gegen ihren Arbeitgeber und den Personaldienstleister aus datenschutzrechtlichen Gründen etwas unternommen werden könne. Der TLfDI kam nach der datenschutzrechtlichen Prüfung zu dem Ergebnis, dass eine Datenverarbeitung im Auftrag nicht vorlag, weil die Arbeit-

nehmerin unmittelbar einen Vertrag mit dem Arbeitsvermittler geschlossen hatte. Gegenstand dieses Vertrages waren nicht Daten Dritter, sondern nur ihre personenbezogenen Daten. Auch zwischen dem Unternehmen und dem Arbeitsvermittler lag kein Auftragsdatenverhältnis vor, da die Stellenausschreibung ohne personenbezogene Daten erfolgte. Der TLfDI antwortete der Arbeitnehmerin folgendermaßen:

Der Vorgesetzte der Beschwerdeführerin hätte von vornherein die Informationen über anderweitige Bewerbungen gar nicht erheben dürfen. Nach § 32 Abs. 1 Bundesdatenschutzgesetz (BDSG) dürfen personenbezogene Daten über Beschäftigte für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, wenn dies für die Begründung des Beschäftigungsverhältnisses, für dessen Durchführung oder für dessen Beendigung erforderlich ist. Eine Notwendigkeit für die Durchführung oder Beendigung des Beschäftigungsverhältnisses lag nicht vor, da die Bewerbung bei einem anderen Unternehmen arbeitsrechtlich kein anerkannter Kündigungsgrund ist. Die Arbeitnehmerin hatte sich auf die vom Personaldienstleister ausgeschriebene Stelle beworben, da sie nicht wissen konnte, dass der Personaldienstleister die Stelle im Auftrag ihres derzeitigen Arbeitgebers ausgeschrieben hatte. Für den Personaldienstleister hingegen wäre es nicht erforderlich gewesen, die Geschäftsführer über den Veränderungswunsch ihrer Mitarbeiterin zu informieren, da die Begründung eines weiteren Arbeitsverhältnisses bei dem gleichen Unternehmen sicher nicht zur Debatte stand.

Nach § 34 BDSG hat ein Betroffener das Recht, von der verantwortlichen Stelle Auskunft über die zu seiner Person gespeicherten Daten zu verlangen, das heißt, die Beschwerdeführerin kann von ihrem Beschäftigungsunternehmen eine direkte Auskunft dazu fordern, woher der Geschäftsführer seine Informationen hatte. Allerdings ist es auch hier sehr wahrscheinlich, dass die Angabe über die anderweitige Bewerbung nirgendwo schriftlich dargelegt und eine Überprüfbarkeit somit nicht möglich ist.

Ein datenschutzrechtlich überprüfbarer Aspekt ist jedoch die Tatsache, dass das gesamte Gespräch zwischen der Arbeitnehmerin und der Geschäftsführung (Arbeitgeber) unter zwei Zeugen stattfand, insbesondere, wenn dabei der berufliche Veränderungswunsch der Beschwerdeführerin dargelegt wurde. Dieser Veränderungswunsch hätte den anwesenden Personen (Assistenz der Geschäftsführung und Personalmitarbeiter) nicht mitgeteilt werden dürfen.

Im Hinblick darauf bot der TLfDI der Beschwerdeführerin an, diesen Aspekt nach § 38 Bundesdatenschutzgesetz gegenüber dem Beschäftigungsunternehmen aufzugreifen. Da sich die Beschwerdeführerin nicht mehr meldete und dem TLfDI das Unternehmen nicht bekannt war, konnte er in der Angelegenheit nicht weiter tätig werden.

Gemäß § 32 Abs. 1 BDSG dürfen Unternehmen personenbezogene Daten über Beschäftigte nur für Zwecke des Beschäftigungsverhältnisses erheben, verarbeiten oder nutzen, wenn dies für die Begründung des Beschäftigungsverhältnisses, für dessen Durchführung oder Beendigung erforderlich ist. Daraus ergibt sich, dass ein Vorgesetzter oder Personalverantwortlicher keine Informationen darüber erheben darf ob oder inwiefern seine Mitarbeiter sich anderweitig bewerben, wenn die Mitarbeiter ihn hierüber nicht freiwillig in Kenntnis setzen. Eine anderweitige Bewerbung stellt keinen zulässigen Kündigungsgrund dar.

7.9 Betriebsärztliche Untersuchungen: keine automatische Schweigepflichtentbindung im Arbeitsvertrag

Nach § 8 Abs. 1 des Gesetzes über Betriebsärzte, Sicherheitsingenieure und andere Fachkräfte für Arbeitssicherheit (Arbeitssicherheitsgesetz – ASiG) haben auch Betriebsärzte die Regeln der ärztlichen Schweigepflicht zu beachten. Lediglich auf Wunsch des Arbeitnehmers ist nach § 3 Abs. 2 ASiG das Ergebnis arbeitsmedizinischer Untersuchungen mitzuteilen.
Die Arbeitnehmervertretung eines Thüringer Unternehmens wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), da das Unternehmen dazu übergegangen war, von seinen Arbeitnehmern im Arbeitsvertrag gleichzeitig die Unterschrift zur Entbindung der Betriebsärzte von ihrer Schweigepflicht gegenüber dem Arbeitgeber zu fordern.
Nach Prüfung der entsprechenden Klausel im Arbeitsvertrag teilte der TLfDI der Arbeitnehmervertretung mit, dass der Arbeitnehmer mit der Unterschrift unter den Arbeitsvertrag mit einer Klausel zur Schweigepflichtentbindung noch keine wirksame Schweigepflichtentbindung erklärt hätte. Die Einwilligung entsprach nämlich nicht der Form nach § 4a Abs. 1 Satz 1 BDSG, denn sie war nicht besonders hervorgehoben. Weiterhin kommt eine Entbindung von der Schweigepflicht des behandelnden Arztes nur dann in Frage,

soweit der Arbeitgeber ein berechtigtes Interesse an der entsprechenden Information darlegt. Praktisch müsste der/die Betroffene also vor einer Mitteilung des behandelnden Arztes an den Arbeitgeber im Einzelfall jeweils eine Schweigepflichtentbindung erteilen bzw. kann diese auch verweigern oder einschränken. Daher war aus Sicht des TLfDI die Befürchtung der Arbeitnehmervertretung unbegründet, dass auf der Grundlage des unterschriebenen Arbeitsvertrags vom Betriebsarzt dem Arbeitgeber der ärztlichen Schweigepflicht unterliegende Einzelheiten mitgeteilt werden könnten.

Eine pauschale Schweigepflichtentbindungserklärung in einem Arbeitsvertrag ist mit der Unterschrift des Vertrags keine wirksame Einwilligung zur Datenübermittlung zwischen Betriebsarzt und Arbeitgeber. Der Betriebsarzt muss vor jeder Datenübermittlung an den Arbeitgeber eine gesonderte zweckgebundene Schweigepflichtentbindung einholen.

7.10 Auskunftspflicht von Unternehmen

Grundsätzlich hat die verantwortliche Stelle nach § 34 Abs. 1 Bundesdatenschutzgesetz (BDSG) dem Betroffenen auf Verlangen Auskunft zu erteilen über die zu seiner Person gespeicherten Daten, deren Herkunft, den Empfänger, an den die Daten weitergegeben werden und den Zweck der Speicherung. Mit der Beantwortung von Auskunftsverlangen Betroffener machen es sich manche Unternehmen mitunter allerdings etwas zu leicht.
Ein Betroffener machte von seinem Auskunftsrecht gegenüber einem Thüringer Unternehmen Gebrauch und verlangte gleichzeitig – selbstverständlich nach Erteilung der Auskunft – die Löschung, ersatzweise Sperrung, seiner Daten. Daraufhin erhielt er die nicht näher differenzierte Auskunft, man habe die von ihm im Zusammenhang mit seiner Online-Bewerbung angegebenen Daten im internen System gespeichert, eine Weitergabe sei zum Zweck der Arbeitnehmerüberlassung erfolgt, seine Daten würden aus dem System gelöscht. Damit war der Betroffene nicht zufrieden und machte wegen unzureichender Auskunft eine Eingabe an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), weil er nämlich genau wusste, dass seine personenbezogenen Daten an ein Jobcenter in einem anderen Bundesland gelangt waren und diese Information in der Auskunft fehlte.

Der TLfDI wandte sich als Datenschutzaufsicht mit einem Auskunftsverlangen nach § 38 Abs. 3 BDSG an das Unternehmen und bat unter Berufung auf die einschlägigen Auskunftsregelungen um Stellungnahme. Das Unternehmen teilte daraufhin mit, es habe dem Betroffenen nun mit ergänzender Auskunft auch mitgeteilt, zu welchem Kunden zum Zweck der Arbeitnehmerüberlassung seine Bewerbungsunterlagen weitergegeben wurden. Ob das Unternehmen auch Daten an das Jobcenter in einem anderen Bundesland übermittelt hatte, blieb zunächst noch im Dunkeln. Eine Befragung des Jobcenters zur Aufklärung war für den TLfDI mangels Zuständigkeit nicht möglich. Dies wurde dem Beschwerdeführer mitgeteilt, der sich im Übrigen seinen Angaben zufolge auch bereits an die für das besagte Jobcenter zuständige Bundesbeauftragte für den Datenschutz und die Informationsfreiheit gewandt hatte.
Der Beschwerdeführer gab sich indes mit dem Ergebnis der Bemühungen des TLfDI nicht zufrieden, denn seiner Meinung nach war die ihm vom Unternehmen erteilte Auskunft falsch. Nach seinen Informationen, die er nun nachschob, habe es einen regelrechten Datenaustausch des Thüringer Unternehmens mit dem Jobcenter im anderen Bundesland gegeben.
Angefragt teilte daraufhin die Niederlassung des Thüringer Unternehmens in einem anderen Bundesland dem TLfDI zur Aufklärung mit, der Beschwerdeführer selbst habe gebeten, mit dem Sachbearbeiter des Jobcenters in Kontakt zu treten, um zu klären, weshalb ein Fahrkostenantrag abgelehnt worden sei. Hierfür habe er telefonisch die Kontaktdaten durchgegeben. Aufgrund der dargelegten eindeutigen Bitte war das Unternehmen auch nach Auffassung des TLfDI zu Recht davon ausgegangen, dass der Beschwerdeführer damit auch zum Anruf des Sachbearbeiters seine Einwilligung erteilt hatte.
Ob möglicherweise in dem Gespräch mit dem Sachbearbeiter beim Jobcenter weitere personenbezogene Daten zu dem Beschwerdeführer ausgetauscht wurden, wie der Beschwerdeführer vermutete, konnte aber vom TLfDI nicht weiter überprüft werden, da weder die Niederlassung des Unternehmens noch das Jobcenter seiner Datenschutzaufsicht unterlagen.

Die Auskunft an den Betroffenen nach § 34 BDSG über die zu seiner Person gespeicherten Daten umfasst auch Angaben zur Herkunft dieser Daten und die Empfänger, an die die Daten weitergegeben werden sowie den Zweck der Speicherung.

7.11 GPS für Arbeitgeber attraktiv – aber oft unzulässig

Im Berichtszeitraum erreichte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) eine Anfrage auf Auskunft zur Rechtmäßigkeit von Global-Positioning-System (GPS)-Ortung an Firmenfahrzeugen. Die Mitarbeiterin eines Sanitätshauses, die dort als Außenmitarbeiterin angestellt ist und ein Dienstfahrzeug nutzt, wünschte Auskunft zur datenschutzrechtlichen Zulässigkeit der GPS-Überwachung des Fahrzeuges.
Da sie den Sachverhalt nicht genauer schilderte, konnte der TLfDI nur eine allgemeine Auskunft erteilen. Durch den Einsatz von GPS-Technik werden Standortdaten erfasst, aufgrund derer Bewegungsprofile erstellt werden können. Es gilt daher, eine unzulässige Mitarbeiterüberwachung zu verhindern.
Grundsätzlich ist der Einsatz von GPS an Firmenfahrzeugen zulässig, sofern dies für eine Feststellung von Einsätzen, beispielsweise zu Abrechnungszwecken, erforderlich ist. In jedem Fall ist eine schriftliche Festlegung notwendig, die beinhaltet, in welchem Umfang und unter welchen Voraussetzungen Positionsdaten eines Fahrzeugs von einem bestimmten Personenkreis festgestellt und genutzt werden dürfen. Solche Festlegungen müssen aus Gründen der Transparenz dem Fahrzeugnutzer offengelegt und in einer Dienstvereinbarung abgestimmt werden.
Es kann zum Beispiel zulässig sein, GPS-Daten für steuerliche Zwecke auszudrucken. Diese Angaben ersetzen dann das früher übliche Fahrtenbuch. Dagegen wäre es unzulässig, wenn anhand der GPS-Positionsdaten ein lückenloses Bewegungsprofil ständig (auch für die Vergangenheit) einsehbar ist und damit eine vollständige Leistungs- und Verhaltenskontrolle vom Arbeitgeber ausgeübt wird.
Unzulässig sind auch Auswertungsfunktionalitäten, die nur einer persönlichen Überwachung von Beschäftigten dienen können, etwa Geschwindigkeitsaufzeichnungen und im Außendienst auch die Dauer von Fahrtunterbrechungen. Derartige Funktionen sind in der Regel technisch zu unterbinden, um die Mitarbeiter nicht einem permanenten Kontrolldruck auszusetzen.

Bei der Nutzung von GPS-Technik in einem Firmenwagen muss vom Arbeitgeber offengelegt werden, welche Daten für welchen Zweck erhoben werden, wie lange sie gespeichert werden dürfen und

zu welchem Zweck sie genutzt werden sollen. Ein lückenloses Bewegungsprofil ist wegen der damit verbundenen Leistungs- und Verhaltenskontrolle unzulässig.

7.12 Lehrlinge im Fokus – kein Videogaga bei Nichterkennbarkeit

Ein Thüringer Unternehmen richtete eine neue Lehrwerkstatt ein. Weil man Arbeitsunfälle befürchtete und der Lehrausbilder nicht ständig präsent sein konnte, wollte man auf die technischen Möglichkeiten zurückgreifen und eine Videoüberwachung installieren. Eine Verhaltenskontrolle der Lehrlinge wollte man natürlich nicht. Zugriff auf das Videomaterial sollte auch nur der Lehrausbilder und daneben auch der Empfang haben, denn Letzterer war ständig besetzt, um gegebenenfalls Hilfe zu organisieren. Der Betriebsrat des Unternehmens bat den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) um eine Einschätzung der Zulässigkeit des Vorhabens und um Beratung.

Der TLfDI verwies zunächst auf die „Orientierungshilfe Videoüberwachung durch nichtöffentliche Stellen“ in der die Datenschutzaufsichtsbehörden der Länder die Grundsätze für eine datenschutzkonforme Videoüberwachung festgelegt haben. Diese Orientierungshilfe ist auf der Homepage des TLfDI unter https://www.tlfdi.de/mam/tlfdi/gesetze/orientierungshilfen/oh-v -durch-nicht- ffentliche-stellen.pdf für jedermann abrufbar.

Die Videoüberwachung von Arbeitnehmern ist, wie in der Orientierungshilfe dargestellt, nur unter sehr engen Voraussetzungen möglich. Bei sicherheitsrelevanten Belangen müssen diese konkret dargelegt werden. Allein die Befürchtung, es könnte aufgrund von Unerfahrenheit zu Arbeitsunfällen kommen, reicht nicht aus. Auch ist eine Videoüberwachung nicht geeignet, Arbeitsunfälle zu verhindern. Darüber hinaus war auf den Fall bezogen nicht klar, weshalb Lehrausbilder und Empfang Zugriff auf die Bilder haben sollten. Alle Aspekte sind im Rahmen einer Vorabkontrolle nach § 4d Abs. 5 Bundesdatenschutzgesetz (BDSG) durch den für das Unternehmen bestellten Datenschutzbeauftragten zu prüfen.

Der Betriebsrat teilte dann mit, aufgrund der Hinweise und Beratung durch den TLfDI habe man sich dazu entschieden, ein reines Monitoring einzurichten, weil die hohe Verletzungsgefahr durch die Nutzung der Holzverarbeitungsmaschinen im Lehrbereich bestehe und man eine Nothilfe sicherstellen wolle. Die dort anwesenden Personen seien durch einen Schleier, den man über zu übertragende Bilder gelegt habe, nicht mehr erkennbar. Damit sei sichergestellt, dass sobald der Stillstand von Maschinen oder Personen erkennbar werde, Hilfe geleistet werden könne. Damit war das Vorhaben aus datenschutzrechtlicher Sicht als akzeptabel anzusehen.

Ein reines Monitoring eines Unternehmensbereiches, in dem hohe Verletzungsgefahr besteht, ist unter der Voraussetzung, dass Personen grundsätzlich nicht erkennbar sind und damit eine Leistungs- und Verhaltenskontrolle ausgeschlossen werden kann, aus datenschutzrechtlicher Sicht zulässig.

7.13 Anfrage zum Passwortschutz von Arbeitsplatzrechnern

Ein interessierter Bürger bat den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) um Informationen dazu, wie Passwörter an Arbeitsplatzrechnern möglichst datenschutzgerecht gestaltet werden können. Konkret wollte er wissen, inwiefern ein Arbeitgeber seinen Beschäftigten die Möglichkeit einräumen muss, das Passwort am Arbeitscomputer ändern zu können.
Hierzu teilte der TLfDI mit, dass der Arbeitgeber jedem seiner Beschäftigten die Möglichkeit einräumen muss, eine Passwortänderung an seinem Arbeitsrechner durchführen zu können. Nach § 9 Bundesdatenschutzgesetz (BDSG) hat die Stelle, die die personenbezogenen Daten erhebt, verarbeitet und nutzt (verantwortliche Stelle), die technischen und organisatorischen Maßnahmen zu treffen, die nötig sind, um die datenschutzrechtlichen Vorgaben einzuhalten. Es muss nach Nummer 2 der Anlage zu § 9 BDSG insbesondere verhindert werden, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle). Mitarbeiterpasswörter dürfen nur dem Mitarbeiter selbst bekannt sein und dürfen daher auch grundsätzlich nicht bei Dritten hinterlegt werden. Entscheidend ist, dass solche Passwörter dabei nicht an Dritte, also auch nicht an den Vorgesetzten, weitergegeben werden. Das Bundesamt für die Sicherheit

in der Informationstechnik (BSI) empfiehlt unter *https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02011.html* unter anderem folgende Maßnahmen zu Passwortgestaltung und -gebrauch:
Das Passwort darf nicht leicht zu erraten sein.

- Ein Passwort sollte aus Großbuchstaben, Kleinbuchstaben, Sonderzeichen und Zahlen bestehen. Es sollten mindestens zwei dieser Zeichenarten verwendet werden.
- Wenn für das Passwort alphanumerische Zeichen gewählt werden können, sollte es mindestens 8 Zeichen lang sein.
- Es muss getestet werden, wie viele Stellen des Passwortes vom Rechner wirklich überprüft werden.
- Voreingestellte Passwörter (z. B. des Herstellers bei Auslieferung von Systemen) müssen durch individuelle Passwörter ersetzt werden.
- Passwörter dürfen nicht auf programmierbaren Funktionstasten gespeichert werden.
- Passwörter müssen geheim gehalten werden und sollten nur dem Benutzer persönlich bekannt sein.
- Das Passwort sollte allenfalls für die Hinterlegung schriftlich fixiert werden, wobei es in diesem Fall in einem verschlossenen Umschlag sicher aufbewahrt werden muss.
- Das Passwort muss regelmäßig gewechselt werden, z. B. alle 90 Tage.
- Ein Passwortwechsel ist durchzuführen, wenn das Passwort unautorisierten Personen bekannt geworden ist oder der Verdacht besteht.
- Die Eingabe des Passwortes sollte unbeobachtet stattfinden.

Laut § 9 BDSG muss die Daten erhebende Stelle alle technischen und organisatorischen Maßnahmen treffen, um die datenschutzrechtlichen Vorgaben einzuhalten. Hierzu zählen auch die Zugangskontrolle und die Zugriffskontrolle sowie die Eingabekontrolle. Daher hat jeder Mitarbeiter das Recht, sein Passwort am Arbeitsplatzrechner zu ändern. Es sind die Vorgaben des BSI für die Vergabe von Passworten zu beachten.

7.14 Veröffentlichen von Bildern behinderter Menschen

Eine Behinderteneinrichtung fragte beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) an, ob es datenschutzrechtlich zulässig ist, wenn sie Bilder von der Tätigkeit der Behinderten in den Werkstätten auf den Fluren der Einrichtung aushängt und somit veröffentlicht. Auch wollten sie zur Freude der Behinderten die Bilder von Weihnachtsfeiern aushängen. Jedoch zweifelte die Behinderteneinrichtung, dass es überhaupt möglich ist, die Einwilligungserklärung von einigen einzuholen, da Zweifel hinsichtlich der Geschäftsfähigkeit bestünden.
Der TLfDI nahm hierzu wie folgt Stellung:
Das Recht am eigenen Bild ist ein Spezialfall des Rechts auf informationelle Selbstbestimmung und wird durch das Kunsturheberrechtsgesetz (KunstUrhG) geschützt. Gemäß § 22 Kunsturhebergesetz dürfen Bildnisse nur mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden. Nach dem Tode des Abgebildeten bedarf es bis zum Ablaufe von zehn Jahren der Einwilligung der Angehörigen des Abgebildeten. Angehörige im Sinne dieses Gesetzes sind der überlebende Ehegatte oder Lebenspartner und die Kinder des Abgebildeten und, wenn weder ein Ehegatte oder Lebenspartner noch Kinder vorhanden sind, die Eltern des Abgebildeten.
Ein Arbeitgeber darf Bilder seiner Beschäftigten, nach § 3 Abs. 11 Nr. 4 Bundesdatenschutzgesetz (BDSG) sind auch behinderte Menschen in anerkannten Werkstätten Beschäftigte, entsprechend der oben zitierten Bestimmung nur mit der Einwilligung verbreiten, etwa in Broschüren oder auf der Intra- oder Internetseite des Unternehmens (vgl. Auernhammer / Forst BDSG-Kommentar 4. Auflage, § 32 Rdnr. 68). Es muss also eine Einwilligung der Betroffenen vorliegen. Nach § 4a BDSG ist die Einwilligung nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Die Einwilligung ist eine rechtsgeschäftliche Erklärung bei der es darauf ankommt, ob die Betroffenen in der Lage sind, die Konsequenzen der Verwendung ihrer Daten zu überblicken und sich daher verbindlich dazu äußern zu können (Simitis in: Simitis, BDSG Kommentar, 8. Auflage, § 4a Rdnr. 20). Der TLfDI entnahm der Darstellung der Einrichtung, dass einige Beschäftigte nicht über die erforderliche Einsichtsfähigkeit verfügen, um die Tragweite ihrer Einwilligung zu überblicken. In diesem Fall fällt dem auch für arbeitsrechtliche

Sachverhalte bestellten Betreuer als gesetzlicher Vertretung die Aufgabe zu, über die Erteilung einer Einwilligung zu entscheiden.

Im Ergebnis muss vor einer Veröffentlichung von Aufnahmen, auf denen Arbeitnehmer einer Werkstätte zu erkennen sind, eine Einwilligung eingeholt werden. Bei geschäftsunfähigen Arbeitnehmern ist der Betreuer um die Einwilligung zu ersuchen. Bei geschäftsfähigen Arbeitnehmern ist eine in § 4a BDSG geregelte Einwilligung einzuholen, soweit dies möglich ist. Kann der Betroffene z. B. nicht schreiben, kann die Willensbekundung auch vom Betreuer schriftlich festgehalten werden. Ist die Behinderteneinrichtung der Auffassung, dass der Betroffene den Sinn der Einwilligung nicht erfasst, so muss sie sich zur Klärung über den Fortgang der Angelegenheit an dessen Betreuer wenden.

7.15 Beschäftigtendatenschutz – lückenlose Leistungs- und Verhaltenskontrolle unzulässig

Die Datenschutzbeauftragte eines Thüringer Unternehmens wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), und wollte wissen, welche personenbezogenen Daten eines Mitarbeiters (zum Beispiel zur Arbeitsleistung, Ausnutzung der Arbeitszeit, Effektivität der Arbeit, Motivation) innerhalb der Firma zum Beispiel an den Vorgesetzten oder die gesamte Abteilung weitergegeben werden können.
Da die Datenschutzbeauftragte keine weiteren Angaben machte, wies der TLfDI sie allgemein auf die Regelung des § 32 Bundesdatenschutzgesetz (BDSG) hin. Danach dürfen personenbezogene Daten eines Beschäftigten für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet und genutzt werden, wenn dies für die Entscheidung über die Begründung oder Durchführung oder Beendigung des Beschäftigtenverhältnisses erforderlich ist. Darüber hinaus kann der Betriebsrat interne Festlegungen treffen. Außerdem müssen gegebenenfalls tarifrechtliche Regelungen einbezogen werden. Allerdings gilt immer, dass eine lückenlose Leistungs- und Verhaltenskontrolle nicht zulässig ist. Insgesamt kommt es regelmäßig auf den jeweiligen Einzelfall an. Da die Anfrage ein sehr weites Feld des Beschäftigtendatenschutzes betraf, konnte sie ohne Kenntnis näherer Umstände nicht in der gebotenen Ausführlichkeit beantworten werden. Der Datenschutzbeauftragten wurde angeboten, konkrete Einzelfragen an

den TLfDI zu richten oder nähere Angaben zum Sachverhalt zu machen. Offenbar genügte die gegebene Auskunft, sodass die Datenschutzbeauftragte sich nicht wieder meldete.

Im Bereich des Beschäftigungsverhältnisses findet der § 32 BDSG Anwendung, grundsätzlich dürfen danach personenbezogene Daten für den Zweck des Beschäftigungsverhältnisses erhoben, verarbeitet und genutzt werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist.

7.16 Satte Rabatte contra Beschäftigtendatenschutz

Ein großer Discounter mit Filialen in Thüringen hatte im Herbst 2015 mit einer Rabattaktion geworben. Dabei konnte der Kunde selbst bestimmen, auf welche Artikel er welchen Rabatt geltend machen wollte. Hierfür wurden Werbebögen mit Aufklebern verteilt, damit die Kunden auf von ihnen ausgewählter Ware Rabatte bis zu 20 Prozent erhalten konnten. Pro Einkauf duften jedoch maximal zehn Coupons, so viele wie auf dem Werbebogen enthalten, eingelöst werden.
Da die Kassen offenbar die Anzahl der eingelösten Rabatte nicht automatisch erkennen konnten, wurden die Mitarbeiter belehrt, dass mit arbeitsrechtlichen Konsequenzen zu rechnen sei, falls die Einlösung der Rabatte nicht genau nach den Vorgaben für die Kunden erfolgte, nämlich pro Einkauf maximal nur einmal 20 Prozent, drei mal 10 Prozent und sechs mal 5 Prozent Rabatt.
Um der Androhung Taten folgen zu lassen, erfolgte eine mitarbeiterbezogene Auswertung der Kassenbons. Hatte ein Kunde mehr als die auf einem Werbebogen enthaltenen Rabatte bei einem Einkauf genutzt, wurde das Kassenpersonal unter Androhung empfindlicher Konsequenzen zur Stellungnahme aufgefordert. Über dieses Vorgehen erhielt der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) einen Hinweis. Nach Auffassung des Hinweisgebers musste eine Kassenauswertung in Form einer Leistungs- und Verhaltenskontrolle ausgeschlossen sein, denn nach seinen Informationen war dies in einer entsprechenden Betriebsanweisung so festgelegt. Der TLfDI wandte sich daher als Datenschutzaufsicht nach § 38 Abs. 1 Satz 1 Bundesdatenschutzgesetz

(BDSG) an die regionale Thüringer Vertriebsleitung und verlangte Auskunft.
Vom Hauptsitz des Unternehmens erklärte man, in der Revision der Zentrale habe man zunächst eine anonyme Statistik für alle Filialen gefertigt. Als man zu dem Ergebnis kam, dass auf einem Bon unerlaubter Weise mehrere 20 Prozent Gutscheine aus der Aktion eingelöst worden waren, sollten die Regionalrevisoren prüfen, welcher Kassenbediener den Bon erstellt hatte. Dabei habe man in erster Linie Fehlbedienungen frühzeitig erkennen und Nachschulungen der Mitarbeiter veranlassen wollen, was nach § 32 Abs. 1 Satz 1 BDSG, nämlich zur Durchführung des Beschäftigungsverhältnisses, möglich sei. Da diese Auswertung aber auch einen konkreten Verdacht auf Straftaten der Kassenmitarbeiter begründet hätte, sei § 32 Abs. 1 Satz 2 BDSG einschlägig. Danach können zur Aufdeckung von Straftaten personenbezogene Daten eines Beschäftigten dann erhoben, verarbeitet oder genutzt werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat, die Erhebung, Verarbeitung oder Nutzung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse des Beschäftigten an einem Ausschluss der Erhebung, Verarbeitung oder Nutzung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.
Ob diese Voraussetzungen vorlagen, war letztendlich nicht durch den TLfDI zu prüfen, da die gegenständlichen personenbezogenen Auswertungen nach Versicherung der Zentrale auf deren Veranlassung erstellt wurden. Nach § 3 Abs. 1 Nr. 2 Thüringer Verwaltungsverfahrensgesetz ist nämlich der TLfDI als Datenschutzaufsicht für Betriebsstätten nur dann zuständig, wenn diese in eigener Verantwortung die personenbezogene Auswertung durchgeführt haben. Mangels eigener Befugnis der Filiale war damit die Datenschutzaufsicht am Sitz der Zentrale für die weitere Prüfung zuständig. Die Angelegenheit wurde folglich an die zuständige Datenschutzaufsicht in einem anderen Bundesland am Sitz der Zentrale abgegeben. Diese teilte nach Prüfung mit, dass sie die Vorgehensweise für vertretbar hielt, da es den Arbeitgebern möglich sein muss, im Rahmen des § 32 Abs. 1 Satz 1 BDSG nach Belehrung die Einhaltung der Vorgaben zu kontrollieren.

Datenschutzrechtliche Vorschriften verhindern bei konkreten Anhaltspunkten für nicht vorgabenkonformes Vorgehen der Beschäftigten eine konkrete personenbezogene Überprüfung nicht. Folgt eine Betriebsstätte in Thüringen den bindenden Anforderungen der Zentrale in einem anderen Bundesland und hat die Betriebsstätte keine eigenen Handlungsspielräume bei der Verarbeitung von Beschäftigtendaten, ist die Datenschutzaufsicht am Sitz der Zentrale zuständig.

7.17 Arbeitszeitüberwachung: nur datenschutzgerecht, wenn ... – Videogaga 32

Im Berichtszeitraum wurde der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) anonym um datenschutzrechtliche Beratung gebeten. Der Sachverhalt wurde wie folgt geschildert. Ein in einer Notrufserviceleitstelle (NSL) eingesetzter Mitarbeiter überwache mitunter auch Techniker bei der Störungsbeseitigung. Das sei den Technikern bewusst, da sie in ihrem Arbeitsvertrag darüber informiert würden. Im Tätigkeitsbereich der Techniker befänden sich auch Automaten, die zum Schutz vor Vandalismus kameraüberwacht seien.
Im Störungsfall wenden sich die Kunden an die NSL, dann spult der NSL-Mitarbeiter vom Livebildmodus zur Zeit des Störungsauftritts zurück und gibt dem Techniker eine Information über den Vorfall. Nachdem die Störung behoben wurde, wird normalerweise der Techniker angerufen und es wird nachgefragt, wie lange er brauche, um die Störung zu beseitigen. Diese Zeit wird dann von der NSL in ein dafür vorhergesehenes Protokoll eingetragen. Wird dieser Vorgang aufgrund des Schichtsystems versäumt, kontrolliert der NSL-Mitarbeiter die Kameraaufnahmen zur Zeit der Störungsbeseitigung und trägt dann die festgestellte Zeit in das Protokoll ein.
Allerdings werde die Störung auch im Programm der Automaten angezeigt, dort seien auch die Zeit der Störung sowie die Zeit der Beseitigung der Störung ersichtlich. Ein Techniker fühlte sich durch diesen Ablauf überwacht und brachte seine Beschwerde dem Betriebsrat des Unternehmens vor.
Es wurde nun darum gebeten, die datenschutzrechtliche Zulässigkeit des zum Einsatz kommenden Verfahrens der Überprüfung der Arbeitszeit festzustellen.
Da die Anfrage sehr allgemein gehalten war und keine weiteren Informationen enthielt, fasste der TLfDI die in Betracht kommenden

datenschutzrechtlichen Aspekte wie folgt zusammen: Bevor eine Kamera installiert wird und eine Videoüberwachung stattfindet, sollte das Risiko für das informelle Selbstbestimmungsrecht der Betroffenen berücksichtigt und geprüft werden, ob eine Installation überhaupt nach einer Rechtsgrundlage zulässig ist. Nach § 6b BDSG ist die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) nur zulässig, soweit sie zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Bei der Videoüberwachung nicht-öffentlich zugänglicher Räume müssen die Voraussetzungen des § 28 BDSG beziehungsweise bei gezielter Erhebung von Beschäftigtendaten die Voraussetzungen des § 32 BDSG vorliegen. Genauere Anforderungen finden sich in der „Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen“ (www.tlfdi.de/mam/tlfdi/gesetze/orientierungshilfen/oh-v -durch-nicht- ffentliche-stellen.pdf). Ob eine Videoüberwachung in diesem Fall zulässig war, konnte durch den TLfDI aufgrund der geringen Informationen nicht bestimmt werden.

Der Arbeitnehmer ist durch den Arbeitsvertrag verpflichtet, in zutreffender Weise seine Arbeitszeit anzugeben. Ob dies im automatisierten Verfahren (elektronische Arbeitszeiterfassung) erfolgt oder ob hierzu handschriftliche Aufzeichnungen anzufertigen sind, kann der Unternehmer bestimmen. Die Erhebung und Verarbeitung der Arbeitsdaten ist nach § 32 Abs. 1 Satz 1 BDSG zulässig, sie sind für die Durchführung des Beschäftigtenverhältnisses erforderlich. Ein datenschutzrechtlicher Schutz dagegen, dass der Arbeitgeber im Falle von berechtigten Zweifeln an der Richtigkeit der Angabe der Arbeitszeiten eine Überprüfung vornimmt, besteht grundsätzlich nicht, denn der Arbeitgeber hat hierzu ein berechtigtes Interesse. Regelmäßig werden für solche Fälle Nachprüfungsmodalitäten festgelegt. Es kommt dabei auf die Art und Weise der Überprüfung an. Grundlage für eine rechtliche Prüfung dessen sind die entsprechenden Festlegungen des Arbeitgebers, die dem TLfDI nicht vorlagen. Der TLfDI bot an, die Angelegenheit zu prüfen und bat um nähere

Informationen. Der Anfragende bedankte sich für die Informationen und wünschte keine weitere Prüfung.

Ein Arbeitgeber kann eine Überprüfung der Arbeitszeiten vornehmen. Ob dies im automatisierten Verfahren (elektronische Arbeitszeiterfassung) erfolgt oder ob hierzu handschriftliche Aufzeichnungen anzufertigen sind, kann der Unternehmer bestimmen. Es besteht aus datenschutzrechtlichen Gründen grundsätzlich kein Schutz davor, dass, wenn der Arbeitgeber berechtigte Zweifel an der Richtigkeit der Angaben der Arbeitszeiten hegt, er eine Überprüfung dessen vornehmen kann. Regelmäßig werden für solche Fälle Nachprüfungsmodalitäten festgelegt, die einzuhalten sind.

7.18 Leistungsdruck durch GPS

Ein Mitarbeiter eines Thüringer Unternehmens wandte sich ohne konkrete Benennung seines Arbeitgebers an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), um Auskunft einzuholen, ob es zulässig ist, wenn der Vorgesetzte in die Firmenfahrzeuge ohne Wissen des Mitarbeiters Global-Positioning-System (GPS)-Technik einbauen lässt. Das GPS übermittelt Standortdaten, durch die Bewegungsprofile erstellt werden können. Zweck des GPS war es, nach Ansicht des Beschwerdeführers, den Mitarbeiter zu überwachen und ihn gegebenenfalls unter Druck zu setzen, falls er zu langsam arbeite.
Der TLfDI wies den Mitarbeiter auf die Regelung des § 32 Bundesdatenschutzgesetz (BDSG) hin. Danach ist die Verarbeitung von personenbezogenen Daten eines Beschäftigten nur zulässig, soweit dies zur Begründung, Durchführung oder Beendigung des Beschäftigungsverhältnisses erforderlich ist. GPS-Nutzung ist danach nicht generell unzulässig. Durchaus können zulässige Zwecke zur Erhebung und Verarbeitung personenbezogener Daten mittels GPS vorliegen, beispielsweise die Führung eines Fahrtenbuchs für steuerliche Zwecke oder die Erhebung von Positionsdaten für besondere Einsatzzwecke in Eilfällen. Dies setzt jedoch voraus, dass die Beschäftigten entsprechend aufgeklärt sind. Da es sich um eine automatisierte Verarbeitung von personenbezogenen Daten handelt, ist in der Regel eine Vorabprüfung unter Abwägung der schutzwürdigen Interessen der Betroffenen durchzuführen. Sofern ein Betriebsrat vorhanden ist, sind die schriftlichen Festlegungen Grundlage für eine

entsprechende Betriebsvereinbarung und Betriebsanweisung. Ein lückenloses Bewegungsprofil der Mitarbeiter ist aber wegen der damit verbundenen Leistungs- und Verhaltenskontrolle unzulässig. Von dem Angebot, sich zu melden, damit genauere Prüfungen vorgenommen werden können, machte der Beschwerdeführer keinen Gebrauch.

Sollten Mitarbeiter wahrnehmen, dass ihr Vorgesetzter heimlich Daten von ihnen durch GPS erhebt, um die Mitarbeiter auf diese Weise zu kontrollieren, können sich diese an den TLfDI wenden. Der TLfDI kann als Datenschutzaufsicht nach § 38 BDSG den Einsatz von GPS in Unternehmen mit Sitz in Thüringen konkret überprüfen. Grundsätzlich ist es zulässig, GPS-Technik in Firmenwagen zu installieren. Jedoch ist ein lückenloses Bewegungsprofil wegen der damit verbundenen Leistungs- und Verhaltenskontrolle unzulässig.

7.19 Gab ein Arbeitsvermittler die Bewerbungsunterlagen seiner Mitarbeiterin ungefragt weiter?

Die Beschäftigte bei einem privaten Arbeitsvermittler beschwerte sich beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), weil sie davon ausging, dass der Arbeitgeber, nachdem er das Arbeitsverhältnis in der Probezeit gekündigt hatte, sie ungefragt weitervermitteln wollte. Sie wurde nämlich von einem Unternehmen für Personaldienstleistungen angeschrieben, sie solle sich doch bitte zu ihrer Bewerbung einmal melden. Die Unterlagen seien dem Unternehmen von dem privaten Arbeitsvermittler übersandt worden. Die Betroffene war sehr erstaunt, zumal sie sich aufgrund ihres Arbeitsverhältnisses nicht anderweitig beworben hatte.
Auf die Nachfrage des TLfDI teilte der private Arbeitsvermittler mit, er habe die Personalunterlagen der bei ihm beschäftigten Beschwerdeführerin keineswegs weitergeleitet. Vor der Beschäftigung in seinem Unternehmen habe er jedoch tatsächlich die von der Beschwerdeführerin eingereichten Bewerbungsunterlagen auf eine bestimmte ausgeschriebene Stelle zur Personalvermittlung weitergereicht. Dies sei damals telefonisch in einem Interview mit der Beschwerdeführerin vor der Beschäftigung in seinem Unternehmen so vereinbart worden, denn die Betroffene habe dringend Arbeit gesucht. Das

Personaldienstleistungsunternehmen habe aber noch vor der Beschäftigung der Betroffenen dem Arbeitsvermittler per E-Mail mitgeteilt, dass die Unterlagen dort nicht weiter berücksichtigt werden könnten. Weshalb just nach der Kündigung des Arbeitsverhältnisses das Personaldienstleistungsunternehmen auf den Plan trat, war nicht zu klären.
Die Beschwerdeführerin bestritt vehement, jemals eine Einwilligung zur Weiterleitung ihrer Bewerbungsunterlagen erteilt zu haben. Sie vertrat die Auffassung, die Beweislast für das Vorliegen ihrer Einwilligung treffe ihren ehemaligen Arbeitgeber und dieser könne die erforderliche schriftliche Einwilligung nicht vorlegen, weil es keine gäbe. Sie äußerte ihr Unverständnis, dass man ihr das offenbar nicht glaube.
Eine Einwilligungserklärung ist zwar grundsätzlich schriftlich abzugeben, das Gesetz sieht aber vor, dass wegen besonderer Umstände eine andere Form angemessen sein kann (§ 4a Abs. 1 Satz 3 Bundesdatenschutzgesetz (BDSG). Aufgrund der Schilderung des Arbeitgebers, in dem telefonischen Interview sei die Beschwerdeführerin vor ihrer Einstellung in seinem Unternehmen mit der Weitergabe der Unterlagen einverstanden gewesen, weil sie dringend Arbeit gesucht hatte, hat der TLfDI ausnahmsweise eine mündliche Einwilligung aufgrund der geschilderten Eilbedürftigkeit für angemessen angesehen. Der TLfDI wies die Beschwerdeführerin darauf hin, dass es nicht darum gehe, der einen oder anderen Seite mehr oder weniger zu glauben. Um weitergehende Schritte - also ein Bußgeldverfahren - einzuleiten, bedürfe es der Feststellung eines datenschutzrechtlichen Verstoßes. Den Darlegungen des Arbeitgebers waren jedoch keine ausreichenden Anhaltspunkte dafür zu entnehmen, dass die dem Arbeitsvermittler zugeleiteten Bewerbungsunterlagen unter Verstoß gegen datenschutzrechtliche Vorschriften der genannten Personaldienstleistungsfirma übersandt wurden.

Die Einwilligung zur Weitergabe von Bewerbungsunterlagen bedarf grundsätzlich der Schriftform, es sei denn, dass wegen besonderer Umstände eine andere Form angemessen sein kann. Ein besonderer Umstand kann unter Umständen auch in einer eiligen Angelegenheit begründet sein. Um Missverständnisse zu vermeiden, sollte die mündlich erteilte Einwilligung nochmals schriftlich bestätigt werden.

7.20 Kündigung wegen Bewerbung in einem anderen Unternehmen?

Eine Beschäftigte in einem Handwerksbetrieb wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) mit dem Vorbringen, ihr sei gekündigt worden, weil sie sich bei einem anderen Unternehmen beworben hatte. Die Chefin habe auch den anderen Kollegen ihre Bewerbung zur Kenntnis gegeben.
Damit waren Verstöße gegen datenschutzrechtliche Vorschriften sowohl seitens des Unternehmens, bei dem sich die Betroffene beworben hatte als auch seitens des Beschäftigungsunternehmens möglich. Die Bewerbungsunterlagen enthielten personenbezogene Daten der Beschäftigten, die von dem Unternehmen, bei dem sie sich beworben hatte, nur für Zwecke der Begründung eines Beschäftigungsverhältnisses erhoben, verarbeitet und genutzt werden durften (§ 32 Abs. 1 Bundesdatenschutzgesetz – BDSG). Anderen Unternehmen oder einem früheren Arbeitgeber die Unterlagen weiterzuleiten ist unzulässig, da es hierfür keine gesetzliche Grundlage gibt und im vorliegenden Fall auch nicht von einer erteilten Einwilligung der Betroffenen ausgegangen werden kann, § 4 Abs. 1 BDSG. Für das beschäftigende Unternehmen besteht ebenfalls keine Befugnis, die personenbezogenen Daten einer Beschäftigten anderen Mitarbeitern zur Kenntnis geben.
Auf das Auskunftsersuchen des TLfDI nach § 38 BDSG teilte das Beschäftigungsunternehmen mit, die ganzen Vorwürfe seien falsch, lückenhaft und dienten nur der Stimmungsmache. Die Bewerbungsunterlagen hätten sich eines Tages unvermittelt im Briefkasten der Geschäftsräume befunden. Es sei nicht nachvollziehbar, wer sie dort eingelegt hatte. Die Unterlagen seien inzwischen vernichtet, ohne dass sie anderen Beschäftigten zur Kenntnis gegeben worden waren. Dies war ausweislich des zugeleiteten Protokolls auch im arbeitsgerichtlichen Verfahren so vorgetragen worden.
Hat sich die Angelegenheit wie von dem Unternehmen vorgetragen abgespielt, ist kein Datenschutzverstoß durch dieses Unternehmen feststellbar. Werden einem Unternehmen ohne dessen Zutun Bewerbungsunterlagen, die an ein anderes Unternehmen gesandt wurden, zugeleitet und nutzt es diese nicht für andere Zwecke, ist kein Datenschutzverstoß erkennbar. Zeugen dafür, dass den anderen Beschäf-

tigten die Bewerbungsunterlagen zur Kenntnis gegeben wurden, hat die Beschwerdeführerin nicht benannt.

Bewerbungsunterlagen dürfen ohne Einwilligung des Bewerbers nicht an andere Stellen weitergegeben werden. Erhält ein Unternehmen ohne eigenes Zutun Kenntnis davon, dass sich ein Mitarbeiter anderweitig beworben hat, besteht keine Rechtsgrundlage dafür, diese zur Kenntnis gelangten personenbezogenen Daten des Mitarbeiters zu nutzen.

7.21 Jobsuche und alle wissen es

Eine Zeitarbeitsfirma hatte eine attraktive Stelle bei einem konkreten Unternehmen ausgeschrieben, für die sich der spätere Beschwerdeführer sehr interessierte. Also schickte er seine vollständigen Bewerbungsunterlagen, zugeschnitten auf die ausgeschriebene Stelle, an die Zeitarbeitsfirma. Kurz darauf wurde er von einem Mitarbeiter der Zeitarbeitsfirma telefonisch kontaktiert und um weitere Angaben gebeten. Dabei nahm er an, dass sich die geforderten Angaben auf die Stelle bezogen, für die er sich interessierte. Wiederum kurze Zeit später wurde er von Dritten darauf hingewiesen, dass seine personenbezogenen Daten in einem sogenannten Bewerbungsnewsletter sämtlichen Firmenkunden der Zeitarbeitsfirma zugänglich gemacht wurden. Dies umfasste neben seinem Foto, den Geburts- und Adressdaten auch die Angabe aller bisherigen Arbeitgeber inklusive der Austrittsgründe. Damit nicht genug, denn überraschenderweise besaß er nach den Angaben der Zeitarbeitsfirma besondere Fähigkeiten, von denen er bislang gar nichts gewusst hatte. Da die öffentliche Anbietung nun gar nicht seiner Intention entsprach, zog der Beschwerdeführer eiligst seine Bewerbung zurück und bat um Löschung seiner Daten, was ihm auch unverzüglich bestätigt wurde. Dennoch wurde er daraufhin weiterhin per E-Mail zum Zweck der Vermittlung angeschrieben, was eigentlich nicht möglich gewesen wäre, wenn seine Daten tatsächlich gelöscht worden wären.
Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit, an den sich der Betroffene nun wandte, richtete ein Auskunftsverlangen nach § 38 Abs. 3 Bundesdatenschutzgesetz an die in Thüringen ansässige Betriebsstätte der überregionalen Zeitarbeitsfirma. Das Unternehmen teilte mit, üblicherweise erhalte ein Bewerber eine sogenannte Bewerberkarte, die einen Abschnitt „Da-

tenschutzerklärung“ enthalte, in dem darauf hingewiesen werde, dass die Daten auch anderen potenziellenen Einsatzbetrieben gegeben werden können. Ist der Bewerber damit einverstanden, muss er diesen Passus anhaken und unterschreiben. Der Beschwerdeführer habe zwar die Karten noch nicht ausgefüllt, jedoch habe es eine mündliche Rücksprache gegeben, dass das Profil anderen Kunden vorgestellt werden dürfe. Man habe das Profil nicht gelöscht, sondern nur gesperrt, weil es möglich sei, dass ein Bewerber noch Ansprüche auf Schadensersatz oder Entschädigung nach dem Allgemeinen Gleichbehandlungsgesetz geltend machen könnte. Dafür benötige man die Daten gegebenenfalls noch. Systemseitig sei an die fehlende Datenschutzerklärung erinnert worden, um bei Nichtvorlage die notwendige Löschung vornehmen zu können. Das Zeitarbeitsunternehmen wurde gefragt, ob es eine Dokumentation zu der mündlichen Rücksprache mit dem Bewerber gegeben habe. Das Unternehmen teilte mit, dass die mündliche Absprache im EDV-System dokumentiert worden sei. Aufgrund dieser Dokumentation werde eine systemseitig automatisierte Erinnerung an den Bewerber erzeugt, wenn zwischenzeitlich keine unterzeichnete Datenschutzerklärung eingegangen sei, um der zuvor mündlich getroffenen Vereinbarung eine schriftliche Grundlage zu geben. Der Beschwerdeführer habe diese Benachrichtigung erhalten, was zu Irritationen bei ihm geführt habe.

Nach § 4a Bundesdatenschutzgesetz (BDSG) bedarf die Einwilligung der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Das BDSG sieht danach nicht vor, dass die Einwilligung notwendigerweise schriftlich abgegeben wird. Wird eine andere Form gewählt, insbesondere die mündliche Einwilligung, gibt es, wie auch der vorliegende Fall zeigt, in der Praxis immer wieder Nachweisprobleme. Zwar schließt das Gesetz die Möglichkeit der mündlichen Einwilligung nicht aus, sie sollte aber wegen der mit ihr verbundenen Nachweisprobleme auf wenige Ausnahmefälle beschränkt werden. Hier hatte die möglicherweise mündlich erteilte Einwilligung zur Folge, dass andere Arbeitgeber erfuhren, dass eine bestimmte Person eine neue Arbeitsstelle sucht. Dabei ist es nicht ausgeschlossen, dass sich unter diesen Unternehmen auch der derzeitige Arbeitgeber eines Bewerbers befindet. Da mit einer derartigen Veröffentlichung unter Umständen weitreichende Folgen für den Betroffenen verbunden sind, hält der TLfDI in diesem Fall eine schriftliche Einwilligung für zwingend erforderlich. Dies hat er dem Zeitarbeitsunternehmen mitgeteilt. Das Zeitarbeitsunternehmen

teilte mit, dies sei im Nachhinein auch versucht worden, denn eine mündliche Absprache werde im EDV-System dokumentiert. Aufgrund dieser Dokumentation werde eine automatisierte Erinnerung an den Bewerber erzeugt, wenn keine unterzeichnete Datenschutzerklärung vorliege. Leider erfolgte diese automatische Ansprache erst, nachdem die Bewerbung bereits zurückgezogen worden war.
Wenn nach einem Löschbegehren der Bewerber im System gesperrt wird, ist unter Berücksichtigung der von der Zeitarbeitsfirma angeführten Gründe dagegen grundsätzlich nichts einzuwenden. Allerdings muss, wenn ein Bewerber seine Bewerbung zurückzieht, davon abgesehen werden, ihm weitere Angebote zukommen zu lassen. Die datenschutzrechtliche Prüfung hinsichtlich des Inhalts der veröffentlichten Bewerbung ist noch nicht abgeschlossen.

Vorsicht bei telefonischen Einwilligungen, die erhebliche datenschutzrechtliche Eingriffe nach sich ziehen. Insbesondere bei Eilbedürftigkeit kann man unter Umständen von einer Schriftlichkeit der Einwilligungserklärung absehen. Wenn mit einer Einwilligung weitreichende Folgen für den Betroffenen verbunden sind, sollte immer eine schriftlich erteilte Einwilligung vorliegen.

7.22 Kontrolle in einem Logistik-Unternehmen

Im Berichtszeitraum kontrollierte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) ein Logistikunternehmen. Ihm war zur Kenntnis gekommen, dass Leistungsdaten einzelner Arbeitnehmer aus den Logistikdaten zur Leistungskontrolle verwendet worden sein sollen.
Aufgrund der Komplexität der Datenverarbeitung dauerte die Kontrolle einige Zeit an. Das Unternehmen war äußerst kooperativ und unterstützte den TLfDI in all seinen Tätigkeiten vor Ort. So konnte der gesamte Logistikprozess begutachtet und Datenflüsse konnten nachvollzogen werden.
Im Ergebnis konnte festgestellt werden, dass der initiale Vorwurf wohl das Fehlverhalten einer einzelnen Führungskraft im unteren Managementbereich betraf und nicht systematisch Logistikdaten zur Leistungsüberwachung von Arbeitnehmern durch das Logistikunternehmen ausgewertet wurden.

Dennoch hat der TLfDI im Laufe seiner Kontrolle Mängel in der Datenverarbeitung aufgedeckt, die aber vom Unternehmen so schnell als möglich beseitigt wurden.
Im ganz überwiegenden Teil begründeten sich diese in der technischen Umsetzung von Datenflüssen und -verarbeitung im Logistikprozess. Bei jedem Logistikprozess, an dem Menschen beteiligt sind, entstehen personenbezogene Daten. Sobald zum Beispiel ein Arbeitnehmer einen Gegenstand in das Warensystem einordnet, wird dieser Umstand im System vermerkt. Während dies vordergründig ein systembezogenes Datum ist, lässt sich daraus natürlich auch eine Aussage über die Tätigkeit des Arbeitnehmers ableiten. Wenn dessen Tätigkeit darin besteht, regelmäßig Waren in die Warenwirtschaft einzupflegen, lässt sich hieraus eine sehr detaillierte Aussage über die Leistung des einzelnen Arbeitnehmers treffen. Insbesondere, weil man diese Daten mit denen anderer Arbeitnehmer, die eine vergleichbare Tätigkeit ausüben, vergleichen kann.
Nach § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG) ist das Erheben, Verarbeiten oder Nutzen von personenbezogenen Daten nur dann erlaubt, wenn ein Gesetz diese Verarbeitung erlaubt oder anordnet oder der Betroffene in die Verarbeitung eingewilligt hat.
Einwilligungen lagen hier nicht vor. Da es sich um Daten über Arbeitnehmer handelt, ist einzige einschlägige Norm, die einen Umgang mit diesen Daten erlaubt, § 32 Abs. 1 Satz 1 BDSG. Hier hat der Gesetzgeber abschließend geregelt, wann eine Verarbeitung dieser Daten erlaubt ist. Dies ist dann der Fall, wenn der Umgang, also die Erhebung, Verarbeitung oder Nutzung für die Begründung, Durchführung oder Beendigung des Arbeitsverhältnisses erforderlich ist. Eine darüber hinausgehende Berechtigung, Arbeitnehmerdaten zu verarbeiten besteht nur in Fällen von begründeten, dokumentierten Verdachtsfällen zu Straftaten gegenüber einzelnen Arbeitnehmern oder einer eng begrenzten Gruppe an Arbeitnehmern, § 32 Abs. 1 Satz 2 BDSG.
Die von oben erwähnter Führungskraft vorgenommene Leistungskontrolle war von der Verarbeitungsbefugnis, die sich aus § 32 Abs. 1 Satz 1 BDSG ergibt, nicht gedeckt, da sie für die Durchführung des Arbeitsverhältnisses nicht erforderlich war. Die Kontrolle über die Tätigkeit der Arbeitnehmer und deren Recht auf informationelle Selbstbestimmung sind zwei Interessen, die bei der Bewertung der Erforderlichkeit der Datenverarbeitung gegeneinander abgewogen werden müssen. Dabei ist auf der einen Seite das Interesse und

auch das Recht des Arbeitgebers zu berücksichtigen, die Leistung des einzelnen Arbeitnehmers bewerten zu können. Dies ist auch selbstverständlich, da es sich bei der konkreten Arbeitsleistung des Arbeitnehmers um die Primärleistung aus seinem Vertrag handelt. Wird diese nicht oder nur teilweise erfüllt, kann dies dazu führen, dass der Arbeitnehmer seinen Anspruch auf das Arbeitsentgelt ganz oder teilweise verliert. Der Arbeitgeber muss in der Lage sein, dieses Gegenseitigkeitsverhältnis von Ansprüchen prüfen zu können.
Andererseits darf, auch um dem informationellen Selbstbestimmungsrecht des Arbeitnehmers gerecht zu werden, kein „gläserner Arbeitnehmer“ entstehen. Diese Abwägung ist im Einzelfall sehr schwierig. Vorliegend war dies jedoch einfach, da jedenfalls dann die Interessen des Arbeitnehmers überwiegen, wenn der Arbeitgeber – oder wie hier eine einzelne Person – ein annähernd lückenloses Tätigkeits- und Bewegungsprofil des Arbeitnehmers erstellt.
Nun kann das einzelne Fehlverhalten einer Person nicht in jedem Fall auch dem Logistikunternehmen zugeordnet werden, so war dies auch hier. Die einzelne Person selber war leider nicht mehr ermittelbar, weswegen der TLfDI gegen diese nicht vorgehen konnte.
Allerdings muss ein Unternehmen seine Prozesse so gestalten, dass solch ein Fehlverhalten nicht möglich ist. Der beste Weg hierfür ist, den Zugriff von Daten so zu beschränken, dass jeder nur den Teil zu sehen bekommt, den er braucht, und die Daten, sobald ein Personenbezug nicht mehr notwendig ist, zu anonymisieren, also den Personenbezug zu entfernen. Diesen Weg hat das Unternehmen auf Anraten des TLfDI eingeschlagen und sein Logistiksystem insoweit überarbeitet.

Auch wenn die Verarbeitung von (auch) personenbezogenen Daten nicht der primäre Zweck einer Datenverarbeitung ist, müssen dabei das Datenschutzrecht und seine Vorschriften beachtet werden. Auch sind solche Systeme immer so zu gestalten, dass ein Zugriff auf Daten nur durch Personen erfolgt, die diese unbedingt benötigen und zu diesem Zweck auch verwenden dürfen. Werden Daten längerfristig benötigt, um Verarbeitungsschritte zu optimieren oder Fehler zu identifizieren, sind die Daten so früh wie möglich vom Personenbezug zu befreien.



Stressed Spam - © alphaspirit / Fotolia.com

8 Werbung

8.1 Beschwerde über aufdringliche Telefonwerbung

Mit einer Beschwerde über aufdringliche Telefonwerbung wandte sich ein Bürger an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und bat darum, ihn dabei zu unterstützen, dass er von solchen dreisten und anhaltenden Werbeanrufen zukünftig verschont bleibt. Da sich der Beschwerdeführer die Telefonnummer des Anschlusses, von dem aus die Werbeanrufe erfolgten, notiert hatte, war es dem TLfDI möglich, bei der Bundesnetzagentur anzufragen, welcher Netzbetreiber für den entsprechenden Anschluss verantwortlich ist. Die Bundesnetzagentur erteilte daraufhin diese Auskunft. Eine weitergehende Recherche zur

Ortsnetzrufnummer ist über die Bundesnetzagentur jedoch nicht möglich, da diese über derartige Informationen nicht selbst verfügt. Die Bundesnetzagentur vergibt lediglich sog. Rufnummernblöcke an Netzbetreiber, die daraufhin die einzelnen Rufnummern eigenverantwortlich an die Endkunden ausgeben. Diesen Auskunftsanspruch gegen die Bundesnetzagentur, der in § 66i Abs. 1 des Telekommunikationsgesetzes (TKG) enthalten ist, kann jeder, der ein berechtigtes Interesse hat, geltend machen und in Textform von der Bundesnetzagentur Auskunft über den Namen und die ladungsfähige Anschrift desjenigen verlangen, der eine Nummer von der Bundesnetzagentur zugeteilt bekommen hat.
§ 66i Abs. 3 TKG enthält auch einen Auskunftsanspruch gegen Dritte. Hiernach kann jeder, der ein berechtigtes Interesse daran hat, von demjenigen, dem von der Bundesnetzagentur Rufnummern zum Beispiel für Massenverkehrsdienste (0)137, Neuartige Dienste (0)12 oder Kurzwahldienste zugeteilt sind, unentgeltlich Auskunft über den Namen und die ladungsfähige Anschrift desjenigen verlangen, der über eine dieser Rufnummern Dienstleistungen anbietet, oder die Mitteilung verlangen, an wen die Rufnummer gemäß § 46 TKG übertragen wurde. Bei Kurzwahlnummern, die nicht von der Bundesnetzagentur zugeteilt wurden, besteht der Anspruch sogar gegenüber demjenigen, in dessen Netz die Kurzwahlnummer geschaltet ist.
Im Falle des Beschwerdeführers handelte es sich um eine Ortsnetzrufnummer. Diese werden nicht von der Bundenetzagentur vergeben, sondern vom jeweiligen Netzbetreiber. Der Beschwerdeführer kann sich in diesem Fall an den Netzbetreiber wenden, den die Bundesnetzagentur mitgeteilt hat, um den Inhaber einer bestimmten Ortsnetzrufnummer in Erfahrung zu bringen. Diese Anfrage ist jedoch nicht immer erfolgreich, da hinsichtlich der Ortsnetzrufnummern der Anspruch aus § 66i Abs. 3 TKG gegen das jeweilige Telekommunikationsunternehmen nicht wie bei den Rufnummernbereichen (0)137 für Massenverkehrsdienste, (0)12 für Neuartige Dienste oder bei Kurzwahldiensten gegeben ist. Auch kann der Netzbetreiber aus vertraglichen oder datenschutzrechtlichen Gründen an einer Auskunft über seine Kunden gehindert sein. Dem Beschwerdeführer wurde durch die Anfrage des TLfDI bei der Bundesnetzagentur die Möglichkeit gegeben, beim Netzbetreiber hinsichtlich der ihn mit Werbeanrufen belästigenden Rufnummer eine Auskunft über den Namen und die ladungsfähige Anschrift zu erhalten.

Gegen lästige und aufdringliche Telefonwerbung kann die Hilfe der Bundesnetzagentur auch direkt vom Bürger selbst gemäß § 66i Abs. 3 TKG in Anspruch genommen werden (https://www.bundesnetzagentur.de/ortsnetz). Wenn der Netzbetreiber gefunden ist, kann eine Anfrage an diesen gestellt werden, um heraus zu finden, wer sich hinter einer bestimmten Rufnummer verbirgt, um mit diesem Wissen weitere Schritte einleiten zu können.



8.2 Auch Werbe-E-Mails entgehen dem Datenschutz nicht

Wer kennt das nicht: Bei Onlinebestellungen werden in der Regel vom Käufer sämtliche Angaben zu seiner Person verlangt; wie z. B. seine Adressdaten und/oder E-Mail-Adresse. Doch was passiert dann mit den Daten und wofür werden sie genutzt?
Ein typischer Fall ereignete sich bei einem Käufer eines Bürofachhandels. Der Käufer bestellte dort online und erhielt im Anschluss des Kaufes weitere E-Mails mit werblichem Inhalt. Er wandte sich daraufhin an das Unternehmen und bat nach § 34 Bundesdatenschutzgesetz (BDSG) um Auskunft, welche Daten letztendlich über ihn gespeichert sind, welche Daten evtl. an Dritte weitergegeben werden und forderte die Löschung seiner Daten. Da er nach seiner Aussage keine Antwort vom Bürofachhandel erhielt, wandte er sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und teilte sein Anliegen mit.
Nach § 34 Abs. 1 BDSG hat die verantwortliche Stelle dem Betroffenen auf Verlangen Auskunft zu erteilen über die zu seiner Person gespeicherten Daten, den Empfänger oder die Kategorien von Empfängern, an die Daten weitergegeben werden, und den Zweck der Speicherung. Vor diesem Hintergrund wandte sich der TLfDI an den Bürofachhandel und forderte diesen auf, dem Auskunftsersuchen nach § 34 Abs. 1 BDSG gegenüber dem betroffenen Käufer nachzukommen. Der Bürofachhandel reagierte und teilte u. a. mit, dass er bereits beim ersten Schreiben vom Käufer auf dessen Anliegen rea-

giert habe, er die geforderte Auskunft gegeben habe und legte das anhand der Ausgangsschreiben dem TLfDI vor. Auch auf Nachfrage bei dem betroffenen Käufer stellte sich heraus, dass er mit der Auskunft zufriedengestellt wurde und das nun endlich seine personenbezogenen Daten, die beim Bürofachhandel gespeichert waren, gelöscht wurden. Er sollte keine weiteren Werbe-E-Mails erhalten.

Nach § 34 BDSG besteht eine gesetzliche Auskunftspflicht über gespeicherte Daten eines Betroffenen bei einer verantwortlichen Stelle. Jeder Betroffene kann sich auf Grundlage des § 34 BDSG an verantwortliche Stellen wenden und Auskunft über seine gespeicherten Daten verlangen. Erhält der Betroffene keine Auskunft, kann er sich jederzeit an den TLfDI wenden.



Lupe Schufa - ©JiSign / Fotolia.com

9 Auskunfteien

9.1 Verhindert die SCHUFA Dispositionskredit?

Ein Abgeordneter des Thüringer Landtags bat den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) um Auskunft zur Frage der Löschung von Einträgen bei der Schufa. Der Abgeordnete selbst hatte eine Anfrage eines Bürgers vorliegen, dem ein beantragter Dispositionskredit in geringer Höhe verwehrt worden war. Dies war möglicherweise auf eine Forderung zurückzuführen, die bereits getilgt war und auf die Eintragung der Privatinsolvenz, zu der bereits eine Restschuldbefreiung erteilt wurde.
Der TLfDI wies zunächst darauf hin, dass er für die Schufa Holding AG keine Zuständigkeit habe, weil sie ihren Sitz nicht in Thüringen hat. Zuständig ist für die SCHUFA die hessische Datenschutzaufsicht.
Unter dieser Prämisse führte der TLfDI in der Sache aus, dass § 28 Abs. 1 Bundesdatenschutzgesetz (BDSG) die Zulässigkeitsvoraussetzungen für die Einmeldung von Forderungen aufzählt. Selbstverständlich besteht für den Betroffenen die Möglichkeit, nach § 34 Abs. 2 BDSG Auskünfte über die zu seiner Person gespeicherten

Daten bei der SCHUFA zu beantragen. Nach § 34 Abs. 8 BDSG ist die Auskunft unentgeltlich und kann vom Betroffenen einmal je Kalenderjahr verlangt werden. Sollte sich ergeben, dass noch Forderungen gespeichert sind, die bereits ausgeglichen sind, kann der Betroffene unter Umständen Löschung verlangen.
Die Erhebung und Verarbeitung der personenbezogenen Daten des Betroffenen durch die SCHUFA im Falle der Eröffnung einer Privatinsolvenz erfolgt in der Regel nach der Veröffentlichung in den Insolvenzbekanntmachungen als öffentlich zugängliche Quelle nach § 29 Abs. 1 Nummer 2 BDSG und liegt im Sinne des Gläubigerschutzes. Liegt bereits eine Restschuldbefreiung vor, kann auch diese veröffentlichte Entscheidung bei der SCHUFA gespeichert werden. Nach den Informationen auf der Internetseite der SCHUFA wird nach Erteilung der Restschuldbefreiung nach Ablauf eines Zeitraums von drei Jahren zum Jahresende dies im SCHUFA-Datenbestand gelöscht. Diese grundsätzliche Datenspeicherfrist kann aufgrund der Abwägung der Interessen der Wirtschaft zur Einschätzung eines geschäftlichen Risikos mit den Interessen des Betroffenen gerechtfertigt werden und ist datenschutzrechtlich nicht unzulässig.
Trotz der Restschuldbefreiung war demnach noch mit einer weiteren Speicherung zu rechnen. Kommt es in dieser Zeit zur Ablehnung eines beantragten Dispositionskredits, kann sich der Betroffene an die entsprechende Bank wenden und seine Belange vortragen. Die Entscheidung, einem Betroffenen einen Dispositionskredit einzuräumen oder zu versagen, unterliegt jedoch keiner datenschutzrechtlichen Bewertung.

Lehnt eine Thüringer Bank die Gewährung eines Dispositionskredites unter Hinweis auf Eintragungen bei der SCHUFA ab, kann sich der Betroffene durch eine Auskunft nach § 34 BDSG über die Eintragungen informieren und sich gegebenenfalls an die für die SCHUFA zuständige hessische Datenschutzaufsicht wenden. Die Entscheidung, einem Betroffenen einen Dispositionskredit einzuräumen oder zu versagen, unterliegt allerdings nicht der datenschutzrechtlichen Bewertung.

9.2 Überraschung: Ware nur nach Bonitätsabfrage

Im 2. Tätigkeitsbericht für den nicht-öffentlichen Bereich wurden unter Nummer 7.6 die Abläufe im Onlinehandel und die datenschutz-

rechtlichen Aspekte beim Onlineeinkauf dargestellt. Immer wieder gibt es Irritationen, wenn der Kauf unbemerkt für den Kunden eine Bonitätsabfrage bei einer Auskunftei voraussetzt.
Ein Betroffener wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), nachdem er versucht hatte, bei einem Thüringer Onlinehändler Ware im mittleren zweistelligen Wert zu bestellen und im Lastschriftverfahren zu bezahlen. Für ihn unerwartet wurde von ihm Vorkasse verlangt. Dies erklärte er sich damit, dass offenbar automatisch eine im „Kleingedruckten“, also in den Allgemeinen Geschäftsbedingungen (AGB), angesprochene Bonitätsabfrage bei einer Auskunftei durchgeführt worden war, was er im Hinblick auf den doch relativ geringen Warenwert für unverhältnismäßig ansah. Seine Anfrage an das Onlineunternehmen, welche negativen Auskünfte denn vorlägen, war nur kurz und knapp beantwortet worden. Bei einer erstmaligen Bestellung behalte man sich unabhängig vom Warenwert das Recht auf Vorkasse vor. Schließlich habe er die AGB bestätigt, die auf diese Möglichkeit hinwiesen. Wegen der Einstufung seiner Bonität solle er sich bitte an die Auskunftei wenden, denn hierzu speichere das Unternehmen keine Daten.
Der TLfDI teilte dem Betroffenen zu dem Problem der Verweisung an die Auskunftei mit, dass sich bei einer datenschutzrechtlichen Prüfung bestätigt hatte, dass das Unternehmen tatsächlich eine eventuell eingeholte Auskunft über die Bonität nicht speichere und daher nur die Auskunftei ihm Auskunft darüber erteilen könne, welche Bonitätswerte dort gespeichert werden. Weiterhin konnte vom TLfDI bei einer Kontrolle nicht festgestellt werden, dass das Unternehmen generell und automatisch unabhängig vom Vorliegen eines möglichen wirtschaftlichen Risikos Bonitätsabfragen vornimmt. Auf der Internetseite werden verschiedene Bezahlmöglichkeiten angeboten. Beim Kauf nach Vorkasse oder per Nachnahme bestehen für den Verkäufer der Ware keine wirtschaftlichen Risiken. Er erhält sicher Geld gegen Ware. Der Kauf auf Rechnung und das Lastschriftverfahren sind dagegen mit einer gewissen Unsicherheit behaftet, ob das Konto gedeckt ist oder ob der Kunde zahlungswillig und -fähig ist. Das Unternehmen muss sich nicht auf eine dieser „unsicheren“ Zahlungsarten einlassen, bei denen das Risiko besteht, dass der Kaufpreis möglicherweise nicht entrichtet wird und damit wirtschaftlicher Schaden entsteht. Dass der Verkäufer versucht, sein wirtschaftliches Risiko zu minimieren, muss akzeptiert werden. Dies darf er aber

nicht unbemerkt durch den Kunden durch eine Bonitätsabfrage als Datenerhebung über den Kunden tun.
Zieht die Auswahl einer unsicheren Zahlungsart eine Bonitätsabfrage bei einer Auskunftei nach sich, muss dies der Käufer frühzeitig bei der Auswahl der Zahlungsart erkennen können. Um sich bewusst für eine Zahlungsart mit oder ohne Bonitätsauskunft entscheiden zu können, darf der Kunde nicht nur darauf verwiesen werden, es sei aus den umfangreichen Allgemeinen Geschäftsbedingungen zu entnehmen, dass Bonitätsabfragen grundsätzlich möglich sind. Im Falle der Auswahl einer unsicheren Zahlungsart bedarf es keiner Einwilligung des Betroffenen nach § 4a Bundesdatenschutzgesetz (BDSG) zur Auskunfteiabfrage, denn die Rechtsgrundlage für die Auskunfteiabfrage bildet § 28 Abs. 1 Nr. 2 BDSG. Danach ist eine Datenverarbeitung aufgrund der Erforderlichkeit zur Wahrung des berechtigten Interesses des Onlineverkäufers zulässig. Jedoch bedarf es zur Information für den Betroffenen der konkreten Angabe, in welchem Fall mit einer Bonitätsabfrage zu rechnen ist, damit er sich bewusst für eine Zahlungsart mit oder ohne Auskunfteiabfrage entscheiden kann. Aus Gründen der Transparenz und Klarheit hat sich das Onlineunternehmen bereit erklärt, neben der Auswahlmöglichkeit von sogenannten unsicheren Bezahlarten einen Hinweis aufzunehmen, dass dies die Bonität voraussetzt und damit eine Auskunfteiabfrage verbunden sein kann.
Das Vorgehen des Unternehmens, bei erstmaligen Bestellungen nur auf Vorkasse zu liefern, stieß im Übrigen ebenfalls nicht auf datenschutzrechtliche Bedenken, denn mit diesem Vorgehen sind keine weiteren Datenerhebungen und Verarbeitungen verbunden.

Bei der Auswahl der Zahlungsart muss der Käufer im Onlinehandel wissen, ob eine bestimmte Art eine Bonitätsabfrage bei einer Auskunftei voraussetzt. Es ist kein Datenschutzproblem, wenn bei der ersten Bestellung eines Kunden das Unternehmen eine bestimmte sichere Zahlungsart verlangt, um sein wirtschaftliches Risiko zu begrenzen.

9.3 Schweigen eines Versandhandels

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichte eine Beschwerde eines Bürgers, der in einem großen Versandhandel in Thüringen eine Bestel-

lung getätigt hatte. Nachdem das Produkt dort aber wohl nicht mehr erhältlich gewesen ist, wurde seine Bestellung vom Versandunternehmen storniert und er darüber in Kenntnis gesetzt.
Daraufhin wollte der Bürger gerne wissen, welche Daten das Unternehmen über ihn speichert, und verlangte zudem, dass sein Kundenaccount, den er eigens für diese nicht ausgeführte Bestellung eingerichtet hatte, gelöscht wird. Er verlangte eine Auskunft gemäß § 34 Bundedatenschutzgesetz (BDSG) über die zu seiner Person gespeicherten Daten, auch soweit sie sich auf die Herkunft der Daten beziehen, den Empfänger oder die Kategorien von Empfängern, an die die Daten weitergegeben werden, und den Zweck der Speicherung, § 34 Abs. 1 Nr. 1 bis 3 BDSG. Als er nach Ablauf einer ausreichend bemessenen Frist keine Antwort vom Unternehmen erhalten hatte, schrieb er es erneut unter Fristsetzung an. Das Versandunternehmen reagierte allerdings überhaupt nicht auf dieses Auskunftsverlangen, auch nicht mit einer Negativauskunft. Diese wäre immer dann zu erteilen, wenn keine Daten mehr im Unternehmen vorliegen oder gespeichert werden. Aus diesem Grund wurde das Versandunternehmen seitens des TLfDI aufgefordert, eine entsprechende Auskunft gemäß § 34 BDSG an den Betroffenen zu erteilen, und es wurde mitgeteilt, dass der Account zu sperren und ggf. auch zu löschen ist, soweit keine gesetzlichen Aufbewahrungspflichten entgegenstehen. Weiterhin wurde durch den TLfDI ein Auskunftsersuchen an das Unternehmen gerichtet, indem es aufgefordert wurde mitzuteilen, welche technischen und organisatorischen Maßnahmen es getroffen hat, um dafür Sorge zu tragen, dass ein Auskunftsersuchen gemäß § 34 BDSG umfassend an den Betroffenen beantwortet wird. Dem Auskunftsverlangen nach § 34 BDSG an den Betroffenen kam das Unternehmen dann auch nach. Es erklärte weiterhin durch seinen betrieblichen Datenschutzbeauftragten gegenüber dem TLfDI, künftig dafür Sorge zu tragen, dass alle Auskunftsverlangen direkt dem Datenschutzbeauftragten zugeleitet werden und nicht wie bisher an die Sachbearbeiter des Unternehmens, die diese nach eigenem Ermessen beantwortet haben oder eben auch nicht.

Das Auskunftsrecht des Betroffenen gem. § 34 BDSG ist von der verantwortlichen Stelle immer zu beachten. Die Auskunft muss sich dabei auf alle zu seiner Person gespeicherten Daten, auch soweit sie sich auf die Herkunft der Daten beziehen, den Empfänger oder die Kategorien von Empfängern, an die die Daten weitergegeben wer-

den, und den Zweck der Speicherung beziehen, § 34 Abs. 1 Nr. 1 bis 3 BDSG. Für den Fall, dass eine verantwortliche Stelle keine Daten über den Betroffenen erhoben oder gespeichert hat, ist eine sog. Negativauskunft zu erteilen.



Siethoskop mit Gesundheitskarte auf Geldscheinen - © Zerbor / Fotolia.com

10 Gesundheit

10.1 Ansteckende Krankheiten sind Privatsphäre, oder nicht?

Anfang Februar 2016 erkundigte sich die Mitarbeiterin einer Betreuungseinrichtung danach, inwieweit die Mitarbeiter zu betreuende Schwerstkranke und deren Familien über nachgewiesene Keime (zum Beispiel MRSA) bei einer betreuten Person informieren dürfen. Hintergrund dieser Frage war der Schutz vor Infektionen für die weiteren Familien. Nach eigener Angabe traf die Einrichtung bei Keimbelastungen umfangreiche, hygienische Schutzmaßnahmen, die die Familie der betreuten Person einzuhalten hatte. Dennoch war es den Mitarbeitern wichtig, einen weitgehend normalen Aufenthalt zu ermöglichen und beispielsweise die Isolation der betroffenen Personen zu vermeiden. Die Einhaltung der Schutzmaßnahmen würde jedoch erschwert, wenn nicht alle potenziell Betroffenen über die Infektion informiert sind.
Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) beantwortete die Fragen der Betreuungseinrichtung folgendermaßen: Nach § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG) dürfen personenbezogene Daten an Dritte grundsätzlich nur übermittelt werden, wenn es eine Rechtsgrundlage hierfür gibt

oder der Betroffene eingewilligt hat. Bei der Frage, ob ein Befall mit multiresistenten Keimen vorliegt, handelt es sich um Angaben über die Gesundheit und damit um besondere Arten von Daten nach § 3 Abs. 9 BDSG. Diese Daten unterliegen einem besonderen gesetzlichen Schutz. Die Fälle, in denen die Übermittlung von Gesundheitsdaten zulässig ist, regelt § 28 Abs. 6 beziehungsweise Abs. 7 Satz 2 BDSG. In einer Betreuungseinrichtung ist davon auszugehen, dass die Mitteilung über den Befall mit multiresistenten Keimen an andere potenziell Betroffene zum Schutz ihrer Interessen notwendig ist. Hier werden Betreute behandelt, deren Immunabwehr u. U. sehr geschwächt ist. Für deren Familien ist es von existenzieller Bedeutung, die Ansteckungsgefahr zu kennen, denn nur dann können sie sich und vor allem ihre betreuten Familienangehörigen auch innerhalb der Einrichtung hinreichend schützen. Nach § 28 Abs. 7 Satz 2 und Satz 2 BDSG richtet sich die Zulässigkeit der Verarbeitung und Nutzung von Daten zur Gesundheitsvorsorge, medizinischen Diagnostik, Gesundheitsversorgung oder -behandlung nach den für ärztliches Personal geltenden Geheimhaltungspflichten (ärztliches Personal oder sonstige Personen). Die Übermittlung stellt einen Fall der Verarbeitung von Daten dar. Den Maßstab für die Zulässigkeit stellt § 203 Strafgesetzbuch (StGB) mit seiner Wertung zur Geheimhaltungspflicht dar. Danach darf ein Geheimnis, das einem Arzt oder medizinischem Personal anvertraut oder bekannt gemacht wurde durch diese nur offenbart werden, wenn sie dazu befugt sind. Dies kann sich aus einer Einwilligung (Schweigepflichtentbindung) oder einer Offenbarungsbefugnis ergeben. Gemäß § 34 StGB kann sich die Befugnis auch aus einem sogenannten rechtfertigenden Notstand ergeben, beispielsweise dem Schutz von Rechtsgütern Dritter. Dies wäre der Fall, wenn ein Patient sich trotz der Belehrung des Arztes weigert, gefährdete Personen über eine bestehende Infektionsgefahr aufzuklären (Fischer, Kommentar zum StGB, 63. Aufl. Rn. 47 zu § 203 m. w. N.). Somit ist die Information der Familienangehörigen über die Infektion einer betreuten Person mit multiresistenten Keimen nach § 28 Abs. 7 Satz 2 BDSG zulässig. Um die Akzeptanz dieser Information zu erhöhen, empfahl der TLfDI der Einrichtung, alle Beteiligten über die Gründe der Weitergabe in Kenntnis zu setzen und die Einrichtung sollte versuchen, die mit den multiresistenten Keimen infizierten Betroffenen bzw. deren Familien zur Einwilligung in die Weitergabe der Daten zu bewegen.

Besteht eine tatsächliche Gefahr für Leib und Leben von Personen, kann die Übermittlung von Gesundheitsdaten an gefährdete Personen nach § 34 StGB im Einzelfall gerechtfertigt sein, auch wenn sie mangels gesetzlicher Übermittlungsbefugnis oder Einwilligung der datenschutzrechtlich Betroffenen rechtswidrig ist.

10.2 Antworten zum betriebsärztlichen Datenschutz

Im Januar 2016 bat der Arbeitsmedizinische Dienst (AMD) eines Klinikums in Jena den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) um datenschutzrechtliche Auskunft zu Dokumentationen von Betriebsärzten. Der AMD betreut als Dienstleister Firmen in und um Jena betriebsärztlich. Infolge der Beendigung des Betreuungsvertrages mit einer Firma und dem Wechsel des externen Betriebsarztes ergab sich die Frage, inwiefern Betriebsarztdokumentationen an den betriebsärztlichen Nachfolger übergeben werden dürfen. Bei der eigenen Recherche hatte der AMD hierzu teilweise verschiedene Festlegungen gefunden.
Der Sachverhalt wurde vom AMD Jena folgendermaßen dargestellt:
Vor dem Ausscheiden des alten Betriebsarztes hatte die Firma ihre Mitarbeiter in einem Rundschreiben über den betriebsärztlichen Wechsel informiert und ihnen die Möglichkeit gegeben, der Aktenübergabe zu widersprechen. Nachdem kein Widerspruch ergangen war, forderte die Firma den ausscheidenden Betriebsarzt auf, dem neuen Betriebsarzt sämtliche Akten zu übergeben. Während der Aktenübergabe stellte sich heraus, dass der neue Betriebsarzt keine Möglichkeit hatte, die Akten in seinen Räumen aufzubewahren. Da das Unternehmen für die Datenverarbeitung durch den Betriebsarzt verantwortlich ist, sollten die Akten bei der Firma selbst aufbewahrt werden, vorausgesetzt, die Firma als Arbeitgeber kann selbst keinen Einblick in die Unterlagen nehmen. Die Akten sollten nach aktiven und inaktiven Mitarbeitern sortiert werden. Akten von aktiven Mitarbeitern sollten mit Zugriffsmöglichkeit des Betriebsarztes verschlossen und Akten von nicht mehr im Dienst befindlichen Mitarbeitern verschlossen und verplombt im Archiv des Betriebes aufbewahrt werden. Die Kisten mit den Akten der aktiven Mitarbeiter sollten vom betrieblichen Datenschutzbeauftragten direkt an den neuen Betriebsarzt übergeben werden. Alternativ wurde vom Klinikum auch eine direkte Übergabe dieses Aktenteils an den neuen

Betriebsarzt erwogen. Es sollte ein datenschutzkonformes Übergabeprotokoll mit der Anzahl der Akten von aktiven und inaktiven Mitarbeitern, namentlich sortiert, erstellt werden.
Im Hinblick auf dieses Vorgehen richtete der AMD an den TLfDI mehrere Fragen: Ist die geplante Archivierung der inaktiven Akten im Betrieb datenschutzrechtlich in Ordnung? Müssen Akten getrennt werden, wenn sie Daten enthalten, die außerhalb der arbeitsmedizinischen Vorsorge oder des Arbeitssicherheitsgesetzes erhoben wurden? Sollten nur objektive Befunde (beispielsweise Labordaten und Impftiter-Daten zu Antikörpern im Blut) übergeben werden? Ist es datenschutzkonform, wenn Akten von inaktiven, nicht mehr angestellten Mitarbeitern übergeben werden? Falls der neue Betriebsarzt gegen das Datenschutzrecht verstößt und ohne Zustimmung der Mitarbeiter Einsicht in eine Akte nimmt, kann dann auch der scheidende Betriebsarzt haftbar gemacht werden, da er die Akte abgegeben hat? Muss für die Aktenübergabe ein Widerspruchsverfahren durchgeführt werden? Bedarf die Akteneinsicht der ausdrücklichen Zustimmung des Mitarbeiters und müssen diese Akten bis zur Freigabe einzeln verschlossen verpackt sein?
Der TLfDI gab für die Übergabe der Dokumentation folgende Hinweise:
Grundlage für die Tätigkeit der Betriebsärzte sind das Arbeitssicherheitsgesetz (ASiG) und die Verordnung zur arbeitsmedizinischen Vorsorge (ArbMedVV). Nach § 3 ASiG ist es die Aufgabe des Betriebsarztes, den Arbeitgeber beim Arbeitsschutz und bei der Unfallverhütung in allen Fragen des Gesundheitsschutzes zu beraten und zu unterstützen. Auf dieser Grundlage erfolgt die Untersuchung von Arbeitnehmerinnen und Arbeitnehmern. Die betriebsärztliche Dokumentation beinhaltet sowohl arbeitnehmerbezogene individuelle medizinische als auch arbeitgeberbezogene Arbeitsplatzaspekte. Der Betriebsarzt unterliegt der ärztlichen Schweigepflicht und ist nach § 8 Abs. 1 ASiG gegenüber dem Arbeitgeber unabhängig. Daher muss ausgeschlossen werden, dass der Arbeitgeber Zugriff auf die Patientenkartei erhält. Dieser Ausschluss ist durch das beschriebene Vorgehen erfüllt. Akten von nicht mehr im Arbeitsverhältnis stehenden Mitarbeitern können beim Arbeitgeber gelagert werden, jedoch hat der frühere Betriebsarzt gemäß § 10 Abs. 4 Satz 1 der Berufsordnung der Landesärztekammer Thüringen dafür Sorge zu tragen, dass sie in gehörige Obhut gegeben werden. Der übernehmende Betriebsarzt muss diese Aufzeichnungen unter Verschluss halten und darf sie

nur mit Einwilligung des Patienten einsehen. Danach darf selbst der Datenschutzbeauftragte des Unternehmens keinen Zugriff auf diese Daten haben.

Nach der ArbMedVV muss der Arbeitgeber Pflicht- und Angebotsvorsorgen sowie Wunschvorsorgeuntersuchungen anbieten. Die Arbeitnehmer sind nur verpflichtet, an der Pflichtvorsorge mit Beratungsgespräch und Arbeitsanamnese teilzunehmen; weitergehende Untersuchungen können sie gemäß § 2 Abs. 1 Nr. 3 ArbMedVV ablehnen. Die strikte Trennung zwischen Vorsorge zur Gesundheit des Arbeitnehmers und Eignungsuntersuchungen für Zwecke des Arbeitgebers sollte sich auch in der Dokumentation des Betriebsarztes widerspiegeln. Insofern müssen Angaben zu Eignungsuntersuchungen getrennt verwahrt werden. Bei einem Wechsel des Betriebsarztes darf der Nachfolger nur mit persönlicher Einwilligung des Betroffenen auf diese Informationen zugreifen.

Arbeitnehmer können die Einsichtnahme durch den neuen Betriebsarzt in die gesundheitsbezogene Dokumentation früherer Untersuchungen ablehnen (§ 10 Abs. 4 Satz 2 Berufsordnung der Landesärztekammer Thüringen). Diese Unterlagen dürfen nicht vom neuen Betriebsarzt beigezogen werden; sie müssen bis zur Löschungsfrist besonders geschützt im Betrieb aufbewahrt werden. Der Nachfolger darf nur mit persönlicher Einwilligung des Betroffenen Zugriff auf diese Informationen nehmen. Der neue Betriebsarzt muss jedoch auf die für seine Arbeit notwendigen Stammdaten seines Vorgängers nach dem ASiG und der ArbMedVV Zugriff haben, d. h. auf die Angaben, die gegenüber dem Arbeitgeber zu attestieren sind: Art und Datum der Vorsorge und Datum der nächsten Vorsorge. Auch auf die vom Betriebsarzt erstellte Arbeitsplatzbeschreibung muss der Nachfolger zugreifen können.

Der Arbeitnehmer muss einer Übergabe der Betriebsarztdokumentation an einen neuen Betriebsarzt im Vorfeld nicht zustimmen. Aus Transparenzgründen müssen die Mitarbeiter jedoch rechtzeitig und umfassend über den geplanten Wechsel des Betriebsarztes informiert werden. Für die Datenverarbeitung durch den Betriebsarzt ist gemäß § 2 Abs. 2 Satz 1 ASiG das Unternehmen verantwortlich, nicht der Betriebsarzt. Wenn der scheidende Betriebsarzt bei der Übergabe der Akten die datenschutzrechtlichen Vorgaben einhält, kann er durch die Aufsichtsbehörde nicht für Datenschutzverstöße des neuen Betriebsarztes herangezogen werden.

Grundlage für die Tätigkeit von Betriebsärzten sind das Arbeitssicherheitsgesetz (ASiG) und die Verordnung zur arbeitsmedizinischen Vorsorge (ArbMedVV). Für die Datenverarbeitung durch den Betriebsarzt ist das beauftragende Unternehmen verantwortlich, nicht der Betriebsarzt. Wenn ein Unternehmen den externen Betriebsarzt wechselt, muss die betriebsärztliche Dokumentation unter Einhaltung bestimmter datenschutzrechtlicher Regelungen an den Nachfolger übergeben werden. Aus Transparenzgründen sind die Mitarbeiter im Vorfeld über den Wechsel zu informieren. Der neue Betriebsarzt hat, damit er seine Aufgaben nach dem ASiG erfüllen kann, auch ohne Einwilligung der Beschäftigten regelmäßig nur Zugriff auf die Stammdaten des Vorgängers, die gegenüber dem Arbeitgeber zu attestieren sind, wie beispielsweise Art und Datum der Vorsorge und Termin der nächsten Vorsorge sowie die Arbeitsplatzbeschreibung. Dies ist nicht direkt gesetzlich geregelt, sondern ergibt sich aus der im ASiG festgelegten Aufgabe des Betriebsarztes. Nach § 3 ASiG hat der Betriebsarzt den Arbeitgeber beim Arbeitsschutz und bei der Unfallverhütung in allen Fragen des Gesundheitsschutzes zu beraten und zu unterstützen. Die Einsichtnahme in die gesundheitsbezogene Dokumentation früherer Untersuchungen können die Arbeitnehmer ablehnen. Diese Unterlagen sind nach § 15 Abs. 1 Nr. 2 Thüringer Datenschutzgesetz zu sperren und bis zum Ablauf der Löschungsfrist besonders geschützt im Betrieb aufzubewahren.

10.3 Der Apotheker als Ermittlungshelfer der Polizei?

Im Berichtszeitraum erreichte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) die Frage einer Apotheke, ob sie Kundendaten an die Polizei zur Strafverfolgung herausgeben kann. Hintergrund war die Anfrage einer Landespolizeiinspektion, die wegen eines Verkehrsunfalls ermittelte. Die Polizeibehörde war auf der Suche nach dem Unfallverursacher, der sich unerlaubt vom Tatort entfernt hatte. Laut der Polizei kämen hierfür drei Kunden der Apotheke in Frage, weshalb um eine namentliche Bekanntgabe gebeten wurde.
Die Apotheke erfasst Daten für kundenorientierte Zwecke nur nach zuvor erteilter Einwilligung der betroffenen Person. Ein anderer Weg der Ermittlung von Kundendaten wäre, nach Auskunft der Apotheke, durch Zuordnung von anonymisierten Rezeptdaten möglich. Die

Erhebung und Speicherung der personenbezogenen Daten durch die Apotheke unterliegt jedoch dem Zweckbindungsgebot. Nach § 28 Abs. 1 Nr. 1 BDSG sind die Erhebung, Speicherung, Veränderung oder Übermittlung personenbezogener Daten sowie ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist.
Fraglich ist also, ob die Apotheke die Daten zweckentfremden kann und zur Ermittlung einer Straftat an die Polizeibehörden übermitteln darf.
Die Polizei ist nach § 163 Abs. 1 Strafprozessordung (StPO) dazu verpflichtet, Straftaten zu erforschen. Zu diesem Zweck ist sie befugt, Ermittlungen jeder Art vorzunehmen, worunter auch ein Auskunftsersuchen an ein privates Unternehmen fällt. Allerdings kann die Datenauskunft nicht verlangt werden, denn dem privaten Unternehmen wird keine Mitwirkungspflicht auferlegt. Nach § 28 Abs. 2 Nr. 2b BDSG ist die Übermittlung oder Nutzung der Daten zu einem anderen Zweck zulässig, soweit es zur Abwehr von Gefahren für die staatliche oder öffentliche Sicherheit oder zur Verfolgung von Straftaten erforderlich ist und kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung oder Nutzung hat. Allerdings verlangt auch diese Norm keine Pflicht der Übermittlung.
Allerdings könnte die Staatsanwaltschaft oder das Gericht eine Pflicht der Mitteilung herbeiwirken (Vorladung des Apothekers als Zeugen nach § 161a StPO oder Beschlagnahmung der Unterlagen §§ 95,98 StPO).
In dem vorliegenden Fall kann sich die Apotheke jedoch auf ihr Zeugnisverweigerungsrecht gemäß § 53 Abs. 1 Nr. 3 StPO berufen. Demnach sind Apotheker dazu berechtigt, über das, was ihnen in dieser Eigenschaft anvertraut oder bekannt geworden ist, das Zeugnis zu verweigern. Laut Kommentarliteratur zählt zu dem geschützten Bereich auch der Name des Patienten (Radke/Hohmann, § 53,Rn. 19). Dies ist nach Ansicht des TLfDI auch anwendbar auf den Apotheken – „Kunden“.
Eventuell könnte sich der Apotheker sogar nach § 203 Abs. 1 Nr. 1 Strafgesetzbuch (StGB) strafbar machen, wenn er die Daten herausgibt. Gemäß § 203 Abs. 1 Nr. 1 StGB macht sich strafbar, wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Le-

bensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als Apotheker anvertraut worden oder sonst bekannt geworden ist.
Der Apotheker kann sich auf sein Zeugnisverweigerungsrecht berufen, das sich auf die Tatsachen erstreckt, die dem Apotheker als Zeuge bei der Berufsausübung anvertraut oder bekannt geworden sind, wozu auch die Namen seiner Kunden zählen. Somit muss der Apotheker der Bitte der Polizei nicht Folge leisten.

Nach § 28 Abs. 1 BDSG ist das Erheben von Daten zum Durchführen von Rechtsgeschäften zulässig. Jedoch muss der Zweck der Verarbeitung oder Nutzung von personenbezogenen Daten zuvor definiert werden. Eine zweckentfremdete Nutzung und Übermittlung von Daten ist nur innerhalb der genannten Ausnahmen des § 28 Abs. 2 BDSG erlaubt. Berufsgeheimnisträger, zu denen unter anderem auch Apotheker gehören, haben das Recht auf Zeugnisverweigerung, um Ihrer Pflicht, kein fremdes Geheimnis zu verraten, gerecht zu werden (Verbot aus § 203 StGB).

10.4 Datenschutz bald verschreibungspflichtig?

Eine Mitinhaberin einer Apotheke wandte sich im Berichtszeitraum an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) mit dem Anliegen, dass sie den Verdacht hat, ihre ehemalige Mitarbeiterin habe Patientendaten aus der Kundenkartei gestohlen. Die ehemalige Mitarbeiterin arbeite jetzt bei einem neu eröffneten Sanitätshaus. Seit dem wurden Kunden der Apotheke vom Sanitätshaus kontaktiert, um für dessen Produkte und Leistungen zu werben. Viele Kunden waren über die Werbeanrufe empört und konnten es nicht nachvollziehen, wie das Sanitätshaus an die nicht-öffentlich zugänglichen Telefonnummern gekommen sei. Des Weiteren bestand der Verdacht, dass ausgestellte Rezepte der Apotheke kopiert worden waren, da das Sanitätshaus gezielt Anrufe an die Betroffenen getätigt und an den Ablauf des Rezepts erinnert hatte.
Der TLfDI hatte im Rahmen seiner aufsichtsbehördlichen Tätigkeit eine Vor-Ort-Kontrolle bei dem genannten Sanitätshaus veranlasst. Die mit der Kontrolle beauftragten Personen des TLfDI sind nach § 38 Abs. 4 Bundesdatenschutzgesetz (BDSG) berechtigt, soweit es zur Erfüllung der der Aufsichtsbehörde übertragenen Aufgaben er-

forderlich ist, während der Betriebs- und Geschäftszeiten die Grundstücke und Geschäftsräume der verantwortlichen Stelle zu betreten und dort Prüfungen und Besichtigungen vorzunehmen. Im Vorfeld der Kontrolle wurden von der Beschwerdeführerin Nachweise geliefert, die dazu dienen sollten, dass Patientendaten von der ehemaligen Mitarbeiterin gestohlen wurden. Bei der Kontrolle wurden diese Patientendaten abgeglichen. Das Sanitätshaus wies glaubhaft mit seinen Unterlagen nach, dass die Patientendaten selbst erhoben wurden. Die einzige Neukundengewinnung wurde über Werbeanzeigen in der Tagespresse sowie über Informationsmaterial geschaltet; gezielte Anrufe wurden nicht getätigt. Auch die in Rede stehenden Patientendaten von verstorbenen Patienten der Apotheke konnten bei der Sichtung der Unterlagen nicht nachgewiesen werden. Somit konnte der TLfDI keinen Datendiebstahl der Patientendaten und damit keinen Datenschutzverstoß feststellen.

Im Rahmen seiner aufsichtsbehördlichen Tätigkeit nach § 42 Thüringer Datenschutzgesetz (ThürDSG) führt der TLfDI regelmäßig Unternehmenskontrollen oder Kontrollen, bei denen der Verdacht eines Verstoßes gegen die Vorschriften des Bundesdatenschutzgesetzes vorliegt, durch. Hierzu ist der TLfDI nach § 38 Abs. 4 BDSG berechtigt. Im oben genannten Fall konnte allerdings kein datenschutzrechtlicher Verstoß festgestellt werden.

10.5 Patientendaten unverschlüsselt im IT-Dschungel

Der Landesbeauftragte für den Datenschutz von Sachsen-Anhalt (LfD Sachsen-Anhalt) leitete die Anfrage eines IT-Unternehmens aus seinem Bundesland an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) weiter. Die Anfrage des Unternehmens bezog sich auf die Patientensoftware einer Firma aus Thüringen.
Das IT-Unternehmen gab an, eine ambulante Tagespflege zu betreuen. Dieses Pflegeunternehmen setzte die Software einer Thüringer Firma ein. Die Mitarbeiter des Pflegedienstes sollten mit mobilen Endgeräten (Smartphones bzw. Tablets) ausgestattet werden. Um auf den zentralen Server zugreifen zu können, sollte das betreuende IT-Unternehmen die Firewall entsprechend einrichten. Die freizugebenden Schnittstellen erschienen dem beauftragten IT-Unternehmen nicht sicher. Das IT-Unternehmen wollte jedoch nicht für Datenlecks

haftbar gemacht werden und kritisierte im Hinblick darauf die eingesetzte Software. Dem sachsen-anhaltischen LfD lagen keine Informationen zur genutzten Software des Pflegedienstes vor. Das IT-Unternehmen bat darum, den Thüringer Software-Hersteller auf seine Verantwortung für den Datenschutz hinzuweisen.
Der TLfDI bat das IT-Unternehmen zunächst um eine genaue Darlegung der technischen und organisatorischen Gegebenheiten des Pflegedienstes. Diese wurden folgendermaßen beschrieben: Der Pflegedienst betrieb in Sachsen-Anhalt einen Server, auf dem das Programm der Thüringer Software-Firma lief. Auf diesen Server sollten die Mitarbeiter über Smartphones und Laptops zugreifen können. Genauere Zugriffsmethoden konnten durch das IT-Unternehmen nicht benannt werden. Nach Auskunft des IT-Unternehmens werde die Patientensoftware ebenso von anderen Pflegediensten, u. U. auch in Thüringen, genutzt und sei sehr verbreitet.
Der TLfDI informierte sich bei der Thüringer Herstellerfirma über die Patientensoftware bzw. die zum Einsatz kommende App und bewertete sie technisch und datenschutzrechtlich. Der TLfDI kam zu folgendem Ergebnis:
Der Betrieb und die Betreuung des zentralen Software-Servers erfolgt in der Regel nicht bei der Softwarefirma, sondern beispielsweise direkt beim Pflegedienst bzw. bei größeren Organisationen in einem eigenen Rechenzentrum oder auf einem externen angemieteten Server. In Ausnahmefällen, allerdings nicht im vorliegenden Fall, ist das Softwareunternehmen jedoch bereit, die Wartung der Server zu übernehmen. Daraus ergibt sich für derartige Fälle die datenschutzrechtliche Forderung des TLfDI, einen Vertrag zur Auftragsdatenverarbeitung nach § 11 Bundesdatenschutzgesetz (BDSG) mit dem technischen Betreiber und der Wartungsfirma abzuschließen.
Da es sich bei Patientendaten, die im Rahmen der Pflege anfallen, um besondere Arten von personenbezogenen Daten im Sinne des § 3 Abs. 9 BDSG handelt, unterliegen diese Daten einem besonderen Schutz. Gemäß § 9 BDSG müssen öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, die technischen und organisatorischen Maßnahmen treffen, die erforderlich sind, um die Einhaltung der datenschutzrechtlichen Vorschriften des BDSG zu gewährleisten. Somit ergibt sich für den TLfDI datenschutzrechtlich die Forderung nach § 9 BDSG an die verantwortlichen Stellen in derartigen Fällen, die Daten in der Datenbank zu verschlüsseln und den Personenkreis mit

dem notwendigen Wissen für den Zugriff so gering wie möglich zu halten. Die zentrale Datenbank ist auf Wunsch des Kunden, der nach geltendem Recht immer die verantwortliche Stelle ist, zu verschlüsseln. Das bedeutet, dass der Kunde ermitteln muss, ob aufgrund des Schutzbedarfs der Daten eine Verschlüsselung erforderlich ist, wovon bei den in Rede stehenden Daten auszugehen ist. Die Datenübertragung vom Web-Portal und der Smartphone-App soll ebenfalls verschlüsselt über HTTPS erfolgen. Datenschutzrechtlich ergab sich hierbei für den TLfDI die Forderung, HTTPS in jedem Fall zu nutzen, in dem der Web-Client nicht im selben internen Netz wie der Server betrieben wird. Der Browser übernimmt in diesem Fall die Prüfung der Authentizität, d. h. ob die Daten von der erwarteten Quelle stammen. Die App muss immer HTTPS nutzen, da sie regelmäßig nicht über das interne Netzwerk kommuniziert. Gerade die HTTPS-Nutzung war jedoch technisch zu diesem Zeitpunkt nicht gegeben. Die Datenübertragung vom Client-PC zum Server erfolgte in der Regel unverschlüsselt über die SQL-Schnittstelle des Servers. Dies ist nach Auffassung des TLfDI datenschutzrechtlich sehr bedenklich, wenn die Client-zu-Server-Verbindung nicht innerhalb des internen Netzwerks des Pflegedienstes zustande kommt. Wird der Server bei einem externen Anbieter betrieben, wäre eine Virtuelle-Private-Netzwerk-Verbindung (VPN) zum externen Anbieter notwendig, um eine sichere Verbindung vom Client zum Server zu gewährleisten.

Zum Zeitpunkt der Bewertung des TLfDI wurden bei der App-Nutzung nur Stammdaten (Wer ist zu pflegen?), Tourdaten (Welche Route wurde gefahren?) und Leistungsdaten (Welche Pflegeleistungen wurden summarisch erbracht?) vom Smartphone an den Server übertragen. Die Authentifizierung der Mitarbeiter ist über PIN/Passwort und Nutzername möglich. Nach Auffassung des TLfDI sollte die minimale Passwortlänge grundsätzlich den Forderungen des Bundesamtes für Sicherheit in der IT (BSI) folgen.

Auf den mobilen Endgeräten werden die Daten unverschlüsselt gespeichert. Auf den Client-PCs erfolgt die Löschung der Daten beim „Verlassen der Browsersitzung“, ohne dass dabei klar wird, wann dies geschieht. Im Sinne des Datenschutzes sollte der Löschzeitpunkt präzisiert werden. Eine automatisierte Funktion zur Datenlöschung auf Serverseite gibt es nicht. Daraus ergab sich für den TLfDI die datenschutzrechtliche Forderung, dass die Thüringer Softwarefirma mittel- bis langfristig eine einstellbare Löschfunktion einrichten

sollte. Eine Verschlüsselung auf dem Smartphone befand sich zum Zeitpunkt der Bewertung durch den TLfDI in der Entwicklung. Ob eine Verschlüsslung der gespeicherten Daten auf dem Smartphone zu fordern ist, wurde der datenschutzrechtlichen Bewertung der für den Pflegedienst, bei dem die App zum Einsatz kommt, zuständigen Aufsichtsbehörde in Sachsen-Anhalt überlassen. Für die datenschutzrechtliche Aufsicht über die Softwarefirma ist der TLfDI zuständig.

Patientendaten sind besondere Arten von personenbezogenen Daten im Sinne des § 3 Abs. 9 BDSG und unterliegen als Gesundheitsdaten einem besonderen Schutz. Gemäß § 9 BDSG müssen öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, die technischen und organisatorischen Maßnahmen treffen, die erforderlich sind, um die Einhaltung der datenschutzrechtlichen Vorschriften des BDSG zu gewährleisten. Hierzu zählen neben den Maßnahmen zur Verschlüsselung auch die Regelung des Datenzugriffs und die technische Umsetzung einer angemessenen Löschfrist. Im vorliegenden Fall sind hier noch Nachbesserungen notwendig.

10.6 Einsicht in die Patientenakte – beim Therapeuten oder bei dessen Anwalt?

Ein Patient wollte bei seinem dem Berufsgeheimnis unterliegenden Therapeuten Einsicht in seine Patientenakte nehmen. Der Therapeut verwies ihn an seinen Anwalt, bei dem sich die Akte befinde. Damit war klar, dass der Therapeut die Gesundheitsdaten an seinen Anwalt weitergegeben hatte. Um diese Übergabe seiner sensiblen Gesundheitsdaten vom Therapeuten an dessen Anwalt datenschutzrechtlich prüfen zu lassen, wandte sich der betroffene Patient an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI).
Selbstverständlich steht jedem Patienten das Einsichtsrecht in die Patientenakte gemäß § 630g Bürgerliches Gesetzbuch (BGB – sog. Patientenrechtegesetz) zu. Die gesetzlichen Vorschriften gehen grundsätzlich von einer Einsichtnahme beim jeweiligen Berufsgeheimnisträger aus. Dies vor dem Hintergrund, dass nur der die Akte führende Berufsgeheimnisträger auch beurteilen kann, ob einer Einsichtnahme erhebliche therapeutische Gründe oder sonstige erhebli-

che Rechte Dritter entgegenstehen. Daher stellte sich die Frage, weshalb der Beschwerdeführer zwecks Akteneinsicht an den Rechtsanwalt verwiesen wurde.
Patientenunterlagen können sich aus verschiedenen Gründen bei einem von einem Berufsgeheimnisträger beauftragten Rechtsanwalt befinden. Soll eine Rechtsfrage geklärt werden, kann ein Berufsgeheimnisträger selbstverständlich einen Rechtsanwalt damit befassen. Zu diesem Zweck können dem Rechtsanwalt die erforderlichen Angaben aber auch nur diese übergeben werden. Steht eine Rechtsstreitigkeit (beispielsweise ein Arzthaftungsprozess oder die Geltendmachung von Honoraren) im Hintergrund, können ausnahmsweise auch alle Angaben in der Patientenakte für die prozessuale Vertretung erforderlich sein. Nach § 3 Abs. 3 Bundesrechtsanwaltsordnung hat jedermann im Rahmen der gesetzlichen Vorschriften das Recht, sich in Rechtsangelegenheiten aller Art durch einen Rechtsanwalt seiner Wahl beraten und vor Gerichten, Schiedsgerichten oder Behörden vertreten zu lassen. Ohne die erforderlichen Unterlagen könnte das Mandat durch den Rechtsanwalt nicht wahrgenommen werden. Ob und in welchem Umfang einem Patienten Auskunft aus oder Einsicht in seine Patientenakte nach § 630b BGB gewährt werden muss und kann, bedarf allerdings als abstrakte Rechtsfrage grundsätzlich keiner Einsicht in die Patientenakte durch den beratenden Rechtsanwalt.
In allen anderen Fällen hängt eine Übergabe von Patientendaten an einen Rechtsanwalt ebenso wie jede Datenübermittlung zwischen Berufsgeheimnisträgern (z. B. Arzt zu Arzt, Psychologe oder Psychotherapeut zu Kollegen etc.) davon ab, ob eine Einwilligung des Patienten vorliegt. Liegt keine Einwilligung vor, wäre eine Strafbarkeit aufgrund der Verletzung von Privatgeheimnissen gemäß § 203 Abs. 1 Nr. 2 Strafgesetzbuch (StGB) möglich, was auf Antrag von den Strafverfolgungsbehörden zu prüfen ist.
Auf das Auskunftsersuchen des TLfDI nach § 38 Abs. 3 Bundesdatenschutzgesetz (BDSG) teilte der behandelnde Therapeut mit, die Patientenakten würden in seiner Praxis grundsätzlich in einem verschließbaren Stahlschrank aufbewahrt. Weiterhin wurde jedoch der TLfDI um Verständnis dafür gebeten, dass keine weiteren Angaben zum Umstand der Einsichtsgewährung durch den Rechtsanwalt gemacht würden, da eine sachgerechte Beantwortung mit dem Berufsgeheimnis und damit mit der Schweigepflicht kollidieren würde.
Damit gab sich der TLfDI selbstverständlich nicht zufrieden. Er wies darauf hin, dass die Aufsicht nach § 38 BGSG grundsätzlich unab-

hängig von etwaigen Berufs- und Amtsgeheimnissen bestehe. Damit können auch Geheimnisträger im Sinne des § 203 StGB ebenso uneingeschränkt der Datenschutzaufsicht nach § 38 BDSG wie jede andere nicht-öffentliche Stelle unterliegen. Soweit neben den allgemeinen Regeln des BDSG für diese Personengruppen, z. B. Ärzte und Psychotherapeuten, bereichsspezifische Schweige- und Geheimhaltungsverpflichtungen gelten, werden hierdurch die allgemeinen Regeln des BDSG nur punktuell berührt. Der TLfDI forderte daher nochmals dazu auf, die Beantwortung der gestellten Fragen nachzuholen. Dies wurde unter Verweis auf eine Entscheidung des Kammergericht Berlin aus dem Jahr 2010, nach der ein **Rechtsanwalt** wegen § 38 Abs. 3 Satz 2 BDSG grundsätzlich nicht verpflichtet ist, dem Datenschutzbeauftragten mandatsbezogene, seiner Verschwiegenheitspflicht unterliegende Informationen zu geben, erneut verweigert. Seine Verschwiegenheitsverpflichtung bewertete der behandelnde Therapeut genauso wie diejenige der Rechtsanwälte. Dabei wurde allerdings nicht beachtet, dass der Entscheidung des Kammergerichts Berlin zugrunde lag, dass Rechtsanwälte auch Organe der Rechtspflege sind, was für andere Berufsgeheimnisträger jedoch nicht zutrifft. Zugleich drehte der Therapeut den Spieß um und bat den TLfDI um Beratung und forderte eine Versicherung, dass er sich nicht strafbar mache, wenn er das Auskunftsbegehren beantworte.
Der TLfDI konnte die Zwangslage des Therapeuten durchaus verstehen und versuchte, den Interessenkonflikt zu entschärfen, indem er den Beschwerde führenden Patienten bat, dem behandelnden Therapeuten eine Schweigepflichtentbindung gegenüber dem TLfDI zu erteilen. Daraufhin teilte der Patient mit, dass er gegen den Therapeuten im Übrigen Strafanzeige erstattet habe. Da die Staatsanwaltschaft eindeutig festgestellt hatte, dass die Unterlagen vom Therapeuten nicht unbefugt an den Rechtsanwalt gelangt waren und somit auch kein Verstoß gegen datenschutzrechtliche Vorschriften vorlag, war das Verwaltungsverfahren durch den TLfDI einzustellen.

Einsicht in die Patientenakte hat nach § 630g BGB der behandelnde Berufsgeheimnisträger zu gewähren. Nur dieser kann einschätzen, ob eine Beschränkung der Akteneinsicht erforderlich und zulässig ist. Allein zur Gewährung der Akteneinsicht bedarf es keines rechtlichen Beistands.

10.7 Fotoshooting in der Arztpraxis – wenn der Patient ungewollt zum Model wird

Ein Bürger beschwerte sich darüber, dass eine Arztpraxis bei der Anmeldung Fotos von den Patienten fertigen würde. Auf Nachfrage wäre ihm mitgeteilt worden, dass die Fertigung der Fotos für die Patientenkartei nötigt wärden. Das Foto auf der Versicherungskarte sei dafür nicht geeignet. Insbesondere, so der Patient gegenüber dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), werde gegenüber den Patienten der Eindruck vermittelt, ohne eine entsprechende Zustimmung zur Fotoaufnahme würde keine ärztliche Behandlung stattfinden bzw. kein Termin zu bekommen sein. Der Bürger bat nun den TLfDI um rechtliche Bewertung.
Der TLfDI wandte sich mit einem Auskunftsverlangen nach § 38 Abs. 3 Bundesdatenschutzgesetz (BDSG) an die Praxis und bat um Stellungnahme zum Sachverhalt und um Mitteilung der Rechtsgrundlage für die Anfertigung von Fotoaufnahmen.
Daraufhin teilte die Praxis mit, dass sie die Vorwürfe mit Nachdruck zurückweise. Weiterhin teilte sie mit, dass die Mitarbeiterinnen bei der Anmeldung angehalten sind, alle Patienten zu fragen, ob ein Foto für die Patientenakte gefertigt werden darf. Besteht kein Einverständnis des Patienten, wird dies von den Mitarbeiterinnen in der Patientenakte vermerkt. Durch diesen Vermerk wird der Patient auch bei erneuter Vorstellung nicht noch einmal gefragt. Ebenfalls befindet sich – für alle Patienten sichtbar und zur Information – an der Anmeldung ein Schild mit einem entsprechenden Hinweis auf das Foto und die Möglichkeit, dies abzulehnen. Weiterhin wurde mitgeteilt, dass – entgegen der Behauptungen – kein Zwang zur Fotodokumentation bestehe. Das erstellte Foto befinde sich ausschließlich in der jeweiligen Patientenakte und unterliege dem Datenschutz und der ärztlichen Schweigepflicht. Als Begründung für die Erstellung der Fotos nannte man die Erhöhung der Patientensicherheit und das sie dazu dienen sollen, Verwechslungen der Patienten und damit einhergehende Behandlungsfehler zu vermeiden. In der Praxis wurde vermehrt festgestellt, dass die Fotos auf den Versicherungskarten häufig nicht dem Erscheinungsbild des Patienten entsprechen. Patienten, die kein Einverständnis zu einem Foto für die Patientenakte erteilen, würden selbstverständlich in der Praxis behandelt und bekämen auch Termine.

Nachdem der TLfDI die Stellungnahme der Praxis rechtlich bewertet hatte, wurde der Praxis mitgeteilt, dass das bisherige Vorgehen nicht den Anforderungen des BDSG entspricht. Denn die Schriftform ist – zumindest in solchen Fällen – für die Einwilligung verbindlich vorgeschrieben, § 4a Abs. 1 BDSG. Bei der Befragung der Patienten und dem daraufhin erteilten Einverständnis zur Anfertigung eines Fotos handelt es sich aber allenfalls um eine mündliche Einwilligung. Ausnahmen von der vorgeschriebenen Schriftform sieht das BDSG jedoch nur vor, wenn wegen besonderer Umstände eine andere Form angemessen ist. Dies ist bei Geschäften unter Anwesenden jeglicher Art kaum der Fall. Die mündlichen Absprachen hinsichtlich der Fotos mit den Patienten entsprachen folglich zumindest nicht der notwendigen Form und waren damit nichtig, § 125 Bürgerliches Gesetzbuch. Diesem Umstand könnte aber Abhilfe geleistet werden, indem eine schriftliche Einwilligung der Patienten, die auch im Übrigen den Anforderungen des § 4a BDSG entspricht, eingeholt würde. Dann wäre die Anfertigung der Fotos datenschutzrechtlich nicht mehr zu beanstanden.
Die Praxis hat sodann auf Raten des TLfDI ein entsprechendes Formular erarbeitet, das den Patienten vorgelegt wird und, mithilfe dessen er der Fotoaufnahme schriftlich zustimmen kann.

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist nach § 4 Abs. 1 BDSG nur zulässig ist, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Aufgrund einer wirksam erteilten Einwilligung der Patienten ist daher auch die Aufnahme und Speicherung eines Fotos des Patienten möglich. Allerdings ist eine solche Einwilligung nur wirksam, wenn sie die Anforderungen des § 4a BDSG, insbesondere auch die dortigen Formvorschriften erfüllt. Danach bedarf es für eine wirksame Einwilligung grundsätzlich der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist, vgl. § 4a Abs. 1 Satz 3 BDSG.

10.8 Fotoshooting in der Arztpraxis

Nicht schlecht staunte ein Patient bei seinem Besuch in einer Arztpraxis, als er beobachtete, wie am Empfangstresen die Patienten der Praxis mit einer Fotoaufnahme überrascht wurden. Auf Nachfrage der Patienten beim Praxispersonal, wozu derartige Fotos benötigt

würden, wurden diese mit der Antwort „Es sei für die Patientenkartei“ abgefertigt. Damit wandte sich ein Betroffener an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und bat um Aufklärung dieses Vorfalles und ggf. um Erläuterung der rechtlichen Hintergründe, siehe TB Beitrag 10.7.
Bei dieser Gelegenheit schilderte er auch ein weiteres „Shooting“, bei dem im Rahmen eines OP-Vorbereitungsgespräches plötzlich und ohne Vorwarnung vom Fragenden mittels eines Tablets ein Foto von ihm geschossen wurde. Auch in dieser Praxis wurde ihm auf Nachfrage lediglich geantwortet, dass die Fotos gebraucht würden. Der TLfDI wandte sich daher an die Arztpraxis und forderte diese dazu auf, unter Darlegung der rechtlichen Grundlagen ihr fotografisches Engagement näher zu erläutern. Daraufhin teilte die Praxis mit, dass sie aufgrund von Richtlinien, berufsständischen Vorgaben der Bundes- und Landesärztekammer sowie der Kassenärztlichen Vereinigung verpflichtet sei, ein Risikomanagementsystem einzurichten und umfassende Qualitätssicherungsmaßnahmen zum Schutz der Patienten und zur Vermeidung von Behandlungsfehlern zu ergreifen. Es sei im Rahmen von Präventionsmaßnahmen notwendig, die Fotos zu erstellen, da die Möglichkeiten der eindeutigen Identifizierung des Patienten in Bezug auf die Therapie grundlegend zur Vermeidung von Fehlern sind. Die Praxis gab weiterhin an, dass im schriftlichen Behandlungsvertrag, welcher aber zumeist erst kurz vor der OP abgeschlossen wird, die Einwilligung der Patienten zur Erstellung von Bildaufnahmen eingeholt würde. Nach Prüfung der von der Praxis angegebenen Richtlinien und berufsständischen Vorgaben konnten daraus allerdings seitens des TLfDI keine rechtlichen Grundlagen für die Erstellung von Patientenfotos ohne ausdrückliche Einwilligung abgeleitet werden. Nach § 4 Abs. 1 BDSG ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit das BDSG oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.
Da sich keine Rechtsgrundlage zur Erhebung von Patientenfotos im Sinne des § 4 Abs. 1 BDSG aus den von der Praxis vorgetragenen Grundlagen ergibt, ist allein auf eine Einwilligung der Patienten abzustellen. Diese Einwilligung muss den Anforderungen des § 4a BDSG entsprechen und ist nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht, nachdem er über den Zweck der Erhebung und Verarbeitung hingewiesen wurde, und schriftlich erfolgt. Weiterhin muss die Einwilligung vor der Erhebung der Da-

ten, also vor dem Fotoshooting, erfolgen. Der Praxis wurde daher aufgegeben, Patientenfotos nur mit vorheriger schriftlicher Einwilligung der Patienten zu fertigen, da eine nachgeholte Einwilligung im schriftlichen Behandlungsvertrag nicht ausreichend ist.

Es bedarf für die Zulässigkeit der Anfertigung von Patientenfotos immer einer vorherigen, aufgeklärten, freiwilligen und schriftlichen Einwilligung des jeweiligen Patienten.

10.9 Datenspeicherung in Apotheke: Kommerz versus Recht

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichte eine Beschwerde eines Apothekenkunden, welcher dort mit einem Rezept ein Arzneimittel kaufen wollte. Beim Suchen des Apothekers nach dem Medikament im Computer wurde er mit der beiläufigen Mitteilung überrascht, dass er das Medikament ja schon einmal bekommen hätte. Auf die Nachfrage des Kunden, wieso sein Name und die von ihm gekauften Medikamente in der Apotheke gespeichert sind, wurde ihm nur ausweichend geantwortet. Der Kunde widersprach daraufhin der Datenspeicherung noch vor Ort und der Apotheker vermerkte dies auch so.
Der Kunde trat daraufhin an den TLfDI heran mit der Frage, ob es überhaupt zulässig sei, dass die Apotheke speichert, welche Medikamente er dort kauft? Er teilte weiterhin mit, dass er weder eine Kundenkarte habe noch jemals irgendeine Zustimmung abgegeben hätte.
Nach § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG) sind die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Insbesondere erfolgt die Datenerhebung und -verarbeitung in Arztpraxen, Krankenhäusern und auch Apotheken in einem besonders sensiblen Bereich, denn bei Patientendaten und den darin enthaltenen Informationen zum Gesundheitszustand des Patienten handelt es sich um besondere Arten personenbezogener Daten im Sinne von § 3 Abs. 9 BDSG. Aus der Sensibilität der Daten resultiert ein besonderes Schutzbedürfnis, das sich datenschutzrechtlich in § 28 Abs. 6 ff. BDSG niederschlägt. Dort sind strenge Voraussetzungen festgelegt, nach denen im medizinischen Bereich mit Patientendaten verfahren werden darf. Ein Verstoß gegen die Vertraulichkeit der erhobenen

Informationen ist zudem in § 203 Abs. 1 Nr. 1 Strafgesetzbuch mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bedroht. Unter diese Bestimmungen fällt auch der Apotheker.
Die Erhebung sowie die Verarbeitung, worunter auch das Speichern fällt, von besonderen Arten personenbezogener Daten darf nach § 28 Abs. 7 Satz 1 und 2 BDSG nur erfolgen, wenn sie für medizinische Zwecke erforderlich ist und wenn sie von den in der Vorschrift bezeichneten Stellen der Gesundheitsversorgung durchgeführt wird. Die Erhebung und Speicherung der Patientendaten in der Apotheke ist jedoch nicht für medizinische Zwecke erforderlich.
Im Ergebnis ist eine Speicherung von Kundendaten, die besondere Arten personenbezogener Daten enthalten, durch die Apotheke ohne Einwilligung des Kunden nicht zulässig.
Möchte aber eine Apotheke diese Kundendaten speichern, muss eine schriftliche Einwilligung des Kunden gem. § 4a BDSG eingeholt werden. Die Einwilligungserklärung muss den Namen und die Adresse der Apotheke sowie den Grund für die Speicherung enthalten. Auch muss ein Hinweis auf die Möglichkeit des jederzeitigen Widerrufs der Einwilligungserklärung gegeben werden. Soweit Kundendateien ohne dazugehörige Einwilligungserklärungen angelegt werden, handelt es sich um eine rechtswidrige Datenerhebung bzw. -speicherung. Bei einem Widerruf müssen die Daten unverzüglich gelöscht werden.
Etwas anderes gilt nur dann, wenn die Datenspeicherung zur Abwicklung des Vertragsverhältnisses zwischen Kunde und Apotheke erforderlich ist. Hier regelt § 28 Abs. 1 Nr. 1 BDSG die Speicherung für eigene Geschäftszwecke des Apothekers. Dies ist immer dann gegeben, wenn die Speicherung der Daten zur Begründung, Durchführung oder Beendigung eines Schuldverhältnisses erforderlich ist und es sich hierbei um personenbezogene Daten handelt und nicht um Gesundheitsdaten. Dies ist dann der Fall, wenn zum Beispiel eine gesonderte Bestellung der Medikamente erfolgte und die Daten (Adresse, Telefonnummer des Kunden) aufgrund der Abwicklung des bestehenden Vertragsverhältnisses noch benötigt werden und daher auch erforderlich sind.
Vorliegend war jedoch eine Speicherung der Kundendaten weder aufgrund einer Einwilligung möglich, da diese nicht erteilt wurde, noch aufgrund der Abwicklung eines gesonderten Bestellvorganges. Die Datenspeicherung erfolgte daher rechtswidrig. Ein Bußgeldverfahren wurde jedoch nicht eingeleitet, da der Kunde die Apotheke

nicht benannt und nur eine allgemeine Anfrage an den TLfDI formuliert hatte.

Die Speicherung von Kundendaten in der Apotheke ist nur mit einer ausdrücklichen Einwilligung des Betroffenen zulässig, da die Erhebung und Speicherung der Patientendaten in der Apotheke nicht für medizinische Zwecke erforderlich ist. Etwas anderes gilt nur dann, wenn die Datenspeicherung zur Abwicklung des Vertragsverhältnisses zwischen Kunde und Apotheke erforderlich ist, beispielsweise im Rahmen einer Bestellung von Medikamenten.

10.10 Daten im Wartezimmer?

Im Berichtszeitraum erreichte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) eine Beschwerde, dass eine Zahnarztpraxis in Thüringen keine räumliche Trennung zwischen dem Wartebereich und dem Patientenaufnahmebereich vorgenommen hatte.
Grundsätzlich müssen Ärzte bei der Organisation ihrer Praxis den Anforderungen des Geheimnis- und Datenschutzes gerecht werden. Nach § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG) ist die Erhebung, Verarbeitung, unter welche auch die Übermittlung an Dritte fällt, und Nutzung personenbezogener Daten nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Bei personenbezogenen Daten besonderer Art, zu denen auch Gesundheitsdaten zählen (§ 3 Abs. 9 BDSG), ist in besonderem Maße auf das informationelle Selbstbestimmungsrecht der Patienten zu achten.
Gemäß § 9 BDSG haben nicht-öffentliche Stellen, die selbst personenbezogene Daten erheben, verarbeiten oder nutzen, die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften des Bundesdatenschutzgesetz, insbesondere die in der Anlage 1 zu § 9 BDSG genannten Anforderungen, zu gewährleisten. Maßnahmen sind nur erforderlich, solange ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.
Praktisch bedeutet dies, dass Ärzte dafür Sorge tragen müssen, dass unbefugte Dritte keinen Einblick in oder Zugriff auf Patientenakten und -daten haben dürfen. Infolgedessen muss auch bei der Ausrichtung des PC-Bildschirms beachtet werden, dass niemand außer dem

Arzt und dem Praxispersonal Einsicht darin hat. Des Weiteren dürfen keine Gespräche mit den Patienten geführt werden, die über Terminabsprachen hinausgehen, wenn die Möglichkeit des Mithörens besteht.
Auf Nachfrage erklärte die Ärztin, dass wegen der eingeschränkten Platzverhältnisse keine vollständige Trennung des Aufnahme- und Wartebereichs umsetzbar sei. Da es sich um Mieträume handele, wäre eine bauliche Veränderung im Auftrag der Ärztin nicht möglich. Es wurde versichert, dass an der Rezeption lediglich organisatorische Themen besprochen und alle medizinisch relevanten Informationen im Behandlungszimmer ausgetauscht werden.
Somit hat die Ärztin in diesem Fall alle erforderlichen Maßnahmen getroffen. Eine Auseinandersetzung mit dem Vermieter über eine kostenintensive Umbaumaßnahme zu verlangen, wäre im Sinne von § 9 BDSG ein unverhältnismäßiger Aufwand für die verantwortliche Stelle.

Wenn Daten erhoben, verarbeitet oder genutzt werden, müssen auch in einer Arztpraxis technische und organisatorische Maßnahmen getroffen werden, die erforderlich sind, um die personenbezogenen Daten zu schützen (§ 9 BDSG). Eine abschließende Auflistung der entsprechenden Maßnahmen findet sich in der Anlage 1 zu § 9 des BDSG.

10.11 Datenschutz beim Zahnarzt: TLfDI bohrt nach

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) erhielt das Schreiben einer Bürgerin, die sich darüber beklagte, dass in einer Arztpraxis der Wartebereich nicht baulich vom Aufnahme-/ Empfangsbereich getrennt sei. Es sei wohl dadurch möglich, dass andere Patienten die Gespräche zwischen Zahnarzthelferinnen und Patienten bei der Anmeldung mithören könnten. Der TLfDI wandte sich daraufhin mit einem Auskunftsverlangen nach § 38 Abs. 3 Bundesdatenschutzgesetz (BDSG) an die Praxis. Danach sind die Aufsichtsbehörden – wie der TLfDI – befugt, bei den der Kontrolle unterliegenden Stellen Auskunft zu verlangen. Der TLfDI teilte der Praxis im Auskunftsverlangen mit, dass die wesentlichen rechtlichen Grundlagen für den Umgang mit personenbezogenen Daten in Arztpraxen sich im BDSG wiederfinden. Das BDSG regelt, wie mit personenbezogenen Daten durch die

verantwortlichen Stellen und ggf. ihre Mitarbeiter umzugehen ist. Nach § 4 Abs. 1 BDSG ist die Erhebung, Verarbeitung, worunter auch die Übermittlung an Dritte fällt, und Nutzung personenbezogener Daten nur zulässig, soweit das BDSG oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene nach § 4a BDSG eingewilligt hat.
Dabei hat auch die Praxisorganisation den Anforderungen des Geheimnis- und Datenschutzes gerecht zu werden. Denn gerade bei Gesundheitsdaten als besondere Art personenbezogener Daten, § 3 Abs. 9 BDSG, wollen die Patienten den Umgang mit ihren sensiblen Daten geschützt wissen. Dem Datenschutz muss der Arzt dadurch Rechnung tragen, dass er sowohl bei konventionellen Patientenakten als auch beim Einsatz von Datenverarbeitungstechniken gewährleistet, dass unbefugte Dritte weder im Empfangsbereich noch in den Behandlungsräumen Kenntnis von den Patientendaten erhalten. Unbefugte Dritte sind dabei auch andere Patienten. So dürfen papiergebundene Patientenakten in keinem Fall so gelagert werden, dass andere Patienten diese zur Kenntnis nehmen können. Dementsprechend sind Bildschirme so aufzustellen, dass sie nur vom Arzt und dem Praxispersonal eingesehen werden können. In den Fällen, in denen ein Arbeitsplatz nicht besetzt ist, muss der EDV-Arbeitsplatz gesperrt und Akten müssen weggeschlossen werden, sodass wartende Patienten keine Möglichkeit haben, Patientendaten zur Kenntnis zu nehmen. Ebenso können, wenn der Wartebereich und der Anmeldebereich nicht getrennt sind, keine Gespräche mit dem Patienten geführt werden, die über reine organisatorische Themen, wie beispielsweise Terminabsprachen, hinausgehen. Weiterhin wurde der Praxis mitgeteilt, dass bei der Organisation der Praxis sicherzustellen ist, dass unbefugtes Mitlesen oder Mithören ausgeschlossen wird.
Die Praxis reagierte mit Verwunderung über das Schreiben des TLfDI und teilte mit, dass an der Rezeption in der Regel keine weiterführenden Gespräche über Patienten geführt werden würden. Der Computerbildschirm sei für die Patienten nicht einsehbar und in der Rezeption integriert. Die für die Sprechstunde vorbereiteten Patientenakten würden nicht einsehbar für die an der Rezeption stehenden Patienten im hinteren Bereich der Karteikartenschränke liegen. Der Wartebereich war durch ein Möbelstück abgetrennt, allerdings wurde aus Platzgründen diese Trennung wieder rückgängig gemacht. Ebenso konnten dadurch allein wartende Kinder vom Personal besser beaufsichtigt werden. Die Rezeption sei in der Regel während der

Sprechstunde immer besetzt. Nicht ausgeschlossen sei aber das kurzzeitige Verlassen der Rezeption durch die Schwester, um Patientenakten in das Sprechzimmer zu bringen. Die Rezeption für diesen kurzen Zeitraum abzuschließen, sei bei dem Patientendurchlauf schlicht und ergreifend nicht möglich. Der Arzt versicherte, seine Mitarbeiter über den Inhalt des Schreibens zu informieren und sie auch diesbezüglich aktenkundig zu belehren. Die bauliche Veränderung bezüglich der Abtrennung wird er umgehend rückgängig machen.
Der TLfDI behält sich eine Vor-Ort-Kontrolle vor.

In Arztpraxen werden regelmäßig Patientendaten verarbeitet. Diese Daten stehen als besondere Art von personenbezogenen Daten – § 3 Abs. 9 BDSG – unter dem besonderen Schutz des BDSG. Deshalb ist auch hier gemäß § 4 Abs. 1 BDSG die Erhebung, Verarbeitung, worunter auch die Übermittlung an Dritte fällt, und Nutzung personenbezogener Daten nur zulässig, soweit das BDSG oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene nach § 4a BDSG eingewilligt hat.

10.12 Auch Krankenhäuser von DS-GVO betroffen

Die Landeskrankenhausgesellschaft erreichte eine Nachfrage eines Thüringer Krankenhauses im Hinblick auf die neue EU-Datenschutz-Grundverordnung (DS-GVO). Die Krankenhausgesellschaft leitete die Anfrage an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) weiter.
Während bislang durch nationale Gesetzgebungen auf Grundlage der EU-Datenschutzrichtlinie doch erhebliche Unterschiede bestanden, soll mit der DS-GVO das Datenschutzrecht in der EU vereinheitlicht werden. Sie wird ab 25. Mai 2018 wirksam.
In Art. 35 DS-GVO ist die Datenschutz-Folgenabschätzung, die der Verantwortliche für die Datenverarbeitung beratend mit dem Datenschutzbeauftragten, durchzuführen hat, geregelt. Konkret fragte nun das Krankenhaus, ob die nach Art. 35 Abs. 4 DS-GVO von der Aufsichtsbehörde zu erstellende Liste der Verarbeitungsvorgänge, für die gemäß Absatz 1 eine Datenschutz-Folgenabschätzung durchzuführen ist, bereits erstellt ist und falls ja, wo diese zu finden sei.
Der TLfDI erklärte, dass die Liste, in der die Verarbeitungsvorgänge für die Datenschutz-Folgenabschätzung enthalten sind, zu gegebener

Zeit auf der Homepage des TLfDI zu finden sein wird. Noch stimmen sich die Aufsichtsbehörden des Bundes und der Länder darüber ab, welche Verarbeitungsvorgänge einer Datenschutz-Folgenabschätzung zu unterziehen sind, da eine möglichst bundeseinheitliche Handhabung gewünscht ist. Der TLfDI ging aber davon aus, dass die Datenverarbeitung in einem Krankenhaus mit einen Krankenhausinformationssystem einer Datenschutz-Folgenabschätzung zu unterziehen ist. Wenn die Abstimmung unter den Datenschutzaufsichtsbehörden und die Veröffentlichung auf der Homepage des TLfDI erfolgt sind, wird der TLfDI die Krankenhausgesellschaft informieren.

Zudem wollte das Krankenhaus wissen, ob durch die neue EU-DS-GVO Handlungsbedarf bei den vorliegenden Standardvertragsklauseln besteht. Die Standardvertragsklauseln der Europäischen Union finden derzeit Anwendung, wenn personenbezogene Daten außerhalb der Europäischen Union verarbeitet werden. Die Klauseln sollen den Schutz persönlicher Daten auch dann sicherstellen, wenn Unternehmen personenbezogene Daten an andere Unternehmen außerhalb der EU zur Weiterverarbeitung übersenden. Im Gegensatz dazu ist der Privacy Shield (Datenschutzschild) ein informelles Übereinkommen der Europäischen Union mit den Vereinigten Staaten von Amerika, in dem die amerikanische Bundesregierung datenschutzrechtliche Zusicherungen abgegeben hat. Amerikanische Unternehmen können sich dazu verpflichten, die Regelungen des Privacy Shield einzuhalten und sich in eine entsprechende Liste eintragen lassen, die unter https://www.privacyshield.gov/list veröffentlicht wird. Die Europäische Kommission hat am 12. Juli 2016 beschlossen, dass die Vorgaben des Datenschutzschilds dem Datenschutzniveau der Europäischen Union entsprechen. Außerdem fragte das Krankenhaus, ob getätigte Verträge einschließlich der Auftragsdatenverarbeitung gesichtet und überarbeitet werden müssen. Nach dem Kenntnisstand des TLfDI besteht auch für die vorliegenden Standardvertragsklauseln Anpassungsbedarf hinsichtlich der DS-GVO. Die bisher geschlossenen Verträge müssten daher gesichtet und überarbeitet werden. Dies gilt dann auch insbesondere für die Auftragsverarbeitung. Hierzu soll in Zusammenarbeit mit den anderen Aufsichtsbehörden eine Handlungsempfehlung erarbeitet werden.

Mit Inkrafttreten der DS-GVO müssen viele Regelungen hinsichtlich des Datenschutzes angepasst werden. Die Liste der Verarbeitungsvorgänge, in denen die Datenschutz-Folgenabschätzung durchgeführt werden muss, wird auf der Homepage des TLfDI zu finden sein. Da die DS-GVO viele Änderungen enthält, müssen auch die bereits geschlossenen Verträge und Standardklauseln hinsichtlich der neuen datenschutzrechtlichen Regelungen geprüft und gegebenenfalls geändert werden.

10.13 Schreddern im Krankenhaus

Die Datenschutzbeauftragte eines thüringischen Klinikums bat den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) um Auskunft zur Frage der ordnungsgemäßen Vernichtung von Datenträgern. Sie hatte sich bereits selbst über die geltenden Regelungen im Internet informiert und dabei die „Orientierungshilfe zur Ermittlung des Schutzbedarfs personenbezogener Daten für den Prozess der Datenträgervernichtung“ (OH) gefunden. In der OH werden Anforderungen an die datenschutzgerechte Vernichtung von Datenträgern dargelegt, die berücksichtigen, dass im Oktober 2012 die neue DIN 66399 „Büro- und Datentechnik – Vernichten von Datenträgern“ veröffentlicht wurde. Die DIN 66399 empfiehlt jeder verantwortlichen Datenverarbeitenden Stelle, alle im Geschäftsverkehr vorkommenden oder anfallenden Informationen (Daten) bzw. die sie speichernden Datenträger zunächst hinsichtlich des Schutzbedarfs zu klassifizieren; sie definiert hierfür drei Schutzklassen. Darüber hinaus beschreiben sieben Sicherheitsstufen Anforderungen an die Wirksamkeit der Vernichtung, d. h. die Höhe des Aufwands für Angreifer, vernichtete Datenträger bzw. darauf gespeicherte Daten wiederherzustellen und Information zur Kenntnis nehmen zu können. Anschließend empfiehlt die DIN, Datenträger bestimmter Schutzklassen nur nach bestimmten Sicherheitsstufen zu vernichten und trägt so dem Prinzip der Angemessenheit Rechnung. Die DIN bestimmt für diverse Materialklassen (wie Papier, Mikrofilm, magnetische Datenträger, optische Datenträger, Halbleiterspeicher) Grenzwerte für Teilchengrößen, die bei der Vernichtung eines Datenträgers eingehalten werden müssen, um die Wiederherstellung von Informationen aus dem nach der Vernichtung vorliegenden Restmaterial zu verhindern oder zumindest zu erschweren.

Durch das Vernichten von Datenträgern, auf denen personenbezogene Daten gespeichert sind, kommen verantwortliche Stellen nach § 20 Abs. 2 Bundesdatenschutzgesetz (BDSG) ihrer Verpflichtung zum Löschen dieser Daten nach. Personenbezogene Daten sind insbesondere dann zu löschen, wenn ihre Speicherung unzulässig oder ihre Kenntnis für die Aufgabenerfüllung bzw. zur Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist. Unter dem Begriff „Löschen“ wird dabei die Unkenntlichmachung gespeicherter personenbezogener Daten verstanden (§ 3 Abs. 4 Nr. 5 BDSG). Das Vernichten von Datenträgern ist gleichzeitig eine technisch-organisatorische Maßnahme zur Gewährleistung der Datensicherheit, insbesondere zur Verhinderung der Kenntnisnahme personenbezogener Daten durch Unbefugte (Sicherung der Vertraulichkeit nach § 9 BDSG sowie dessen Anlage). Danach muss die Maßnahme dem Schutzbedarf der Daten angemessen sein. Ihre Umsetzung hat sich nach den im Einzelfall zu betrachtenden Risiken und dem Stand der Technik zu richten.

Die Datenschutzbeauftragte wollte wissen, welche Anforderungen danach für das betreffende Krankenhaus gelten. Nach Auffassung des TLfDI sind alle personenbezogenen medizinischen Daten, die einem Berufs- und/oder Amtsgeheimnis unterliegen, der Schutzbedarfsklasse 2 bis 3 zuzuordnen. Dies sind z. B. Behandlungsunterlagen und- Diagnosen. Spezielle Unterlagen, die z. B. Transplantationen betreffen, sind Schutzbedarfsklasse 3 zuzuordnen. Andererseits gibt es Gesundheitsdaten, die nicht dem Berufs- und/oder Amtsgeheimnis unterliegen, wie z. B. Blutspendeaufzeichnungen, die entsprechend der OH nach Schutzbedarfsklasse 2 einzuordnen sind. Es kommt also auf den Einzelfall an.

Zur Erfüllung der Schutzbedarfsklasse 2 wird die Sicherheitsstufe ab P-4 aufwärts empfohlen. Zur Erfüllung der Schutzbedarfsklasse 3 ist aus Sicht des TLfDI die Sicherheitsstufe ab P-5 aufwärts einzusetzen. Entsprechend der DIN 66399-2 bedeutet dies konkret:

Sicherheitsstufe für Papier	Materialteilchenfläche	Toleranz für 10% des Materials
P-4	Die Materialteilchenfläche ≤ 160 mm² und für die regelmäßigen Partikel: Streifenbreite max. 6mm	Materialteilchenfläche max. 480 mm^2

P-5	Die Materialteilchenfläche ≤ 30 mm² und für die regelmäßigen Partikel: Streifenbreite max. 2mm	Materialteil-chenfläche max. 90 mm^2

Der Datenschutzbeauftragten wurden die durch das Krankenhaus einzuhaltenden Anforderungen (Sicherheitsstufe P-5) mitgeteilt.

Auch bei der Datenträgervernichtung sind die datenschutzrechtlichen Vorgaben einzuhalten. Durch das Vernichten von Datenträgern, auf denen personenbezogene Daten gespeichert sind, kommen verantwortliche Stellen ihrer Verpflichtung zum Löschen dieser Daten nach. Das Vernichten von Datenträgern ist gleichzeitig eine technisch-organisatorische Maßnahme zur Gewährleistung der Datensicherheit, insbesondere zur Verhinderung der Kenntnisnahme personenbezogener Daten durch Unbefugte (Sicherung der Vertraulichkeit), § 9 BDSG sowie dessen Anlage. Danach muss die Maßnahme dem Schutzbedarf der Daten angemessen sein. Krankenhäuser müssen in Bezug auf die Gesundheitsdaten die Schutzklasse 3 nach DIN 66399 einhalten.

10.14 Einwilligungserklärung bei Ärzten – So einfach geht das nicht!

Ein externer Datenschutzbeauftragter wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), um eine Zweitmeinung für einen an ihn herangetragenen Fall zu erhalten. Einer seiner Kunden ist Arzt und bietet individuelle Gesundheitsleistungen und Untersuchungen an. Hierzu muss der Patient einwilligen, dass die Praxis für die Auswertung Informationen von vorherigen Untersuchungen anfordern und zur Auswertung die Daten an einen spezifischen Dritten weitergeben und zurückerhalten darf. Dabei wird der Patient darüber informiert, wer nach seinen Daten angefragt wird und wo die Daten verarbeitet werden.
Die Praxis will die Einwilligung jetzt allerdings dahingehend ändern, dass der Patient nur noch eine pauschale Einwilligung unterschreibt. Somit könnte die Praxis auch nach Abschluss der ersten Untersuchung weiterhin ohne erneute Rückfrage und Einwilligung des Patienten bei den mitbehandelnden Ärzten Daten, Befunde usw. abrufen. Durch die neue Einwilligung könnten alle mit dem Behandlungsfall

verknüpften Daten ohne weitere Zustimmung des Patienten gegebenenfalls lange nach dessen Zustimmung abgefragt werden. Der externe Datenschutzbeauftragte hat dabei Bedenken, da medizinische Daten besonders schützenswert sind.
Der TLfDI informierte darüber, dass der Patient gemäß § 4a Abs. 1 Bundesdatenschutzgesetz (BDSG) auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung der Einwilligung hingewiesen werden muss („informierte Einwilligung“). Sowohl die Verwendungsziele als auch und vor allem die Verarbeitungsfolgen lassen sich erst abschätzen, wenn die jeweils gewünschten Daten genauso wie die Verarbeitungsbedingungen und die potenziellen Übermittlungsempfänger angeben werden. In der vorgesehenen neuen Einwilligung waren diese Angaben nicht erkennbar. Die Einwilligung erfüllte daher nicht die Voraussetzungen des § 4a BDSG. Sie wäre unwirksam.
Zudem müssten die Ärzte, die Patientendaten an die Praxis übermitteln, ebenfalls eine datenschutzrechtliche Einwilligung und eine Schweigepflichtentbindung bei den betroffenen Patienten einholen bzw. der Patient müsste diese Ärzte von ihrer Schweigepflicht entbinden. Dies kann in einer gemeinsamen Erklärung geschehen, in der der Patient eine bestimmte Stelle ermächtigt, zu einem bestimmten Zweck bei einem bestimmten Arzt Informationen einzuholen, und gleichzeitig in die entsprechende Übermittlung einwilligt.
Die Einschätzung des externen Datenschutzbeauftragten war damit völlig richtig gewesen.

Eine Datenübermittlung von Patientendaten durch eine Arztpraxis an einen Dritten ist mit schriftlicher Einwilligung des Patienten möglich. Nach § 4a Abs. 1 BDSG ist die Einwilligung nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Der Patient muss darin auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung hingewiesen werden. Damit der Patient erkennt, wozu seine Daten verwendet werden und wer diese erhält, müssen die konkreten Verarbeitungsbedingungen und die potenziellen Übermittlungsempfänger angegeben werden.

10.15 Erwachsene familienversicherte Patienten sind mündig – eine Erhebung von Hauptversichertendaten entfällt damit!

Eine Bürgerin beschwerte sich darüber, dass eine Zahnarztpraxis ihr anlässlich eines Untersuchungstermins nicht nur ihre eigene, sondern aufgrund der Familienversicherung auch die Krankenversicherten-Karte ihres Ehemanns abverlangte. Die Praxismitarbeiter begründeten dies ihr gegenüber damit, dass das PC-Programm die Daten des Ehemanns für die Rechnungsstellung zwingend benötige.
Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) bat die Zahnarztpraxis um eine Stellungnahme zum vorgetragenen Sachverhalt und um Darlegung der Rechtsgrundlage für die Abfrage der personenbezogenen Daten des Ehemannes. Nach § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG) ist die Erhebung personenbezogener Daten nur zulässig, wenn eine Rechtsvorschrift sie erlaubt oder der Betroffene eingewilligt hat.
Daraufhin informierte die Zahnarztpraxis den TLfDI darüber, dass die Praxis 2016 übernommen worden sei. Im Rahmen der Übernahme sei die Abfrage der familienversicherten Patienten nach dem Hauptversicherten standardisiert mit durchgeführt worden. Auch ein neu eingeführtes Computerprogramm verlangte die Eingabe der Daten des Hauptversicherten, sowohl bei minderjährigen als auch bei erwachsenen Patienten. Den Ärzten sei nicht bewusst gewesen, dass auf die Angabe des Hauptversicherten bei erwachsenen Patienten verzichtet werden kann. Sie waren davon ausgegangen, dass diese Information für die Abrechnung auch bei erwachsenen Patienten notwendig ist.
Im Dezember 2016 installierte die Zahnarztpraxis nach eigener Aussage ein neues Update des Abrechnungsprogramms und entfernte in diesem Zusammenhang die Abfrage nach den Daten des oder der Hauptversicherten bei erwachsenen Patienten.
Der TLfDI teilte der Beschwerdeführerin daraufhin mit, dass die Abfrage nach den Daten der bzw. des Hauptversicherten in der Zahnarztpraxis nun nicht mehr erfolgt, da ein neues Abrechnungsprogramm installiert wurde und dass sich die Mitarbeiter der Praxis für entsprechende Unannehmlichkeiten bei der Beschwerdeführerin entschuldigten. Die Zahnarztpraxis informierte der TLfDI darüber, dass er die Angelegenheit als erledigt ansehe, da die Abfrage der Hauptversichertendaten bei erwachsenen Patienten nun nicht mehr stattfinde.

Die in diesem Falle aufgeworfene Problemstellung zur Abfrage nach Daten der Hauptversicherten bei erwachsenen Patienten sollte nach Auffassung des TLfDI auch mit den Krankenversicherungen diskutiert werden. Daher entschied sich der TLfDI, diese Fragestellung in den Arbeitskreis „Gesundheit und Soziales“ der Datenschutzkonferenz des Bundes und der Länder einzubringen, da die meisten Krankenkassen nicht in die Zuständigkeit des TLfDI fallen.

Nach § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG) ist die Erhebung personenbezogener Daten nur zulässig, wenn eine Rechtsvorschrift sie erlaubt oder der Betroffene eingewilligt hat. Im Falle der Familienversicherung von Patienten ist die Abfrage von Daten der oder des Hauptversicherten durch den Arzt im Behandlungsfall bei erwachsenen Patienten datenschutzrechtlich nicht zulässig, weil sich eine entsprechende Ermächtigungsgrundlage weder im BDSG noch im Sozialgesetzbuch findet.

10.16 Beratung durch den Amtsarzt verstößt nicht gegen den Datenschutz

Ein Vater beschwerte sich über eine Amtsärztin und trug gegenüber dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) vor, die Amtsärztin habe in Bezug auf ihn und in Bezug auf seine Tochter persönliche Daten weitergegeben und damit gegen den Datenschutz sowie gegen die ärztliche Schweigepflicht verstoßen. Der Beschwerdeführer gab an, dass er von der Kindesmutter getrennt lebe und beide Elternteile ein gemeinsames Sorgerecht hätten. Die Kindesmutter habe dem Beschwerdeführer anwaltlich mitteilen lassen, dass sie die Übertragung der elterlichen Sorge begehre. Dem entsprechenden anwaltlichen Schreiben habe nach Information des Beschwerdeführers eine Stellungnahme der Amtsärztin beigelegen, aus der hervorging, dass sie betreffend die Tochter des Beschwerdeführers mit zwei weiteren Kinder- und Jugendärzten kommuniziert habe. Dies stellte nach Ansicht des Beschwerdeführers eine Verletzung des Datenschutzes hinsichtlich der persönlichen Daten seiner Tochter und seiner eigenen als sorgeberechtigtem Elternteil sowie eine Verletzung der ärztlichen Schweigepflicht dar. Der Beschwerdeführer gab an, dass er keine persönliche Einwilligung zur Weitergabe seiner Daten erteilt und die Ärztin auch nicht von ihrer Schweigepflicht entbunden hatte.

Der TLfDI bat die entsprechende Stadtverwaltung um Stellungnahme zum vorgetragenen Vorwurf der Datenschutzverletzung durch die Amtsärztin. Die Stadtverwaltung ergänzte und präzisierte den vom Beschwerdeführer vorgetragenen Sachverhalt. Im Rahmen der Besuchsregelungen zum geteilten Sorgerecht war zwischen dem Beschwerdeführer und der Kindesmutter ein Vergleich geschlossen worden. Gegenstand des Vergleichs war u. a. die Festlegung, dass die Mutter regelmäßig ein amtsärztliches Attest vorlegen musste, wenn ihre Tochter zu Besuchsterminen beim Beschwerdeführer und Vater des Kindes wegen einer Erkrankung nicht reisefähig war. Daher stellte die Kindesmutter die gemeinsame Tochter regelmäßig bei der Amtsärztin vor gemäß § 3 Gesundheitsdienstverordnung (GesDV), wenn sie aufgrund der Vergleichsregelung ein Attest benötigte. Im Rahmen dieser Untersuchung informierte die Kindsmutter die Amtsärztin auch über die zwei weiteren Fachärzte, die ihre Tochter behandelten, über den Grund der ärztlichen Vorstellung sowie über den Namen und die Adresse des Kindesvaters als ebenfalls sorgeberechtigtes Elternteil. In der Folge dieser Information nahmen die drei Ärztinnen im Hinblick auf die Behandlung des Kindes miteinander Kontakt auf. Die damit verbundene Datenübermittlung zwischen den Ärztinnen an die Amtsärztin war zur ordnungsgemäßen Begutachtung des Kindes und seiner Weiterbehandlung notwendig und nach § 28 Abs. 7 Satz 2 Bundesdatenschutzgesetz zulässig.
Der TLfDI teilte dem Beschwerdeführer mit, dass die Amtsärztin ihre Informationen gemäß § 3 GesDV erlangte und diese Informationen vorschriftsmäßig gemäß § 20 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) im Rahmen der Ausübung ihrer fachlichen Aufgabe als Amtsärztin verwendet hat. Neben der Untersuchung des Kindes und der Erstellung der gerichtlich angeordneten ärztlichen Atteste gemäß § 3 GesDV gehört zur amtsärztlichen Aufgabe auch die gesundheitliche Beratung und Aufklärung von Kindern und deren Sorgeberechtigten im Hinblick auf ihre gesundheitliche Entwicklung gemäß § 8 GesDV. Somit konnte der TLfDI keinen Verstoß gegen den Datenschutz durch die Amtsärztin feststellen.

Gemäß § 20 Abs. 1 ThürDSG ist das Speichern, Verändern oder Nutzen personenbezogener Daten zulässig, wenn es zur Erfüllung der in der Zuständigkeit der Daten verarbeitenden Stelle liegenden Aufgaben erforderlich ist und es für die Zwecke erfolgt, für die die

Daten erhoben worden sind. Gemäß § 8 GesDV gehört zur amtsärztlichen Aufgabe auch die gesundheitliche Beratung und Aufklärung von Kindern und deren Sorgeberechtigten im Hinblick auf ihre gesundheitliche Entwicklung.

10.17 Ist die Weitergabe der Personaldaten an die Heimaufsicht erlaubt?

Die Leitung eines Seniorenheimes wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), da sie mit der für sie zuständigen Heimaufsicht uneinig darüber war, ob die Weitergabe von Personallisten datenschutzrechtlich zulässig ist. Nach § 10 Abs. 3 Thüringer Gesetz über betreute Wohnformen und Teilhabe (ThürWTG) sind den zuständigen Behörden, in dem Fall der Heimaufsicht, vor Eröffnung einer Einrichtung die Namen, die berufliche Ausbildung der Pflege- und Betreuungskräfte mit Geburtsjahr, die vorgesehene Tätigkeit und wöchentliche Arbeitszeit sowie quartalweise Änderungen personenbezogener Daten aller Mitarbeiter zu melden. Um diese Angaben zu erhalten, sendet die Heimaufsicht den Heimleitern eine vorgegebene Excel-Liste zu, die diese auszufüllen haben. Damit bestehe die Verpflichtung, jährlich eine Personalliste mit vollem Namen, Geburtsdatum, Ausbildung, Einstand, Tätigkeit und Arbeitsstunden der Mitarbeiter zu melden. Quartalsweise müssen Personaländerungen mit denselben Angaben gemacht werden. Jedoch sei unklar, wie lange die personalisierten Daten gespeichert werden, wer sie einsieht, wie sie verarbeitet werden und wann sie gelöscht werden. Die Heimleitung hatte datenschutzrechtliche Bedenken. Sie sei grundsätzlich bereit, der Heimaufsicht die Personalstärke mitzuteilen, allerding würde sie sich wohler fühlen, die Daten anonymisiert zu versenden, um nicht gegen datenschutzrechtliche Bestimmungen zu verstoßen.

Der TLfDI teilte der Heimleitung mit, dass im Datenschutzrecht gemäß § 4 Abs. 1 BDSG, ein „Verbot mit Erlaubnisvorbehalt“ gelte. Das bedeutet, dass jede Erhebung und Verarbeitung von Daten grundsätzlich unzulässig ist, es sei denn ein Gesetz erlaubt sie bzw. der Betroffene hat eingewilligt.

Das am 24. Juni 2014 in Kraft getretene ThürWTG regelt in § 10 eine Anzeigepflicht von stationären Einrichtungen nach § 2 ThürWTG. Stationäre Einrichtungen im Sinne dieses Gesetzes sind Einrichtungen, die dem Zweck dienen, ältere, pflegebedürftige oder

behinderte oder von Behinderung bedrohte volljährige Menschen aufzunehmen, ihnen Wohnraum zu überlassen sowie mit der Wohnraumüberlassung verpflichtend Pflege- oder Betreuungsleistungen zur Verfügung zu stellen oder vorzuhalten, die in ihrem Bestand von Wechsel sowie Zahl der Bewohner abhängig sind und entgeltlich betrieben werden. Das Gesetz verpflichtet diese Einrichtungen, drei Monate vor der vorgesehenen Inbetriebnahme unter anderem die Namen, die berufliche Ausbildung der Pflege- und Betreuungskräfte mit Geburtsjahr, die vorgesehene Tätigkeit und wöchentliche Arbeitszeit anzuzeigen. Nach Absatz 3 der Vorschrift sind der zuständigen Behörde während des Betriebs quartalsweise Änderungen dieser Angaben anzuzeigen. Eine Begründung für diese gesetzliche Regelung ist in der entsprechenden Landtagsdrucksache (5/7006) zu finden, in der ausgeführt wird, dass die Anzeigepflicht schon nach bisherigem Recht die Aufgabe hatte, die zuständige Behörde über die Aufnahme, Änderung oder Einstellung des Einrichtungsbetriebes zu unterrichten. Dazu benötigt die zuständige Behörde Informationen darüber, ob und wie jemand eine stationäre Einrichtung betreiben will. Der Träger hat sicherzustellen, dass Beschäftigte, vor allem Pflege- und Betreuungskräfte, in ausreichender Zahl vorhanden sind und dass ihre persönliche und fachliche Eignung für die von ihnen zu leistende Tätigkeit ausreicht. Die von der Heimaufsicht geforderten Angaben entsprechen nach Prüfung durch den TLfDI der gesetzlichen Verpflichtung des § 10 ThürWTG und sind damit zulässig. Dies wurde der Heimleitung mitgeteilt.

Im Datenschutzrecht gilt ein sogenanntes Verbot mit Erlaubnisvorbehalt. Das bedeutet, dass jede Erhebung und Verarbeitung von Daten grundsätzlich unzulässig ist, es sei denn ein Gesetz erlaubt sie bzw. der Betroffene hat eingewilligt. § 10 ThürWTG verpflichtet stationäre Einrichtungen, drei Monate vor der vorgesehenen Inbetriebnahme bestimmte personenbezogene Daten der Pflege- und Betreuungskräfte anzuzeigen.

10.18 Datenverarbeitung im Auftrag – ein Klinikum war gut vorbereitet

Ein Klinikum wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und bat um datenschutzrechtliche Bewertung hinsichtlich einer Aktenvernich-

tung. Demnach sollten Patientenakten, Verwaltungsakten, Datenträger und Festplatten vernichtet werden. Die Daten hatten die gesetzliche Aufbewahrungsfrist erreicht. Ebenso übersandte das Klinikum dem TLfDI die Angebote und Zertifikate des Vernichtungsunternehmens, woraus ersichtlich wurde, nach welchen Parametern die Vernichtung erfolgen sollte.
Eine Aktenvernichtung stellt nach § 3 Abs. 4 Nr. 5 Bundesdatenschutzgesetz (BDSG) eine Löschung – das Unkenntlichmachen – von gespeicherten personenbezogenen Daten dar. Nach Informationen des Klinikums erfolgt die Löschung der Daten aber nicht durch das Klinikum selbst, sondern durch eine vom Klinikum beauftragte Firma. In solch einem Fall spricht man von einer Datenverarbeitung im Auftrag nach § 11 BDSG. Dieser besagt, wenn personenbezogene Daten im Auftrag durch andere Stellen erhoben, verarbeitet oder genutzt werden, ist der Auftraggeber für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz verantwortlich. Der Auftragnehmer ist unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftrag ist schriftlich zu erteilen, wobei insbesondere im Einzelnen der Gegenstand und die Dauer des Auftrags, der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen, die nach § 9 BDSG zu treffenden technischen und organisatorischen Maßnahmen, die Berichtigung, Löschung und Sperrung von Daten, die nach Absatz 4 bestehenden Pflichten des Auftragnehmers, insbesondere die von ihm vorzunehmenden Kontrollen, die etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen, die Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers, mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen, der Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält, die Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags festzulegen sind. Der Vertrag zur Auftragsdatenverarbeitung wurde dem TLfDI zur Kenntnis gegeben und nach Prüfung für gesetzeskonform befunden. Ebenfalls teilte das Klinikum mit, dass der Datenschutzbeauftragte den gesamten Vernichtungsprozess begleiten würde, um

unrechtmäßige Kenntnisnahmen der sensiblen Daten bis zur letztlichen Vernichtung zu verhindern.
Das generelle Löschen von personenbezogenen Daten ist im § 35 BDSG geregelt. Absatz 2 Nummer 3 besagt, dass jene Daten zu löschen sind, welche für eigene Zwecke verarbeitet werden, sobald ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist. Hierzu zählt wie in diesem Fall die abgelaufene Aufbewahrungsfrist. Ein besonderes Augenmerk liegt hierbei auf der Art der Daten. Da es sich um Gesundheitsdaten handelt, sind diese Daten nach § 3 Abs. 4 Nummer 9 BDSG als besondere Art der Daten einzustufen und es gilt die DIN 66399 als besondere Regelung für diese Vernichtung. Hierbei sind die zu vernichteten Daten in unterschiedliche Schutzklassen und Sicherheitsstufen einzuordnen. Bei Patientenakten gilt demnach die Schutzklasse 3 und Sicherheitsstufe P5. Das Unternehmen, welches die Akten vernichten sollte, belegte diese Parameter bis ins Detail.
Der TLfDI prüfte das gesamte Vorhaben des Klinikums anhand der Fakten und befand es für datenschutzkonform.

Auch eine Aktenvernichtung stellt nach § 3 Abs. 4 Nr. 5 Bundesdatenschutzgesetz (BDSG) einen datenschutzrelevanten Vorgang dar, nämlich eine Löschung, also das Unkenntlichmachen von gespeicherten personenbezogenen Daten. Auch hier ist auf die datenschutzgerechte Vernichtung und insbesondere auf die unterschiedlichen Schutzklassen und Sicherheitsstufen zu achten, vor allem, wenn es sich wie hier um besondere Arten von personenbezogenen Daten handelt. Eine Datenverarbeitung im Auftrag nach § 11 BDSG liegt vor, wenn personenbezogene Daten im Auftrag durch andere Stellen erhoben, verarbeitet oder genutzt werden. Der Auftraggeber ist für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz verantwortlich. Der Auftragnehmer ist unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftrag ist schriftlich zu erteilen, wobei insbesondere im Einzelnen der Gegenstand und die Dauer des Auftrags, der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen beachtet werden muss.

10.19 Bestellung von Arzneimitteln mit WhatsApp

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichte eine Anfrage eines Apothekenkunden zur datenschutzrechtlichen Zulässigkeit einer Serviceleistung, die in einer Nordthüringer Apotheke angeboten wurde: Arzneimittelvorbestellung mittels WhatsApp. Diese spezielle Dienstleistung wird in den Apothekengeschäften immer beliebter und viele Apotheken bieten ihren Kunden diesen Service an. Sie verkennen dabei jedoch zumeist die datenschutzrechtliche Brisanz dieser Unternehmung. Um mittels WhatsApp die Bestellung aufzugeben, werden die Kunden zumeist dazu aufgefordert, ein Foto vom Rezept oder der Verpackung des bereits vorliegenden Medikamentes zu übersenden. Gleichzeitig werden die Telefonnummer und ggf. auch der Name des Bestellenden übermittelt. Vor allem bei Rezepten handelt es sich um besonders schützenswerte, personenbezogene Daten nach § 3 Abs. 9 BDSG, da Informationen zu den vorliegenden Krankheiten oder dem Gesundheitszustand des Bestellers abgeleitet werden können. Weiterhin wird auch die Telefonnummer als personenbezogenes Datum an WhatsApp und an den Apothekenbetreiber übermittelt. Zusätzlich dazu wird bei der Nutzung von WhatsApp automatisch das lokal hinterlegte Adressbuch des Nutzers mit ausgelesen und alle diese Kontaktdaten ungefragt an WhatsApp übertragen und auf den Servern in Kalifornien/USA gespeichert. Was schlussendlich mit diesen Daten passiert, weiß kein Mensch. Denn trotz der mittlerweile plattformunabhängigen Ende-zu-Ende-Verschlüsselung von Text und Bilddaten erhält WhatsApp Kenntnis von den Meta-Daten (IP-Adresse, Geräte-ID, Zeitpunkt usw.) Auch aus diesen Daten können Nutzerprofile erstellt werden, Kaufverhalten analysiert und weitere Rückschlüsse auf die Chatbeteiligten gezogen werden. Schlussendlich bleiben vor Ort in der Apotheke noch wichtige Fragen zu klären: Wie ist das Empfangsgerät des Apothekers geschützt? Wer hat Zugriff auf die übermittelten Rezept-Daten? Werden die übermittelten Fotos nach dem Empfang und der Auswertung wieder gelöscht? Die Handhabung der von den Kunden empfangenen, besonders schützenswerten Daten, obliegt den Apotheken. Diese müssen technisch-organisatorische Maßnahmen zur Datensicherheit treffen und umsetzen. Trotz allem ist die Bestellung per WhatsApp ein datenschutzrechtliches Wagnis, da aufgrund der Übertragung der

Daten in die USA deren weitere Nutzung völlig unklar ist und auch ob die Verschlüsselung an sich von Dauer ist.

Aufgrund der Bequemlichkeit des Bestellvorgangs über WhatsApp sind viele Apotheken daran interessiert gewesen, ihren Kunden diese Bestellmöglichkeit anbieten zu können. Die datenschutzrechtlichen Bedenken, die sich aufgrund der Übermittlung an WhatsApp ergeben, wurden seitens der Apotheker oft übersehen. Daher wurde vom TLfDI in Zusammenarbeit mit dem Apothekerverband auf das Problem aufmerksam gemacht und es wurden die datenschutzrechtlichen Bedenken erörtert und die Apotheker dafür sensibilisiert. Die Prüfung ist beim TLfDI jedoch noch nicht abgeschlossen.

10.20 Wearables und Gesundheits-Apps immer datenschutzkonform?

Einer repräsentativen Umfrage durch die Bitkom Research GmbH zufolge soll bereits knapp ein Drittel der Bevölkerung ab 14 Jahren sogenannte Fitness-Tracker zur Aufzeichnung von Gesundheitswerten und persönlichen Verhaltensweisen nutzen. Die 91. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder hatte deshalb in ihrer Entschließung im April 2016 „Wearables und Gesundheits-Apps – Sensible Gesundheitsdaten effektiv schützen!“ ihre Vorstellungen diesbezüglich veröffentlicht.
So weist die Konferenz darauf hin, dass zahlreiche Wearables und Gesundheits-Apps die aufgezeichneten Daten an andere Personen oder Stellen weiter geben, ohne dass die betroffenen Personen hiervon wissen oder dazu eine bewusste Entscheidung treffen. Zudem müssen die Grundsätze der Datenvermeidung und Datensparsamkeit beachtet werden. Dies sieht auch Artikel 25 der ab 25. Mai 2018 wirksam werdenden Datenschutzverordnung (DS-GVO) vor.
Zudem ist die Konferenz u. A. der Meinung, dass, wer aus eigenen Geschäftsinteressen gezielt bestimmte Wearables und Gesundheits-Apps in Umlauf bringt oder ihren Vertrieb systematisch unterstützt, eine Mitverantwortlichkeit für die rechtmäßige Ausgestaltung solcher Angebote trägt. Nicht zuletzt bezweifelt sie die Rechtmäßigkeit bei Einwilligungserklärungen etwa in Beschäftigungs- und Versicherungsverhältnissen (siehe Anlage 2).

Wearables und Gesundheits-Apps erfahren derzeit einen wirtschaftlichen Aufschwung. Dennoch muss jederzeit der Datenschutz gewährleistet sein. Eine Mitverantwortlichkeit für die rechtmäßige Ausgestaltung solcher Angebote trägt auch der Entwickler und der Betreiber solcher Angebote. Deshalb ist bereits in der Planung und Entwicklung von IT-Systemen Datenschutz und Datensicherheit zu berücksichtigen (Data protection by design). Die IT-Systeme müssen zudem datenschutzfreundlich so voreingestellt sein, dass nur die personenbezogenen Daten verarbeitet werden, die für den verfolgten Zweck erforderlich sind (Data protection by default).

10.21 Beschwerde über ein Reinigungsunternehmen wegen nicht korrekt vernichteter Nachweisblätter

Im Berichtszeitraum wurde der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) darauf aufmerksam gemacht, dass Nachweislisten eines Reinigungsunternehmens mit personenbezogenen Daten nicht datenschutzgerecht vernichtet und entsorgt würden.
Auf Nachfrage gab das Reinigungsunternehmen an, dass es mit der Nachweisliste die geleistete Dienstleistung dokumentiert und diese bei der Abrechnung nutzt. Die vor Ort tätigen Mitarbeiter führen die Listen, auf denen das Datum, die Uhrzeit und eine Kennnummer des Reinigungsobjekts notiert werden. Jede Reinigung wird einzeln mit einer Unterschrift abgezeichnet. Zu Abrechnungszwecken wird diese Liste dann digital eingelesen und die Papierbelege werden nach erfolgter Rechnungslegung in der Müllpresse entsorgt. Hierfür werden die Listen in Müllsäcken gesammelt, mit einem Kabelbinder verschlossen und in der Müllpresse verpresst.
Der TLfDI nahm zu diesem Ablauf Stellung und bemängelte, wie die Entsorgung der Nachweispapiere von-statten-geht, da sie personenbezogene Daten enthalten. Personenbezogene Daten sind nach § 3 Bundesdatenschutzgesetz (BDSG) Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person. Mit den auf der Nachweisliste aufgeführten Uhrzeiten und dem Namen des Mitarbeiters, könnte man nachverfolgen, wann sich die Person an welchem Ort aufgehalten hat. Gemäß § 4 Abs. 1 BDSG ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit das BDSG oder eine andere Vorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt

hat. Das Löschen ist auch eine Art der Verarbeitung. Gemäß § 3 Abs. 4 Nr. 5 BDSG ist das Löschen das Unkenntlichmachen gespeicherter personenbezogener Daten.
Nach § 35 Abs. 2 Satz 2 Nr. 3 BDSG sind personenbezogene Daten zu löschen, wenn sie für eigene Zwecke verarbeitet worden sind und ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist. Im vorliegenden Fall wäre das nach der Rechnungslegung.
Allerdings erfolgt hier keine Löschung. Bei einer datenschutzkonformen Löschung muss sichergestellt werden, dass die enthaltenen personenbezogenen Daten zerstört werden. Eine Müllpresse kann diese Anforderungen nicht erfüllen, da die Daten nachvollziehbar bleiben. Eine Unkenntlichmachung in Form von Schreddern der Listen ist notwendig, um diese datenschutzkonform zu löschen. Hinsichtlich der notierten Daten ist für die Vernichtung der Listen mindestens ein Schredder der Sicherheitsstufe P-3 entsprechend der DIN 66399 ausreichend. Das Unternehmen hat auf die Stellungnahme des TLfDI hin mitgeteilt, dass es zukünftig die Datenblätter datenschutzkonform entsorgen wird und hierzu eigens ein Schredder in der gewünschten Sicherheitsstufe angeschafft würde.

Personenbezogene Daten sind nach § 3 BDSG Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person. Enthalten Dokumente personenbezogene Daten muss bei der Vernichtung darauf geachtet werden, dass sie unleserlich werden. Je nach Art der gespeicherten Daten muss hierfür ein Schredder mit der entsprechenden Sicherheitsstufe genutzt werden.

10.22 Urkundenverifikationsdienst Approbationsurkunden

Bereits im 11. Tätigkeitsbericht berichtete der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) über den Einsatz einer Technik zur Verifikation von Approbationsurkunden von Ärzten und Fachkräften in Pflegeberufen. Es ging dabei darum, dass Patienten die Echtheit einer Approbationsurkunde eines Arztes prüfen können, ohne sich an die Landesärztekammer Thüringen wenden zu müssen. Das Verfahren läuft wie folgt ab: Seit 2016 stellt das Thüringer Landesverwaltungsamt Approbationsurkunden mit einem QR-Code versehen aus. Ein QR-Code (von Quick Response) ist ein zweidimensionales Bild, in dem bestimmte

Informationen hinterlegt sind. Diese können mithilfe eines sogenannten QR-Code-Scanners abgerufen werden, der beispielsweise als App auf das Smartphone geladen kann. Besitzer eines Smartphones können den QR-Code auf diesen „neuen“ Urkunden scannen, der einen 64-stelligen Code (Buschstaben und Zahlen) enthält, mit welchem jede Person mit Internetzugang auf dem Portal https://www.kammerservice.de unter Eingabe dieses Codes die Echtheit der Urkunde prüfen kann.



Bereits im letzten Tätigkeitbericht wurde berichtet, dass das Verfahren zur Generierung des 64-stelligen Codes den Datenschutzanforderungen entspricht. Im aktuellen Berichtszeitraum hatte der TLfDI weiterhin geprüft, wer Zugriff auf die Daten der Urkunden hat und wie diese vor Veränderung geschützt sind. Da die Landesärztekammer Thüringen, welche das Verifikationsportal mit anderen Ärztekammern in Deutschland betreibt, nicht die Stelle ist, die Urkunden selbst ausstellt, werden nur digitale Kopien des Urkundeninhalts bereitgestellt.

Wichtig aus datenschutzrechtlicher Sicht war, dass bei Übertragung der Kopien keine Datenveränderung durch Unbefugte (Hacker, böswillige Angestellte) stattfinden kann und das zum zweiten eine Sicherung der Daten gegen Zerstörung (auch hier durch Hacker bzw. technisches Versagen der Rechentechnik) gegeben ist.

Zum ersten Punkt der Sicherstellung der Integrität der Daten hat der TLfDI eine Lösung mit dem Thüringer Landesverwaltungsamt und der Landesärztekammer Thüringen abgestimmt und Verbesserungsvorschläge eingebracht, wie die zu übermittelnden Daten zusätzlich zum Übertragungsweg sicher verschlüsselt werden können. Zum zweiten Punkt (Schutz vor Datenverlust) trägt das Thüringer Landesverwaltungsamt die Verantwortung für die Richtigkeit der Urkundendaten. Hier muss dem TLfDI zurzeit noch ein schlüssiges Konzept zur Datensicherung nachweisen werden.

Jede öffentliche Stelle bzw. nicht-öffentliche Stelle ist verpflichtet, beim Umgang mit personenbezogenen Daten in technischen Systemen die Daten vor unerlaubter Manipulation und vor Datenverlust zu schützen. Dabei kann es je nach Schutzbedarf der betroffenen Daten

erforderlich sein, nicht nur den Übertragungsweg bei einer Übermittlung zu verschlüsseln, sondern auch die Daten selbst.



Stempel 2 Datenschutz - © S. Engels / Fotolia.com

11 Ordnungswidrigkeiten

11.1 Bußgelder nehmen stetig zu

Wie in den vergangenen Tätigkeitsberichten dargestellt, ist der Thüringer Landesbeauftragte für den Datenschutz und die Informations-

freiheit (TLfDI) seit Übertragung der Zuständigkeit „Aufsichtsbehörde für den nicht-öffentlichen Bereich“ auch zuständige Ordnungswidrigkeitenbehörde für Ordnungswidrigkeiten nach § 43 Bundesdatenschutzgesetz (BDSG).

Das Ordnungswidrigkeitenverfahren ist eine besondere Unterart des Verwaltungsverfahrens. Es ist streng von anderen Verfahren zu trennen. Im Unterschied zum grundsätzlich formfreien Verwaltungsverfahren handelt es sich um ein streng formalisiertes Verfahren mit vielen Parallelen zum strafrechtlichen Ermittlungsverfahren. Ziel des Verfahrens ist es, Verstöße gegen das Bundesdatenschutzgesetz zu ahnden und auf diesem Wege eine Änderung im Verhalten des Verstoßenden zu erreichen. Im Wesentlichen teilt sich die Befugnis des TLfDI in Ordnungswidrigkeiten wegen eines Verstoßes gegen Formalien des BDSG sowie gegen inhaltliche Verstöße auf. Erstere können mit einem Bußgeld bis zu 50.000 Euro, Letztere mit bis zu 300.000 Euro geahndet werden. Dabei wird die Höhe der Geldbuße durch die Bedeutung der Ordnungswidrigkeit und den Vorwurf, der den Täter trifft, bestimmt, aber bis zu einem gewissen Maße auch durch die finanzielle Leistungsfähigkeit des Täters. An die eben genannten Obergrenzen ist der TLfDI allerdings dann nicht gebunden, wenn der zu ahndende Verstoß einen finanziellen Vorteil erwirtschaftet hat, der über diese Obergrenzen hinausgeht. Dieser Vorteil kann dann ebenfalls abgeschöpft werden. Rechtswidriges Verhalten soll sich ja nicht lohnen.

Die Integration des Bußgeldverfahrens beim TLfDI ist abgeschlossen. Es wird aber immer noch daran gearbeitet, dessen Effizienz zu optimieren. Dies ist auch notwendig, weil der TLfDI in der Vergangenheit mit komplexen Verfahren konfrontiert war und in Zukunft bestimmt auch sein wird.

Während im letzten Berichtszeitraum Geldbußen in Höhe von insgesamt knapp über 13.000 Euro verhängt wurden, steigt dieser Betrag für diesen Berichtszeitraum auf über 45.000 Euro. Eine Entwicklung, die hinsichtlich des Datenschutzes auch mit Sorge beobachtet wird, da ein Grund hierfür schwere Verstöße waren, die mit hohen Bußgeldern geahndet werden mussten.

Schwerpunkt der Verfolgung waren die Nichtbestellung von betrieblichen Datenschutzbeauftragten trotz bestehender gesetzlicher Verpflichtung, § 42 Abs. 1 Nr. 2 BDSG, sowie unbefugtes Erheben oder Verarbeiten von personenbezogenen Daten nach § 43 Abs. 2 Nr. 2 BDSG.

Wird eine vorsätzliche Handlung, die nach § 43 Abs. 2 BDSG eine Ordnungswidrigkeit darstellt, gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, begangen, handelt es sich um eine Straftat. Diese zu verfolgen, ist der TLfDI nicht befugt. Vielmehr verfolgt die jeweils zuständige Staatsanwaltschaft die Tat auf Antrag. Neben dem Opfer und der verantwortlichen Stelle selbst, sind die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit und auch der TLfDI in solchen Fällen antragsberechtigt.
Hiervon musste der TLfDI im Berichtszeitraum glücklicherweise nur einmal Gebrauch machen.
Ab Ende Mai 2018 wird die Datenschutz-Grundverordnung (DS-GVO) in Europa und damit auch in Deutschland Geltung erlangen. Dies führt nicht nur zu Änderungen im Datenschutzrecht, sondern auch zu Änderungen bei den Bußgeldern. Die Bußgelder für formale Verstöße erhöhen sich auf 10.000.000 Euro, für materielle Verstöße auf 20.000.000 Euro!



Datenschutz - © Marco 2811 / Fotolia.com

12 Technischer und organisatorischer Datenschutz

12.1 Windows 10, Microsoft-Cloud Deutschland und Windows Office 365

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) ist per Gesetz durch das Thüringer Datenschutzgesetz (ThürDSG) verpflichtet, die Entwicklung und Nutzung der Informations- und Kommunikationstechnik, insbesondere der automatisierten Datenverarbeitung und ihrer Auswirkungen auf die Arbeitsweise und die Entscheidungsbefugnisse der öffentlichen Stellen, zu beobachten (§ 40 Abs. 5 ThürDSG). Gerade zu den oben genannten Themen erreichen den TLfDI auch Anfragen, und Reaktionen des TLfDI hierauf sollen kurz dargestellt werden:

Windows 10:

Für die Microsoft Deutschland GmbH ist die zuständige datenschutzrechtliche Aufsichtsbehörde das Bayerische Landesamt für Datenschutzaufsicht (BayLDA).

Da aber auch beim TLfDI Anfragen zum datenschutzgerechten Einsatz von Windows 10 eingingen, stellte der TLfDI im Juni 2016 eine kurze Handreichung auf seiner Website zur Verfügung (siehe https://www.tlfdi.de/mam/tlfdi/themen/windows_10.pdf).



Microsoft-Cloud Deutschland:

Die Microsoft Deutschland GmbH betreibt in Deutschland zwei deutsche Rechenzentren, mit der T-Systems, einer Tochter-Gesellschaft der Deutschen Telekom, als Datentreuhänder. Dies bedeutet, dass die T-Systems gegenüber dem Kunden vertraglich sicherstellt, dass Daten nicht Dritten offengelegt werden. Nach Angaben der T-Systems kann somit die Herausgabe der Daten nur der Kunde selbst verlangen oder auf einer deutschen Rechtsgrundlage beruhen. Nach derzeitigem Stand geht die T-Systems davon aus, dass somit ausländische Behörden keine Herausgabe der Daten verlangen können.

Ziel der Microsoft-Cloud Deutschland ist es, den Kunden dieser Cloud auf Wunsch hin anzubieten, dass die Daten in den Rechenzentren in Deutschland verbleiben.

Die unabhängigen Datenschutzbeauftragten des Bundes und der Länder sind bezüglich der Microsoft-Cloud Deutschland derzeit im Gespräch, um datenschutzrechtliche Fragen zu klären. Siehe hierzu auch Nummer 2.1 des 13. Tätigkeitsberichts für den öffentlichen Bereich. Ein gemeinsamer Dialog wird sich sicherlich fortsetzen.

Microsoft-Office 365:

Der TLfDI als Vorsitzender des Arbeitskreises „Bildung und Datenschutz“ der unabhängigen Datenschutzbeauftragten des Bundes und der Länder prüft derzeit, ob Microsoft Office 365 für Schulen datenschutzgerecht einsetzbar ist.

Am Anfang bezog sich der Prüfungsbereich auf den Einsatzbereich im rein pädagogischen Kontext. Mittlerweile steht zudem die Frage im Raum, ob nicht auch Schulen für ihre eigene Verwaltung Microsoft Office 365 nutzen dürfen. Eine Antwort auf die letzte Frage interessiert natürlich auch Verwaltungen anderer öffentlicher und nicht-öffentlicher Stellen.

Die unabhängigen Datenschutzbeauftragten des Bundes und der Länder beobachten weiterhin die Entwicklungen verschiedener

Microsoft-Produkte. Jegliche Anwendungen müssen zudem der DS-GVO standhalten.

12.2 Kritische Infrastruktur – Sektor Gesundheit

Im Juni 2016 legten Kriminelle per Hackerangriff das Lukas-Krankenhaus in Neuss mit einer Erpresser-Botschaft lahm. Kaum ein Nachrichtenkanal berichtete nicht davon.
Schon lange sind IT-Systeme von Krankenhäusern derartigen Angriffen ausgesetzt, in letzter Zeit häufen sich derartige Attacken.
Nach einer Meldung des WDR traf es danach weitere Krankenhäuser, unter anderem das Klinikum Arnsberg.
Der Vorteil des Einzugs der digitalen Gesellschaft ist auch im medizinischen Bereich nicht von der Hand zu weisen. Aber mit dem Einzug dieser modernen Technik werden gleichzeitig auch neue Angriffspunkte ermöglicht.
Das seit Juli 2015 gültige Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) hat zum Ziel, bei Kritischen Infrastrukturen die Sicherheit informationstechnischer Systeme zu erhöhen. Im April 2016 wurde dann eine BSI-Kritisverordnung (BSI-KritisV) in Kraft gesetzt, die die Sektoren Energie, Wasser, Ernährung, Informationstechnik und Telekommunikation als Kritische Infrastrukturen einstuft, also Bereiche, deren Ausfall dramatische Folgen für Wirtschaft, Staat und Gesellschaft in Deutschland hätte. Im Juni 2017 wurde die BSI-KritisV dann um die Sektoren Gesundheit, Finanz- und Versicherungswesen, Transport und Verkehr erweitert.
Somit sind nun auch Betreiber dieser Sektoren angehalten, IT-Sicherheit nach dem „Stand der Technik“ umzusetzen und erhebliche IT-Sicherheitsvorfälle an das Bundesamt für Sicherheit in der Informationstechnik zu melden.

Die BSI-Kritisverordnung (BSI-KritisV) regelt, welche Sektoren derzeit als Kritische Infrastruktur eingestuft sind. Bereits nach einem Jahr wurden die Sektoren Gesundheit, Finanz- und Versicherungswesen, Transport und Verkehr nachträglich aufgenommen, da diese 2016 einem hohen Gefährdungspotenzial ausgesetzt waren und deren Folgen bei Ausfall neu bewerten wurden.

12.3 Heiße Debatte um den Entwurf einer EU-e-Privacy-Verordnung

Am 25. November 2009 beschlossen das Europäische Parlament und der Rat der Europäischen Union mit der Richtlinie 2009/136/EG unter anderem Änderungen über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation. Diese e-Privacy-Richtlinie, auch unter „Cookie-Richtlinie“ bekannt, regelt im Wesentlichen in Artikel 5 Absatz 3 die Verwendung von Cookies.
Die zusätzliche Richtlinie war damals ein Ergebnis der Überprüfung der Richtlinie 2002/58/EG („e-Datenschutz-Richtlinie“).
Entsprechend dem Erwägungsgrund 173 i. V. m. Artikel 95 der neuen Datenschutz-Grundverordnung (DS-GVO) sollte die Richtlinie 2002/58/EG nochmal einer Überprüfung unterzogen werden, sobald die DS-GVO angenommen wurde, um insbesondere die Kohärenz mit der DS-GVO zu gewährleisten.
Seit dem 10. Januar 2017 liegt nun ein Entwurf einer e-Privacy-Verordnung der Europäischen Kommission vor. Der Begründung zum Entwurf kann man entnehmen, dass seit der letzten Überprüfung der e-Datenschutz-Richtlinie im Jahr 2009 sich wichtige technische und wirtschaftliche Entwicklungen auf dem Markt vollzogen haben. So heißt es: „Anstatt herkömmliche Kommunikationsdienste zu nutzen, verlassen sich Verbraucher und Unternehmen zunehmend auf neue Internetdienste, die eine interpersonelle Kommunikation ermöglichen, z. B. VoIP-Telefonie, Sofortnachrichtenübermittlung (Instant-Messaging) und webgestützte E-Mail-Dienste. Solche Over-the-Top-Kommunikationsdienste („OTT-Dienste“) werden aber im Allgemeinen vom gegenwärtigen Rechtsrahmen der Union für die elektronische Kommunikation, einschließlich der e-Datenschutz-Richtlinie, nicht erfasst. Folglich hat die Richtlinie mit der technischen Entwicklung nicht Schritt gehalten, was zu einem mangelnden Schutz der über solche neuen Dienste abgewickelten Kommunikation führt.“
Weiterhin liefert der Entwurf der Verordnung die Begründung gleich mit, warum es nun eine Verordnung und keine Richtlinie werden soll: „Die Kommission legt einen Vorschlag für eine Verordnung vor, um die Kohärenz mit der Datenschutz-Grundverordnung (DS-GVO) sowie Rechtssicherheit gleichermaßen für Nutzer und Unternehmen dadurch zu gewährleisten, dass eine unterschiedliche Ausle-

gung in den Mitgliedstaaten vermieden wird. Eine Verordnung kann in der gesamten Union ein gleiches Schutzniveau für die Nutzer und niedrige Einhaltungskosten für grenzüberschreitend tätige Unternehmen sicherstellen."

Geplant ist, dass die Verordnung, zum gleichen Zeitpunkt wie die DS-GVO wirksam wird, also zum 25. Mai 2018. Ob der Termin gehalten werden kann, hängt stark davon ab, wie die einzelnen Gremien und betroffenen Wirtschaftsunternehmen Einfluss auf den Entwurf nehmen werden, denn die neuen Regelungen z. B. für das Online- und Direktmarketing, haben beträchtliches Diskussionspotenzial. Man erinnere sich daran, wie lange es gedauert hat, bis die DS-GVO verabschiedet wurde.

Auch die Artikel-29-Gruppe der EU-Datenschutzbeauftragten veröffentlichte ihre Kritikpunkte zum Entwurf der EU-Kommission. So dürften beispielsweise Analysen von Metadaten und Inhaltsdaten nur erfolgen, wenn alle Endnutzer ausdrücklich eingewilligt haben. Auch sieht die Artikel-29-Gruppe die allgemeinen Browsereinstellungen als Grundlage einer Einwilligung für Cookies als unzureichend an, da dies nicht der Informationspflicht gemäß Artikel 7 DS-GVO entspricht. Bezüglich des Trackings äußerte die Artikel-29-Gruppe z. B. Änderungswünsche dahingehend, dass Angebote von Websites oder Diensten nur erlaubt seien, wenn diese den Zugang auch ohne Tracking ermöglichen. Zudem ist sie der Meinung, dass bei WiFi- und Bluetooth-Tracking eine Information darüber nicht ausreiche, da die DS-GVO i. d. R. eine Einwilligung verlange.

Man wird abwarten müssen, welche Entwicklung der Entwurf der Verordnung noch nehmen wird.

Entsprechend Erwägungsgrund 173 i. V. m. Artikel 95 der Datenschutz-Grundverordnung, sollte, sobald die DS-GVO angenommen wurde, die Richtlinie 2002/58/EG einer Überprüfung unterzogen werden, um insbesondere die Kohärenz mit der DS-GVO zu gewährleisten. Geplant ist, dass die EU-e-Privacy-Verordnung zum gleichen Zeitpunkt wie die DS-GVO wirksam wird, also zum 25. Mai 2018. Wird der Termin nicht gehalten, gelten für die Übergangszeit die DS-GVO und die e-Privacy-Richtlinie 2002/58/EG in Verbindung mit der jeweiligen nationalen Umsetzung.

12.4 Datenschleudern – vom vernetzten Auto

Vor einigen Jahren waren die Fahrzeuge nur reines Transportmittel, dessen Zweck es war, Personen von einem Ort zu einem anderen zu transportieren. Durch den Fortschritt in der digitalen Regelung und Steuerung zog zunehmend die Digitaltechnik auch in die Fahrzeuge ein. Heutzutage sind in Fahrzeugen zahlreiche Computersysteme verbaut, die die Funktion der einzelnen Komponenten überwachen (z. B. Bremsen, Motorsteuerung, Sitzverstellung, Entertainment-System, Navigationssystem) und Daten untereinander austauschen. Seit ca. 1970 können so Fehlerberichte über die einheitliche Schnittstelle ODB-II durch Werkstätten ausgelesen bzw. Speicher zurückgesetzt werden. Die Anzahl der berechtigten Personen, die Zugriff auf die generierten Daten besaßen, war im Regelfall überschaubar.
All dies ändert sich seit einigen Jahren.
Bereits im 10. Tätigkeitsbericht (2012/2013) berichtete der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit über das europäische Vorhaben, bordeigene eCall-Systeme in allen Fahrzeugen der Mitgliedstaaten verbindlich vorzuschreiben. Schon damals war erkennbar, dass in einer weiteren Ausbaustufe neben den Basisdaten zusätzliche Angaben hinzukommen werden, die z. B. Versicherungsgesellschaften, Kraftfahrzeug-Callcenter, Gesundheitsdienste, Rechtsanwälte oder Automobilclubs interessieren werden (siehe 10. Tätigkeitsbericht, Punkt 3.2). Entsprechend der EU-Verordnung 2015/758, müssen nun ab April 2018 alle Neuwagen mit eCall-Systemen ausgestattet werden. So bereitet sich die Wirtschaft seit Jahren darauf vor.
Durch das praktisch flächendeckend verfügbare Datennetz des Mobilfunks ist nun auch eine dauerhafte mobile Erreichbarkeit der Fahrzeuge gegeben.
Die Digitalisierung hat aber auch im Fahrzeug selbst Einzug gehalten. Laptops, Handys usw. können mit dem elektronischen Multimediacenter, sogenannte Infotainmentsysteme, im Fahrzeug bestens kommunizieren, fast so, als wäre man in einer modern ausgerüsteten Wohnstube auf vier Rädern. Wer kennt dies nicht? Steigt man in ein modernes Fahrzeug ein, kann man sich heutzutage schon oft mit mobilen Geräten, z. B. mit seinem Smartphone, mit dem Multimediacenter des Fahrzeuges verbinden und alle Kontakte des Smartphones vom Fahrzeug aus anrufen oder die auf dem Smartphone gespei-

cherte Musik oder Videos abspielen. Dabei werden die Telefonkontakte oft komplett auf das Multimediacenter übertragen.
Vor einiger Zeit haben Hersteller wie Apple und Google sogar Möglichkeiten geschaffen, Apps das Smartphone vom Touch-Display des Fahrzeugs bedienen zu können. Ebenso bieten nun auch schon die Automobilhersteller eigene App-Anwendungen an. Moderne Infotainmentsysteme bieten bereits Apps auf herstellerspezifischen App-Stores an und erlauben die Individualisierung des Erlebnisses Autofahren. Viele Fahrzeuge bringen auch ihre eigene Datenverbindung ins Mobilfunknetz gleich mit und können somit z. B. direkt mit dem Fahrzeughersteller kommunizieren. Das zukünftige Fahrzeug wird also ein vernetztes Fahrzeug sein – bzw. ist es zum Teil schon heute.
So komfortabel wie es ist, in den oben genannten Beispielen fallen große Mengen an Daten an. Also zum einen Daten über das Fahrzeug selbst und das Fahrverhalten, und zum anderen durch den Nutzer selbst, veranlasst aufgrund des Kontaktes zum Multimediacenter. So fallen z. B. Daten an zur Motordrehzahl, Bremsverhalten, Beschleunigungsverhalten, Füllstand des Tanks, Ausschlag der Stoßdämpfer, Navigationszielen, aktuellem Standpunkt und aktueller Geschwindigkeit, Fahrtrichtung, Insassenzahl, Kamerabildern von Rückfahrt- und Frontkameras, Abstandssensoren usw. – die Liste ließe sich noch lange fortsetzten. Zum anderen können evtl. auch Daten von Nutzern erfasst werden, die sich in diesem Fahrzeug befinden und mit ihren Geräten mit dem Multimediacenter gewollt oder nicht gewollt in Kontakt stehen (z. B. indem Verbindungen gespeichert werden oder Gerätekennungen auch bei nichtaktiver Verbindung ausgelesen werden).
Das Problem ist, dass viele dieser Daten einen „Personenbezug“ aufweisen und durch ihre Analysen sogar ein Verhaltensprofil erstellt werden kann. Aus den Daten kann beispielsweise der Fahrstil des Fahrers (und dessen Risikobereitschaft), die Übertretung von Verkehrsregeln und natürlich auch der Verlauf von Aufenthaltsorten, wie z. B. die Route des letzten Urlaubs oder der Dienstreisen, ermittelt werden.
Die Versicherungsbranche und auch die Wirtschaft sehen bereits seit Jahren ein großes Marktpotential bezüglich der Auswertung solcher Daten. Ihre Geschäftsmodelle und die Wertschöpfung werden sich im Rahmen der digitalisierten Fahrzeuge zukünftig enorm auf den digitalen Mobilitätsbereich erweitern. Die vom Bundesministerium für Verkehr und digitale Infrastruktur veröffentlichte Studie „‚Eigen-

tumsordnung‘ für Mobilitätsdaten“ vom August 2017 gibt einen ersten Eindruck, wohin die Reise zukünftig gehen könnte (siehe http://www.bmvi.de/SharedDocs/DE/Artikel/DG/studie-mobilitaetsdaten-fachkonsultation.html).

So gilt es beispielsweise dringend zu klären, welche Daten überhaupt erforderlich sind, wem eigentlich die in einem Fahrzeug anfallenden Daten gehören, wer also „Eigentümer“ (oder Verfügungsberechtigter) dieser Daten und somit auch datenschutzrechtlich verantwortlich für diese ist, und wer sie wann nutzen darf.

Ab dem 25. Mai 2018 tritt zudem die Europäische Datenschutz-Grundverordnung (DS-GVO) in Kraft. So regelt beispielsweise Artikel 25 DS-GVO, dass Datenschutz und Datensicherheit bereits in der Planung und Entwicklung von IT-Systemen berücksichtigt werden müssen (Data protection by design) und IT-Systeme datenschutzfreundlich so voreingestellt sein müssen, dass nur die personenbezogenen Daten verarbeitet werden, die für den verfolgten Zweck erforderlich sind (Data protection by default).

Auch auf die zukünftige Umsetzung des Artikels 6 DS-GVO, Rechtmäßigkeit der Verarbeitung, darf man gespannt sein. Die Erfassung und Weitergabe der Daten bedürfen immer einer Erlaubnisnorm oder einer Einwilligung. Auch das „Recht auf Vergessenwerden“ (Artikel 17 DS-GVO) oder das Auskunftsrecht über die betreffenden Daten (Artikel 20 DS-GVO), ist umzusetzen. Man darf gespannt sein, insbesondere bei Carsharing-Lösungen.

Es gibt also noch viel zu tun, damit Daten in Fahrzeugen datenschutzgerecht verarbeitet werden. Wünschenswert ist dabei u. A., dass Fahrzeughalter oder Fahrzeugnutzer grundsätzlich über die Weitergabe und die Verwendung ihrer anfallenden Fahrzeugdaten selbst entscheiden können.

So weist auch die vom Bundesministerium für Verkehr und digitale Infrastruktur eingesetzte „Ethik-Kommission zum automatisierten Fahren“ in ihrem Bericht vom Juni 2017 daraufhin, dass Geschäftsmodelle, die sich diese anfallenden Daten zunutze machen, ihre Grenze in der Autonomie und Datenhoheit der Verkehrsteilnehmer finden. Fahrzeughalter oder Fahrzeugnutzer sollten grundsätzlich über die Weitergabe und die Verwendung ihrer anfallenden Fahr-

zeugdaten entscheiden können. Die Freiwilligkeit solcher Datenpreisgabe setzt das Bestehen ernsthafter Alternativen und Praktikabilität voraus. Einer normativen Kraft des Faktischen, wie sie etwa beim Datenzugriff durch die Betreiber von Suchmaschinen oder sozialen Netzwerken vorherrscht, so die Ethik-Kommission, sollte frühzeitig entgegengewirkt werden. Weiterhin führt die Ethik-Kommission in ihren 20-Ethik-Leitlinien aus, dass klar unterscheidbar sein muss, ob ein fahrerloses System genutzt wird oder ein Fahrer mit der Möglichkeit des „Overrulings“ Verantwortung behält. Dabei muss bei nicht fahrerlosen Systemen die Mensch/Maschine-Schnittstelle so ausgelegt werden, dass zu jedem Zeitpunkt klar geregelt und erkennbar ist, welche Zuständigkeiten auf welcher Seite liegen, insbesondere auf welcher Seite die Kontrolle liegt. Für die dazu notwendige Protokollierungs- und Dokumentationspflicht ist eine internationale Standardisierung anzustreben.

Auch die 39. Internationale Konferenz der Beauftragten für den Datenschutz und die Privatsphäre forderte in ihrer Entschließung vom 25. bis 29. September 2017 die Hersteller, Behörden und Anbieter fahrzeugbezogener Dienste auf, u. A.

- sichere Datenspeicher bereitzustellen, um Zugriffe steuern zu können,
- Technologien zu entwickeln, die unzulässige Zugriffe und das Mitschneiden von persönlichen Daten bei Fahrzeugen, Infrastrukturen und Einrichtungen verhindern,
- technische Maßnahmen bereitzustellen, die Cyberangriffe verhindern,
- die Datensparsamkeit zu beachten und die Datenlöschung nach einer gewissen Zeit zu gewährleisten und z. B. auch
- eine Datenschutz-Folgeabschätzung für neue, innovative oder riskante Entwicklungen durchzuführen.

Mobilität 4.0, so wird die Digitalisierung der Mobilität oft genannt, um den Komfort und die Verkehrssicherheit zu erhöhen, darf nicht auf Kosten des Rechts auf informationelle Selbstbestimmung gehen. Dieses Recht ist ein Grundrecht gemäß Artikel 2 Abs. 1 i. v. m. Art. 1 Abs. 2 Grundgesetz.

Die Ethik-Kommission weist zu Recht darauf hin, dass auch datenschutzfreundliche Innovationen (Privacy by Design) gefördert werden müssen. Es gilt eben auch zu verhindern, dass z. B. im Rahmen einer zentralen Verkehrssteuerung und der Erfassung aller Kraftfahr-

zeuge, es zu einer Totalüberwachung aller Verkehrsteilnehmer kommt.
Aus Sicht des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) ist es deshalb wichtig, Gelegenheiten zu nutzen, um mit der Auto-Industrie, Politikern und anderen Interessenten in Kontakt zu treten. So nutzte der TLfDI z. B. in Augsburg, Jena und Bielefeld die Möglichkeit, datenschutzrechtliche Hinweise zu geben und datenschutzrechtliche (Fehl-) Entwicklungen zu finden.

Moderne Fahrzeuge werden in naher Zukunft vollständig vernetzt sein. Die anfallenden Daten werden zukünftig Begehrlichkeiten verschiedener Wirtschaftszweige wecken. Die möglichen Daten haben das Potenzial der Verhaltenskontrolle und verraten viel über den Fahrer. Deshalb sind bei der Planung und Entwicklung von IT-Systemen Datenschutz und Datensicherheit zu berücksichtigen (Data protection by design). Die IT-Systeme müssen zudem datenschutzfreundlich so voreingestellt sein, dass nur die personenbezogenen Daten verarbeitet werden, die für den verfolgten Zweck erforderlich sind (Data protection by default).

12.5 Pflichten sozialer Netzwerke

Die Datenschutzbeauftragten des Bundes und der Länder beschäftigten sich schon recht früh mit der datenschutzrechtlichen Thematik von sozialen Netzwerken. Durch Facebook aber mit seinen mächtigen Funktionen, die so viel Daten wie möglich sammeln, um dem Nutzer ein „optimales“ Angebot bereitstellen zu können, wurde eine neue Qualität von sozialen Netzwerken geschaffen. Mit der Idee der „optimalen Kundenbetreuung“ ging zwangsweise die Notwendigkeit einer umfassenden Profilbildung der Nutzer einher. Nach dem Motto: Je mehr ich von einem Nutzer weiß, umso besser kann ich durch Algorithmen geschäftsmäßig die Bedürfnisse der Wirtschaft mit dem Kunden verbinden, auch die eigenen.
So stellte im September 2011 die 82. Konferenz der Datenschutzbeauftragten des Bundes und der Länder u. a. klar, dass sich Anbieter solcher Plattformen, die auf den europäischen Markt zielen, auch dann an europäische Datenschutzstandards halten müssen, wenn sie ihren Sitz außerhalb Europas haben (siehe

https://www.tlfdi.de/mam/tlfdi/datenschutz/entschliessungen/80/82_nutzerdaten.pdf).



In den meisten sozialen Netzwerken werden auch Funktionen angeboten, die es ermöglichen, mit anderen Leuten zu diskutieren, Beiträge, Fotos und Videos zu teilen. Somit können Anbieter sozialer Netzwerke durch deren Inhalte und Kommunikationspartner den Nutzer anhand seiner hinterlassenen Daten noch genauer analysieren. Diese Kommunikationsmöglichkeiten haben aber in den letzten Jahren eine besondere Dynamik erlangt. Neben Cybermobbing und anderen strafbaren Inhalten ist zunehmend eine Verbreitung von Hasskriminalität in den sozialen Netzwerken zu verzeichnen. Facebook z. B. verkündete im Mai 2017, dass nun tausende Mitarbeiter eingestellt würden, um dem entgegenzuwirken. Doch wie will man die Millionen Beiträge täglich überprüfen? Was ist zudem strafbar und was ist Kunst oder Meinungsfreiheit? Fast denkt man hier an Goethes Zauberlehrling und die Geister, die man selber rief.

In Deutschland gilt nun seit dem 1. Oktober 2017 das Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Bundesgesetzblatt Nr. 61 vom 7. September 2017).

Durch dieses Netzwerkdurchsetzungsgesetz (NetzDG), sollen die Hasskriminalität und andere strafbare Inhalte in sozialen Netzwerken minimiert werden. So sind Anbieter sozialer Netzwerke nun verpflichtet, bei einem offensichtlich rechtswidrigen Inhalt innerhalb von 24 Stunden nach Eingang der Beschwerde diesen zu entfernen oder den Zugang zu ihm zu sperren. Dies gilt nicht, wenn der Anbieter mit der zuständigen Strafverfolgungsbehörde einen längeren Zeitraum für die Löschung oder Sperrung des offensichtlich rechtswidrigen Inhalts vereinbart hat.

Handelt es sich um einen rechtswidrigen Inhalt, dessen Offensichtlichkeit nicht gleich erkennbar ist, muss der Anbieter trotzdem in der Regel innerhalb von sieben Tagen die Löschung oder Sperrung durchführen. Diese Zeit verlängert sich, falls der Anbieter zwecks Entscheidungsfindung über die Rechtswidrigkeit des Inhalts z. B. dem Nutzer vor der Entscheidung Gelegenheit zur Stellungnahme zu der Beschwerde gibt.

Falls es zu einer Löschung kommt, hat der Anbieter des sozialen Netzwerks, den Inhalt für die Dauer von zehn Wochen zu speichern. Weiterhin sind der Beschwerdeführer und der Nutzer über jede Ent-

scheidung unverzüglich zu informieren und die Entscheidung ist zu begründen.
Kritiker sehen hier eine Lücke, da nur eine Informationspflicht vorliegt. Ein Widerspruchsrecht für die Nutzer gibt es nicht.
Hat der Anbieter vom sozialen Netzwerk diesbezüglich mehr als 100 Beschwerden im Kalenderjahr, so ist er berichtspflichtig. Der deutschsprachige Bericht ist auf seiner Homepage und im Bundesanzeiger entsprechend dem NetzDG zu veröffentlichen.
Im Übrigen gelten die Regelungen zu den Beschwerden und zur Berichtspflicht nicht für Anbieter sozialer Netzwerke, wenn das soziale Netzwerk im Inland weniger als zwei Millionen registrierte Nutzer hat.

Anbieter sozialer Netzwerke, die auf den europäischen Markt zielen, müssen sich auch dann an europäische Datenschutzstandards halten, wenn sie ihren Sitz außerhalb Europas haben. Zudem gilt es ab dem 1. Oktober 2017 das Netzwerkdurchsetzungsgesetz (NetzDG) zu beachten.

12.6 Google-Analytics

Im 9. Tätigkeitsbericht (TB) des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) wurde auf die Möglichkeit des datenschutzgerechten Einsatzes von Google Analytics hingewiesen. So wurde berichtet, dass die Voraussetzung hierfür die Löschung des letzten Oktetts der IP-Adresse und ein Widerspruch gegen die Erfassung von Nutzungsdaten mittels eines von Google bereitgestellten Deaktivierungs-Add-On durch den Nutzer notwendig ist. Neben diesen umzusetzenden Parametern muss der Website-Betreiber, um einen datenschutzgerechten Betrieb von Google Analytics zu ermöglichen, zudem schriftlich einen Vertrag zur Auftragsdatenverarbeitung mit Google Inc. abschließen. Ein Muster dieses Vertrages wird von der Google Inc. selbst auf deren Website bereitgestellt (siehe 9. TB, Pkt. 4.1).
Aufgrund der Tatsache, dass das Safe-Harbor-Abkommen vom Europäischen Gerichtshof am 6. Oktober 2015 für ungültig erklärt wurde, prüfte der Hamburgische Beauftragte für den Datenschutz und die Informationsfreiheit (HmbBfDI) als zuständige Aufsichtsbehörde erneut den Mustervertrag. Nach Aussagen des HmbBfDI hat die Google Inc. die Zertifizierung nach dem aktuellen EU-US-Privacy-

Shield durchgeführt und somit die rechtlichen Voraussetzungen auch für die Erbringung des Dienstes Google-Analytics im Wege der Auftragsdatenverarbeitung geschaffen.
Hinweise zum aktuellen Mustervertrag zur Auftragsdatenverarbeitung sowie aktuelle Hinweise zum datenschutzgerechten Einsatz von Google-Analytics finden Sie auf der Website: https://www.datenschutz-hamburg.de/uploads/media/GoogleAnalytics_Hinweise_fuer_Webseitenbetreiber_in_Hamburg_2017.pdf



Der Einsatz von Google-Analytics ist aus datenschutzrechtlicher Sicht nur unter bestimmten Voraussetzungen erlaubt. Hinweise hierzu finden Sie auf der Website der zuständigen Aufsichtsbehörde.

12.7 Speicherung von IP-Adressen – Sicherheit oder Datenschutz?

Ob dynamische oder statische IP-Adressen personenbezogene Daten im Sinne des Datenschutzrechtes sind oder nicht, darüber urteilten, seitdem es Websites gibt die jeweiligen Gerichte in den einzelnen Bundesländern recht unterschiedlich. Die Datenschutzbeauftragten des Bundes und der Länder standen aus ihrer Sicht dabei immer auf dem Standpunkt, dass statische IP-Adressen personenbezogen sind und zumindest bei dynamischen IP-Adressen u. U. ein Personenbezug herstellbar sei. Aber unter den jeweiligen Gerichten in den Bundesländern gab es hierzu keine einheitliche Rechtsauffassung.
So muss man fast von Glück reden, dass es eine Klage in dieser Sache vor ein paar Jahren bis zum Bundesgerichtshof (BGH) geschafft hatte. Herr Patrick Breyer, Parteimitglied der Piraten-Partei, hatte vor vielen Jahren geklagt, dass Einrichtungen des Bundes seine Internetprotokoll-Adressen (IP-Adressen) beim Zugriff auf ihre Websites aufzeichnen und speichern. Das Amtsgericht Tiergarten wies die Klage 2008 ab (AZ 2 C 6/08), wogegen Herr Breyer Berufung einlegte. Gegen das nachfolgende Urteil aus dem Jahr 2013 vom Landgericht Berlin wurde Revision eingelegt, sodass es beim BGH landete.

Der BGH entschied in seinem Beschluss vom 28. Oktober 2014 (Beschl. v. 28.10.2014, Az. VI ZR 135/13), das Verfahren auszusetzen und den Europäischen Gerichtshof (EuGH) zwecks Klärung zweier Fragen zu bitten.
Dabei war entsprechend der Informationen des EuGH Folgendes zu klären:

1.) Ob in diesem Zusammenhang auch „dynamische“ IP-Adressen für den Betreiber der Website personenbezogene Daten darstellen, sodass sie den für solche Daten vorgesehenen Schutz genießen. Eine „dynamische“ IP-Adresse ist eine IP-Adresse, die sich bei jeder neuen Internetverbindung ändert. Anders als statische IP-Adressen erlauben dynamische IP-Adressen es nicht, anhand allgemein zugänglicher Dateien eine Verbindung zwischen einem Computer und dem vom Internetzugangsanbieter verwendeten physischen Netzanschluss herzustellen. Somit verfügt ausschließlich der Internetzugangsanbieter von Herrn Breyer über die zu dessen Identifizierung erforderlichen Zusatzinformationen.
2.) Ferner wollte der BGH wissen, ob der Betreiber einer Website zumindest grundsätzlich die Möglichkeit haben muss, personenbezogene Daten der Nutzer zu erheben und zu verwenden, um die generelle Funktionsfähigkeit seiner Website zu gewährleisten. Der BGH wies insoweit darauf hin, dass die einschlägige deutsche Regelung von der deutschen Lehre überwiegend dahin ausgelegt werde, dass die Daten am Ende des jeweiligen Nutzungsvorgangs zu löschen seien, soweit sie nicht für Abrechnungszwecke benötigt würden.

Zwei Jahre später, am 19. Oktober 2016, entschied der EuGH über diese zwei Fragen (Rechtsache C-582/14):
Zu 1.) Eine dynamische Internetprotokoll-Adresse stellt ein personenbezogenes Datum für den Website-Anbieter dann dar, wenn er über rechtliche Mittel verfügt, die es ihm erlauben, die betreffende Person anhand der Zusatzinformationen, über die der Internetzugangsanbieter dieser Person verfügt, bestimmen zu lassen.
Dies bedeutet, er muss rechtlich die Möglichkeit haben, den Internetzugangsanbieter zwecks Zusatzinformationen abfragen zu dürfen. Diese Möglichkeit besteht beispielsweise im Fall von „Cyberattacken“, bei dem ein Strafverfahren eingeleitet werden kann.
Zu 2.) Eine Regelung eines Mitgliedstaats, wonach IP-Adressen nur zu Abrechnungszwecken längerfristig gespeichert werden dürfen, sei

in Bezug auf Art. 7 Buchstabe f der europäischen Datenschutz-Richtlinie europarechtswidrig. Eine nationale Regelung darf nicht die Verarbeitung bestimmter Kategorien personenbezogener Daten ausschließen, indem sie für diese Kategorien das Ergebnis der Abwägung abschließend vorschreibt, ohne Raum für ein Ergebnis zu lassen, das aufgrund besonderer Umstände des Einzelfalls anders ausfällt. Daher stellt sich die Frage, ob § 15 Telemediengesetz (TMG) richtlinienkonform dahin ausgelegt werden muss, dass bei der Sicherstellung der Funktion des Telemediums über die Nutzungsdauer hinaus personenbezogene Daten Verwendung finden dürfen, soweit und solange die Verwendung zu diesem Zweck erforderlich ist.
Am 15. Mai 2017 traf dann der BGH, aufgrund der Einschätzung des EuGH, folgende Entscheidung (VI ZR 135/13):
Zu 1.) Die dynamische IP-Adresse, die von einem Anbieter von Online-Mediendiensten beim Zugriff auf eine Internetseite, die dieser Anbieter allgemein zugänglich macht, gespeichert wird, stellt für den Anbieter ein personenbezogenes Datum dar.
Zu 2.) § 15 Abs. 1 TMG ist nun dahingehend auszulegen, dass Anbieter von Online-Mediendiensten personenbezogene Daten eines Nutzers dieser Dienste ohne dessen Einwilligung auch über das Ende eines Nutzungsvorgangs hinaus dann erheben dürfen, soweit ihre Erhebung und ihre Verwendung erforderlich sind, um die generelle Funktionsfähigkeit des Dienstes zu gewährleisten, wobei es allerdings einer Abwägung mit dem Interesse und den Grundrechten und -freiheiten der Nutzer bedarf.
Allerdings sieht der BGH diese notwendige Abwägung im Streitfall beim Landgericht Berlin nicht geprüft. Für diese Abwägung sind vor allem das Angriffsrisiko auf Anbieterseiten sowie die Schwere des Eingriffs in das informationelle Selbstbestimmungsrecht des Nutzers entscheidend.
Der BGH verwies den Fall schließlich wieder zurück an das Landgericht Berlin.

Dynamische IP-Adressen stellen ein personenbezogenes Datum dar. § 15 Abs. 1 Telemediengesetz ist dahingehend auszulegen, dass Anbieter von Online-Mediendiensten personenbezogene Daten eines Nutzers dieser Dienste ohne dessen Einwilligung auch über das Ende eines Nutzungsvorgangs hinaus dann erheben dürfen, soweit ihre Erhebung und ihre Verwendung erforderlich sind, um die generelle

Funktionsfähigkeit des Dienstes zu gewährleisten, wobei es allerdings einer Abwägung mit dem Interesse und den Grundrechten und -freiheiten der Nutzer bedarf.

12.8 eIDAS – was ist das?

Im 11. Tätigkeitsbericht des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit wurde unter der Überschrift „eIDAS – was ist das?“ über die eIDAS-Verordnung berichtet. Es ging darum, dass mit der am 23. Juli 2014 verabschiedeten EU-„Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (910/2014)“ für alle Mitgliedstaaten die sichere elektronische Identifizierung und Authentifizierung neu festgeschrieben wurde. Diese Verordnung wird eIDAS-Verordnung genannt (electronic identification and trust services) und ist unmittelbar geltendes Unionsrecht.
Die Vorschriften bezüglich der Vertrauensdienste traten allerdings erst ab dem 1. Juli 2016 in Kraft. Vertrauensdienste definiert die eIDAS-Verordung in Artikel 3 wie folgt: Ein Vertrauensdienst ist ein elektronischer Dienst, der in der Regel gegen Entgelt erbracht wird und die Erstellung, Überprüfung und Validierung von elektronischen Signaturen, elektronischen Siegeln oder elektronischen Zeitstempeln, und Diensten für die Zustellung elektronischer Einschreiben sowie von diese Dienste betreffenden Zertifikaten anbietet. Vertrauensdienste sind aber auch Dienste, die die Erstellung, Überprüfung und Validierung von Zertifikaten für die Website-Authentifizierung oder die Bewahrung von diese Dienste betreffenden elektronischen Signaturen, Siegeln oder Zertifikaten, anbietet.



Vertrauensdiensteanbieter können ihre Dienste/Produkte auch zu einem „qualifizierten Dienst“ zertifizieren lassen und dürfen dann ihre Dienste mit dem neuen EU-Vertrauenssiegel bewerben. Um der eIDAS-Verordnung bezüglich der Vertrauensdienste gerecht zu werden, trat in Deutschland am 29. Juli 2017 das eIDAS-Durchführungsgesetz mit zahlreichen Gesetzesänderungen in Kraft (BGBL Nr. 52/2017). Mit dem darin enthaltenen neuen Vertrauensdienstegesetz (VDG) wurde die wirksame Durchführung der Vorschriften über Vertrauensdienste rechtlich geregelt.

Zuständige Aufsichtsstelle für Vertrauensdienste im Bereich der Erstellung, Überprüfung und Validierung von Zertifikaten für Website-Authentifizierung ist in Deutschland das Bundesamt für Sicherheit in der Informationstechnik (BSI). Für die Aufgaben der anderen Bereiche ist die Bundesnetzagentur (BNetzA) zuständig.
Mit dem eIDAS-Durchführungsgesetz wurden zudem das Signaturgesetz und die Signaturverordnung außer Kraft gesetzt. Sämtliche Verweise auf das Signaturgesetz und die Signaturverordnung müssen nun zeitnah aktualisiert werden. Entsprechend der Übergangsvorschrift werden zudem die von der Bundesnetzagentur gemäß § 16 Absatz 1 des Signaturgesetzes ausgestellten Zertifikate mit Ablauf des 14. November 2018 gesperrt. Entsprechende akkreditierte Zertifizierungsdiensteanbieter müssen also rechtzeitig neue Zertifikate beantragen.

Mit Inkrafttreten des Vertrauensdienstegesetzes am 29. Juli 2017 werden alle von der Bundesnetzagentur gemäß § 16 Absatz 1 des Signaturgesetzes ausgestellten Zertifikate mit Ablauf des 14. November 2018 gesperrt. Sämtliche Verweise auf das Signaturgesetz und die Signaturverordnung müssen zudem nun zeitnah überarbeitet werden.

12.9 EU- und nationale Cybersicherheit

Am 5. Juli 2016 veröffentlichte die EU-Kommission eine Mitteilung unter der Überschrift „Stärkung der Abwehrfähigkeit Europas im Bereich der Cybersicherheit und Förderung einer wettbewerbsfähigen und innovativen Cybersicherheitsbranche“. Der Mitteilung war zu entnehmen, dass einer Untersuchung zufolge mindestens 80 Prozent der europäischen Unternehmen im Jahr 2015 zumindest einmal mit einem Cybervorfall zu tun gehabt haben. Zudem nahm die Zahl der Sicherheitsvorfälle in der gesamten Wirtschaft 2015 weltweit um 38 Prozent im Vergleich zum Vorjahreszeitraum zu.
Die Europäische Kommission will deshalb eine verstärkte Zusammenarbeit sowohl über Ländergrenzen hinweg als auch zwischen allen Akteuren und allen Sektoren, die im Bereich der Cybersicherheit aktiv sind, fördern. Außerdem will sie dazu beitragen, dass in der EU innovative und sichere Technologien, Produkte und Dienste entwickelt werden.

Diese Mitteilung ist im zeitlichen Kontext der Maßnahmen zu sehen, die die Cybersicherheit in Europa erhöhen sollen. Denn am Tag darauf, am 6. Juli 2016, verabschiedete das Europäische Parlament die „Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union“, kurz auch NIS-Richtlinie genannt (Richtlinie (EU) 2016/1148 vom 6. Juli 2016, https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016L1148&from=DE).



Die Mitgliedstaaten der EU müssen dem nun Rechnung tragen und die Bestimmungen der NIS-Richtlinie in nationales Recht umsetzen. Die so getroffenen Vorschriften und Umsetzungsmaßnahmen sind bis zum 9. Mai 2018 der Kommission mitzuteilen. Etwaige spätere Änderungen sind dann immer unverzüglich der Kommission zu melden.

Die Bundesrepublik Deutschland hat deshalb ein Gesetz zur Umsetzung der Richtlinie (EU) 2016/1148 beschlossen. Dieses Gesetz ist vom 23. Juni 2017 und im Bundesgesetzblatt Nr. 40 von 2017 veröffentlicht. Es ist als „Gesetz zur Umsetzung der EU-Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union“ (NIS-Richtlinien-Umsetzungsgesetz) am 30. Juni 2017 in Kraft getreten.

Das Gesetz ist ein sogenanntes Artikel-Gesetz und regelt in einzelnen Artikeln die Änderungen von verschiedenen, nachfolgend aufgeführten Gesetzen. So wurden das BSI-Gesetz (BSIG), das Telekommunikationsgesetz (TKG), das Telemediengesetz (TMG), das Energiewirtschaftsgesetz (EnWG), das Atomgesetz (AtG) und auch das Fünfte Buch des Sozialgesetzbuches in Teilen angepasst.

Gemäß BSIG müssen beispielsweise die Betreiber Kritischer Infrastrukturen ihre IT-Sicherheit nach dem „Stand der Technik“ umsetzen und deren Einhaltung regelmäßig gegenüber dem BSI nachweisen. Sofern Sicherheitsmängel aufgedeckt werden, darf das BSI im

Einvernehmen mit den Aufsichtsbehörden deren Beseitigung anordnen.[a]
Im TKG werden Telekommunikationsanbieter sowie auch im TMG Telemediendiensteanbieter nunmehr dazu verpflichtet, IT-Sicherheitsmaßnahmen nach dem „Stand der Technik“ zu ergreifen und zu erhalten, die nicht nur dem Schutz personenbezogener Daten dienen, sondern auch dem Schutz vor unerlaubten Eingriffen in die Infrastruktur.[b]
Bezüglich der Telekommunikationsnetze erweitert sich die bereits bestehende Meldepflicht gemäß § 109 Absatz 5 TKG insofern, dass Beeinträchtigungen sowohl an die Bundesnetzagentur als auch an das BSI gemeldet werden müssen. Betreiber Kritischer Infrastrukturen gemäß BSI-Kritisverordnung müssen ebenfalls eine Kontaktstelle beim BSI registrieren.
Wichtigste Änderung im Energiewirtschaftsgesetz (EnWG) ist die Tatsache, dass das Bundesamt für Sicherheit in der Informationstechnik (BSI) die Meldepflicht von IT-Störungen auf alle Energieversorgungsnetzbetreiber ausgeweitet hat. Letztere müssen hierfür eine zuständige Kontaktstelle einrichten.
Beim Atomgesetz (AtG) ist dies für die Betreiber gleichlautend formuliert.[c]

Zur Stärkung der Abwehrfähigkeit Europas im Bereich der Cybersicherheit haben Mitgliedstaaten der EU die seit 2016 in Kraft gesetzte EU-NIS-Richtlinie in nationales Recht umzusetzen. Bis zum 9. Mai 2018 sind die getroffenen Vorschriften und Maßnahmen der Europäischen Kommission zu melden.

12.10 Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation („Berlin Group“)

Wie bereits an anderer Stelle erwähnt, arbeiten die unabhängigen Datenschutzbeauftragten des Bundes und der Länder themenbezogen bundesweit in sehr vielen Arbeitskreisen und Unterarbeitsgruppen

[a] weitere Details vgl. https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/IT-SiG/Neuregelungen_IT_SiG/neur_IT_SiG_node.html
[b] ebenda
[c] ebenda

zusammen. Darüber hinaus gibt es auch internationale Arbeitsgruppen.
Die internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation („Berlin Group“) finalisierte im April 2016 das Arbeitspapier „Aktualisierung zu Datenschutz und Datensicherheit in der Internettelefonie (Voice over IP – VoIP) und verwandten Kommunikationstechnologien“. Das Arbeitspapier spricht diesbezügliche Empfehlungen aus, die an verschiedene Akteure gerichtet sind, so auch an die Gesetzgeber, bestehende Regelungslücken zu schließen.
Im November 2016 wurde von der internationalen Arbeitsgruppe das „Arbeitspapier zu Biometrie in der Online-Authentifizierung“ verabschiedet. Oft wird der Zugang zur Hard- oder Software schon per Fingerabdruck oder Gesichtserkennung ermöglicht. Aber auch bei dieser Methode müssen Datenschutz und Datensicherheit sichergestellt sein.
Im April 2017 wurde dann das „Arbeitspapier zum Thema E-Learning-Plattformen“ fertiggestellt. Mit dem zunehmenden Einsatz von E-Learning-Plattformen wächst die Menge an personenbezogenen Daten, die über die Lernenden zur Verfügung stehen. Diese Daten könnten beispielsweise zu Prognosen des geistigen Zustands herangezogen werden und gewollte oder ungewollte lebenslange Schlussfolgerungen nach sich ziehen. Betreiber solcher Plattformen tragen hier eine sehr hohe datenschutzrechtliche Verantwortung.
Alle drei Arbeitspapiere sind auf der Seite der internationalen Arbeitsgruppe abrufbar https://www.berlin-privacy-group.org.

Die internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation hat die Arbeitspapiere zu Datenschutz und Datensicherheit in der Internettelefonie (Voice over IP – VoIP) und verwandten Kommunikationstechnologien, zu Biometrie in der Online-Authentifizierung und zum Thema E-Learning-Plattformen veröffentlicht.

12.11 Wenn Kühlschränke eiskalt angreifen

Das ist keine Utopie mehr. Im Herbst 2016 mussten in den USA viele Menschen rund zwei Stunden ohne Musik von Spotify und

Soundcloud, ohne Twitter, ohne Netflix und ohne ein Dutzend anderer beliebter Onlinedienste auskommen.
Was war geschehen?
Zunehmend halten Haushaltsgeräte im privaten Bereich Einzug, die internetfähig sind. Sie haben neben einer IP-Adresse eine Software, die nicht vom Kunden überschaubar bzw. kontrollierbar ist. Dies betrifft z. B. Kühlschränke, Thermostate, Videogeräte, hausinterne Webcams usw.
Oft werden diese Geräte zudem mit Standard-Administrations-Passwörtern ausgeliefert, deren Änderung für den Normalverbraucher schon eine Hürde darstellt.
Hacker haben dies bereits erkannt, schalten sich auf solche Geräte auf, programmieren sie so, dass diese zu einem bestimmten Zeitpunkt zeitgleich einen Angriff ausüben. Also zur gleichen Zeit festgelegte Ziel-Server mit Anfragen zuschütten, sodass die Server dann überlastet sind. Im Fachbereich spricht man von einem Botnetz, welches solche Angriffe ausführt.
Nun mag man denken, so etwas wird nicht in Deutschland geschehen. Im November 2016 wurde aber eine größere Anzahl von Routern der Telekom, die unzählige Haushalte vor Angriffen schützen sollten, selbst Opfer eines Hackerangriffes. Nach Angaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI) waren dabei über 900.000 Kundenanschlüsse betroffen. Nach Angaben der Telekom handelte es sich dabei um Telekom-Router von Drittanbietern. Ziel des Angriffs war die Installation einer Schadsoftware auf diese Router, damit diese dann als Teil eines sogenannten Botnetzes fungierten, also als fernsteuerbare Infrastruktur für weitere Angriffe zur Verfügung stehen. Nach Angaben der Telekom war die Installation der Schadsoftware bei denen, die die Telekom betrieb, nicht erfolgreich. Bei dem Versuch, die Schadsoftware zu installieren, stürzten diese aber ab. So war für viele Kunden kein Internet und keine IP-Telefonie möglich. Der Angriff auf die Drittanbieter-Router diente der Konstruktion eines Botnetzes zum gleichzeitigen Angriff auf externe Server.
Was ist aber, wenn zukünftige Angriffe nicht nur externen Servern gelten, sondern internetfähige Geräte im Haushalt das Ziel solcher Angriffe sind? Also Router gekapert werden, um Geräte innerhalb des Hauses zu manipulieren, auch um diese für Großangriffe fit zu machen?

Was passiert eigentlich zukünftig, wenn auch hier Hacker Kühlschränke eiskalt manipulieren? Welche Folgen ergeben sich zukünftig für den Bürger daraus? Wird dann der komplette digitalisierte Haushalt von staatlicher Seite abgeschaltet, sämtliche Geräte im Haushalt, einschließlich PC und Smartphone, überprüft? Gibt es dann noch Fernsehen und Strom, da auch diese Geräte mittlerweile vernetzt sind? Welche Rechte und Pflichten wird zukünftig der Bürger in der digitalen Gesellschaft haben?
Wenn große Unternehmen sich schon nicht vor Hackerangriffen schützen können, ist es nur eine Frage der Zeit, wann auch in Deutschland beispielsweise Kühlschränke eiskalt angreifen.
Der Einzug in die digitale Gesellschaft kommt und ist auch richtig, nur bedarf es auch einer digitalen und dementsprechenden technischen und rechtlichen Sicherheit für die Bürger, die von den jeweiligen Herstellern solcher Geräte zukünftig sichergestellt werden muss. Die Hersteller von internetfähigen Geräten und auch der Rechtsstaat müssen sich langfristig der Verantwortung bewusst werden, dass die Einführung der digitalen Gesellschaft nicht auf Kosten der Bürger und ihrer Grundrechte gehen darf.
Der TLfDI stellt hierfür seine Erfahrungen und Kenntnisse gern bereit.

Hersteller von internetfähigen Geräten müssen für ihr Produkt haftbar gemacht werden. Geräte sind zudem so zu gestalten, dass neben eindeutigen und verständlichen Hinweisen der Hersteller für Käufer beispielsweise schon beim Erwerb eines solchen Gerätes mit einfachen Mitteln das jeweilige Standard-Passwort vom Eigentümer geändert werden kann.

12.12 Canvas-Fingerprinting

Zunehmend werden bei der Darstellung von Websites Browser-Fingerprints verwendet, um Internetnutzer zu tracken, um so z. B. personalisierte Werbung zu schalten. Fingerprinting ist eine Methode, um Hersteller und Versionen von Software-Anwendungen über ein Netzwerk zu erkennen, obwohl diese Informationen nicht explizit vom System kommuniziert werden. Die Methode erlaubt es, auf Cookies oder Logins zu verzichten. Canvas-Fingerprinting ist eine solche Methode.

Wie funktioniert Canvas-Fingerprinting? Beim Aufruf einer Website werden von der Website im Hintergrund Informationen über bestimmte Software- und Hardware Merkmale ermittelt, die der Browser selbst bei Aufruf zwecks optimaler Darstellung mitliefert oder auf Anfrage nachliefert. Diese Informationen werden bei Canvas-Fingerprinting erfasst, indem sozusagen kleine Grafiken „gezeichnet“ werden. Jede Konfiguration von Hard- und Software erstellt die Grafiken mit leichten Abweichungen zueinander. Diese werden dann zur Identifizierung genutzt. Die so gesammelten Daten, wie beispielsweise der Browsertyp und Version, genutzte Schriftart, installierte Schriftarten, Bildschirmgröße, Sprache, die Art des Grafikprozessors usw., geben Aufschluss über das jeweilige Gerät. Über die gesammelten Daten entsteht somit der o. g. „Fingerabdruck“ (engl.: Fingerprinting) des jeweiligen technischen Gerätes. Je mehr Daten für die Bildung des Fingerabdrucks erfasst werden, umso genauer ist dieser Fingerabdruck und somit der Wiedererkennungswert des Gerätes.
Man kann sich vor Canvas-Fingerprinting schützen, indem man Java-Script in den Browsereinstellungen deaktiviert. Der Nachteil davon ist, dass dann allerdings viele Anzeigen von Webseiten nicht mehr richtig funktionieren. Auch empfehlen IT-Experten, mindestens zwei bis drei verschiedene Browser für verschiedene Suchanfragen zu verwenden. Dies erscheint für normale Nutzer zu umständlich. Weitere IT-Experten empfehlen, Anonymisierungsnetzwerke wie TOR zu nutzen. Letzteres zieht aber nur eine Anonymisierung des Netzverkehrs nach sich – die Inhalte, welche zur Identifikation herangezogen werden, werden durch TOR nicht anonymisiert. Für das tägliche Surfen erscheint dies auch ein umständlicher Weg. Manche Browser bieten auch schon Canvas-Blocker an. Solch ein Canvas-Blocker als sogenanntes Add-on kann Zugriffe auf Canvas-Elemente blockieren. In den Einstellungen des Add-on kann man dann das gewünschte Verhalten konfigurieren. Dieses Add-on sollte aber nur von der Online-Plattform des jeweiligen Browserherstellers geladen werden.
Es gibt demnach durchaus verschiedene Möglichkeiten, sich zu schützen. Jeder muss für sich selbst entscheiden, welchen Weg er gehen möchte.

Zunehmend werden bei der Darstellung von Websites heimlich Browser-Fingerprints verwendet, um Internetnutzer zu tracken. Da-

mit kann z. B. personalisierte Werbung geschaltet werden. Die beschriebene Methode erlaubt es, auf Cookies oder Logins zu verzichten. Bei der Auswahl der Schutzmöglichkeiten wird empfohlen, sich auf dem Portal des jeweiligen Browseranbieters genau zu informieren und dann erst eigene Maßnahmen zu treffen.

12.13 Neues Personalausweis-Gesetz: Daten in Hülle und Fülle für den Staat

Das Zeitalter der digitalen Gesellschaft geht auch nicht spurlos am Personalausweisgesetz vorbei. Im Jahr 2010 wurde der neue digitale Personalausweis eingeführt. Man sah neben der Speicherung von Fingerabdrücken und einer qualifizierten elektronischen Signatur zur rechtssicheren digitalen Unterschrift auch die Speicherung einer elektronischen Identifikationsmöglichkeit (eID-Funktion) vor.
Letztere sollte dazu dienen, sich gegenüber Behörden und Unternehmen online eindeutig gegenüber deren Online-Diensten identifizieren zu können.
Bürger konnten bei Ausgabe des Personalausweises wählen, ob sie diese Identifikationsmöglichkeit (eID-Funktion) zukünftig nutzen möchten.
Der Bundestagsdrucksache 18/11279 vom 22. Februar 2017 zur Änderung des Personalausweisgesetzes konnte man aber nun entnehmen, dass die Nutzung und die Verbreitung der eID-Funktion bisher hinter den Erwartungen zurückblieben. Bei zwei Dritteln der rund 51 Millionen ausgegebenen Ausweise sei die eID-Funktion deaktiviert.
Aber es gibt auch kaum Anwendungen diesbezüglich. Datenschützer warnten zudem auch permanent davor, die eID-Funktion zu nutzen, wenn nicht sichergestellt ist, dass heimlich das Passwort der eID-Funktion ausgelesen werden kann, z. B. durch Schadsoftware, welche die Tastatur-Eingabe am Rechner mit ausliest.
Nur die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zertifizierten Lesegeräte mit einer eigenen Tastatureingabe können dem derzeit Rechnung tragen. Alle anderen vom BSI zugelassenen Geräte sind aus Sicht des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) nicht empfehlenswert. Möchte der Bund ein sicheres Verfahren anbieten, so muss auch aus datenschutzrechtlicher Sicht die Sicherheit des kompletten Verfahrens sichergestellt werden. Dem ist weiterhin nicht so. Die

Verantwortung auf den Bürger zu delegieren, ist nicht mehr zeitgemäß, zudem erfolgen immer mehr Hackerangriffe auf IT-Systeme. Zukünftige repräsentative Verfahren wie z. B. Online-Abstimmungen, Wahlen etc. wären mit Lesegeräten ohne eigene Tastatureingabe wie oben beschrieben von vornherein anfällig oder manipulierbar.
Da nur wenige Bürger die eID-Funktion bei Antragstellung des Personalausweises freigeschaltet haben wollten, entschloss sich der Gesetzgeber, nun das Personalausweisgesetz (PAuswG) dahingehend zu ändern, dass zukünftig die eID-Funktion für alle zukünftigen Personalausweise von vornherein freigeschaltet wird.
Zudem regelte man gleichzeitig in § 25 PAuswG, dass unter bestimmten Voraussetzungen zukünftig bestimmte Behörden im automatisierten Verfahren das Lichtbild aus dem Personalausweisregister abrufen können.
Dies konnten die unabhängigen Datenschutzbeauftragten des Bundes und der Länder nicht unkommentiert lassen und positionierten sich in ihrer Entschließung bereits im Januar 2017 dahingehend, dass weiterhin die eID-Funktion freiwillig sein muss und die zum 1. Mai 2021 vorgesehene Einführung eines nahezu voraussetzungslosen Abrufs des Lichtbildes im automatisierten Verfahren durch die Polizeibehörden des Bundes und der Länder sowie die Verfassungsschutzbehörden und Nachrichtendienste abgelehnt wird (siehe Anlage 3).
Die neuen Regelungen sind im Bundesgesetzblatt Nr. 46 vom 14. Juli 2017 veröffentlicht.

Die unabhängigen Datenschutzbeauftragten des Bundes und der Länder fordern, dass weiterhin die Funktion der elektronischen Identifizierung mittels digitalem Personalausweis freiwillig bleibt. Zudem lehnen sie die vorgesehene Einführung eines nahezu voraussetzungslosen Abrufs des Lichtbildes im automatisierten Verfahren durch die Polizeibehörden des Bundes und der Länder sowie die Verfassungsschutzbehörden und Nachrichtendienste ab.

12.14 WannaCry

Im Frühjahr 2017 wurden weltweit zehntausende Computer Opfer eines Hackerangriffs durch die Schadsoftware WannaCry. Diese Software verschlüsselt die Daten auf den jeweils gehackten Compu-

tern und zeigt dann auf dem Bildschirm des Benutzers eine Lösegeldforderung an. Das Verfahren ist nicht neu. Seit Jahren wird in diesem Zusammenhang auch davon abgeraten, auf solche Lösegeldforderungen einzugehen, denn eine Entschlüsselung der Daten nach der Zahlung ist ungewiss. Tritt ein solcher Fall jedoch auf, hilft nur eine Anzeige bei der Polizei gegen Unbekannt. Der Rechner sollte umgehend neu installiert werden, bestenfalls mit einem Sicherungs-Image neueren Datums.
Neu bei diesem Angriff war allerdings, dass er massenhaft in über hundert Ländern gleichzeitig erfolgte. Man spricht vom größten Hacker-Angriff in der Geschichte der Cyber-Angriffe. Auch in Deutschland waren Behörden, Unternehmen sowie Privatpersonen betroffen. So manche Zuganzeige bei der Deutschen Bahn zeigte beispielsweise anstelle der Fahrverbindungen eine Lösegeldforderung an.
Sicherheitslücken in Betriebssystemen oder Systemanwendungen wird es allerdings wohl immer geben. Diese Lücken werden von den Herstellern zum Teil durch sogenannte Sicherheits-Updates (auch „Patches“ genannt) geschlossen. Deswegen ist es als Nutzer wichtig, immer auf die Aktualität der auf dem eigenen Computer installierten Software zu achten. Im Fall von WannaCry waren nur Windows-Rechner älterer Versionen betroffen. Bei aktuellen Versionen der Microsoft-Betriebssysteme war zuvor schon die Sicherheitslücke durch den Hersteller geschlossen worden. Nachdem WannaCry weltweit einen so großen „Erfolg“ hatte, stellte Microsoft zusätzlich Sicherheits-Updates für ältere Betriebssysteme, deren Support-Zyklen beendet sind – das sind Windows XP, Windows 8 als Client-Betriebssysteme und Windows Server 2003 – bereit.
Hinsichtlich der Nutzung von Rechnern mit dem Betriebssystem Windows XP warnte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) bereits in seinem 11. Tätigkeitsbericht unter Punkt 16.5. Mit der Ankündigung von Microsoft, das Betriebssystem ab dem 8. April 2014 nicht mehr mit Sicherheits-Updates zu versorgen, sah der TLfDI eine Gefahr für die Datensicherheit und somit für den Datenschutz.

Um das Sicherheitsrisiko bei Sicherheitslücken in Betriebssystemen oder Systemanwendungen zu minimieren, sind die vom Hersteller bereitgestellten Sicherheits-Updates zeitnah zu installieren. Client-Betriebssysteme, die im erweiterten Support keine Sicherheits-

Updates mehr erhalten, sind daher durch neuere Client-Betriebssysteme zu ersetzen. Wo dies aus zwingenden Gründen nicht geschehen kann, müssen angemessene technische und organisatorische Sicherheitsmaßnahmen (TOM) bei den verantwortlichen Stellen getroffen werden, um die Sicherheitsrisiken auszuschließen.

12.15 Zerstören Sie die Cayla-Puppe – wenn das Spielzeug mithört

Am 16. Februar 2017 wurde von den Medien eine etwas merkwürdige Meldung verbreitet. Besitzer der Puppe Cayla sollten diese zerstören. Was war geschehen? Cayla ist eine Spielzeugpuppe und wurde von der in Hong Kong ansässigen Firma Genesis Toys hergestellt und durch die britische Spielzeugfirma Vivid Toy Group Limited“vertrieben. In der Puppe war ein Mikrofon verbaut, welches die Sprache aufnehmen konnte und diese Daten an ein über Bluetooth verbundenes Gerät (z. B. Smartphone oder Tablet) weiterschickte, wenn auf diesem die passende Cayla-App installiert und aktiviert war. Diese App schickte dann die Daten zur Analyse an einen Server, damit dieser eine passende Antwort generieren konnte, welche die Puppe dann von sich gab.
Die Bundesnetzagentur stufte die Puppe als eine „versteckte sendefähige Anlage“ nach § 90 Telekommunikationsgesetz (TKG) ein, welches solche „Anlagen“ verbietet. Grund war, dass der Puppe nicht anzusehen war, dass diese als Mikrofon dient. Damit ist nicht nur der Betrieb der Puppe, also deren Benutzung, sondern sogar der Besitz einer solchen Puppe verboten. Daher auch die Meldung, dass Besitzer der Puppe diese umgehend zerstören sollen. Zudem sei die Bluetooth-Verbindung nicht abgesichert, was bedeutet, dass jeder in Reichweite der Puppe sich mit dieser verbinden konnte und diese als Abhöreinrichtung missbrauchen konnte. Nach Angaben der Stiftung Warentest (Ausgabe 09/2017, Seite 35 ff.) ist diese Eigenschaft der unsicheren Verbindung nicht selten anzutreffen. Der Teddy Toy-Fi oder der ebenfalls von Genesis Toys hergestellte Roboter i-Que besitzt ebenso diese Schwachstelle. Auch diese Spielzeuge bieten Apps zum „Abhören“ der Kinder und können auch mit Sprachnachrichten rückantworten. Einziger Unterschied ist hier, dass die Bundesnetzagentur diese Spielzeuge noch nicht verboten hat.
Abgesehen von der potenziellenen Abhörgefahr durch Personen, die sich in Funkreichweite dieser Spielzeuge befinden, ist auch gesell-

schaftlich ein Trend zu erkennen, dass immer mehr intelligente sprachgesteuerte Assistenten im Wohnbereich eingesetzt werden. Was mit „Siri“ auf dem iPhone begann und mit „Hello Google“ auch bei Android-Smartphones heute Stand der Technik ist, kommt nun in Form von Lautsprechern (Amazons „Alexa“, Googles „Home“ Lautsprecher, Apples „HomePod“) in die Wohnzimmer der Bevölkerung. Diese Geräte sind nicht so einfach zu kapern, wie dies bei den Spielzeugen der Fall ist, und von „verstecken sendefähige Anlagen“ kann auch keine Rede sein. Aber letztere Geräte reagieren auf Kommandoworte und schicken auch dann aufgenommene Sprache über das Internet an Server, welche die Kommandos interpretieren bzw. noch unbekannte Datenverarbeitungen damit vollziehen (so gibt es Forschungsarbeiten, die das Geschlecht, die Stimmung bzw. eine Personenidentifikation mit Sprachaufzeichnungen einschätzen können).
Der Trend geht also ganz klar zur Vernetzung der Alltagsgegenstände. Über die Konsequenzen und was man eigentlich über sich dabei preisgibt, herrscht meist beim Nutzer Unklarheit. Im Fall der Puppe Cayla wurde ein Verbot ausgesprochen – allerdings nur aufgrund des „Versteckens“ der Funktion. Zahlreiche andere Produkte sind bereits im Alltag der Menschen angekommen. Hier sollte ein Bewusstsein in der Bevölkerung entstehen, bis wohin solche Geräte in das eigene Leben und das eigene Heim vordringen dürfen und aus welchen privaten Bereichen diese Art von Technik fernbleiben sollte. Im Kinderzimmer hat so etwas nach Auffassung des TLfDI jedenfalls nichts zu suchen.

Der TLfDI rät, „intelligente“ Spielzeuge ohne eine vorherige tiefgründige Recherche und Erklärung gegenüber dem Kind nicht einzusetzen. Sind die Verarbeitungsvorgänge unklar, rät der TLfDI von der Benutzung ganz ab. Das gleiche sollte der mündige Bürger beispielsweise auch für smarte Lautsprecher – ein neuer Techniktrend – beachten.

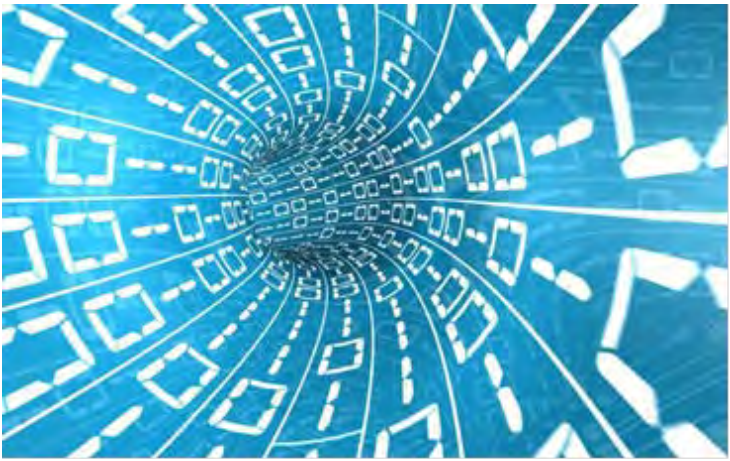


© *fotomek – Runder Tisch / Fotolia.com*

13 Veranstaltungen

13.1 Profiling

PROFILING
Big Data – Small Privacy
Zum Niedergang der Privatsphäre



© Dreaming Andy - Digital flow- fotolia.com

14. Februar 2017
10 Uhr
Augustinerkloster
Erfurt

Das Abfischen von Daten zur Bildung von Persönlichkeitsprofilen zum Beispiel beim Einkaufen, in sozialen Netzwerken, in persönlichen Blogs oder von Kontakt- und Bewegungsdaten ist heutzutage gang und gäbe. Oft geschieht es heimlich.

Aber warum? Wer hat Interesse an den Daten? Zu welchem Zweck werden die Daten genutzt? An wen werden sie weitergegeben?

Wir haben im Nachgang an unsere Profiling-Veranstaltung die von den Referenten freigegebenen Präsentationen als Reader für Sie zusammengefasst. Lassen Sie sich beim Nachlesen nochmals in die Untiefen des Daten-Meeres führen.

Reader zu Tagung zum Nachlesen unter https://www.tlfdi.de/mam/tlfdi/veranstaltungen/reader_querformat_14._februar_2017.pdf

Erstellt aus den Vorträgen von:

Kai Biermann: Journalist bei Zeit Online, Teil des Zeit Online-Teams Investigativ/Daten. Er ist für die Bereiche Internet, Netzpolitik und Datenschutz zuständig.

Prof. Dr. Dorina Gumm: Professorin an der Fachhochschule Lübeck. Sie lehrt u. a. zu den Themen Web Information Systems, IT-Sicherheit sowie digitalisierte Gesellschaft. Im Projekt „Chaos macht Schule“ des CCC engagiert sie sich für Medienkompetenz und Technikverständnis bei Schülern.
Steffen Holly: Er ist Geschäftsfeldleiter Media Management & Delivery am Fraunhofer-Institut für Digitale Medientechnologie IDMT in Ilmenau.
Mike Kuketz: Gründer von Kuketz IT-Security. Er beschäftigt sich seit vielen Jahren intensiv mit den neuesten Entwicklungen im Bereich IT-Sicherheit und Datenschutz. Er ist derzeit u. a. auch Lehrbeauftragter an der Hochschule Karlsruhe und als Referent beim Landesmedienzentrum Baden-Württemberg tätig.
Prof. Dr. Kai-Uwe Sattler: Dekan der Fakultät für Informatik und Automatisierung. Er ist Leiter des Fachgebietes Datenbanken und Informationssysteme an der Technischen Universität Ilmenau.

13.2 Zusammenarbeit mit dem ERFA-Kreis Thüringen

ERFA-Kreise oder ausgeschrieben Erfahrungskreise werden in vielen Bereichen gegründet. Einer davon ist auch der Bereich des Datenschutzes und dort genauer der Bereich der behördlichen und betrieblichen Datenschutzbeauftragten .
Nach § 4f Abs. 1 Bundesdatenschutzgesetz (BDSG) sind bestimmte Unternehmen von Gesetzes wegen gezwungen, einen solchen Datenschutzbeauftragten zu benennen. Etwa dann, wenn besonders viele Personen (mehr als neun) mit der automatisierten (Computer) Verarbeitung von Daten beschäftigt sind oder wenn das Unternehmen in einer besonders benannten Sparte (z. B.: Meinungsforschung) tätig ist.
Dieser zu bestellende Beauftragte bedarf einer entsprechenden Qualifikation (Fachkunde und Zuverlässigkeit) und ist dem Leiter (Behörde) oder der Leitung (Unternehmen) unmittelbar zu unterstellen, wobei er allerdings weisungsfrei zu sein hat.
Dieser Datenschutzbeauftragte hat die Aufgabe, auf die Einhaltung der Vorschriften über den Datenschutz im Unternehmen oder der Behörde, in der er tätig ist, hinzuwirken und stellt damit – dies hat auch die Erfahrung des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) ergeben – ein wichtiges

Instrument zur Verwirklichung datenschutzrechtlicher Vorschriften dar.
Daher engagiert sich der TLfDI ebenfalls im ERFA-Kreis der Thüringer betrieblichen und behördlichen Datenschutzbeauftragten. Regelmäßig wird er zu deren Sitzungen eingeladen, informiert über die neusten Entwicklungen im Bereich Datenschutz und stellt sich den verschiedensten Fachfragen. Auch in diesem Berichtszeitraum sind Teilnahmen erfolgt. Regelmäßig wurde dabei das große Datenschutzthema, die Datenschutz-Grundverordnung, die Ende Mai 2018 Geltung erlangt, behandelt.

14 Vorträge – der TLfDI ist unterwegs!

Ob Datenschutz in Unternehmen, bei freiberuflich Tätigen, in Vereinen und Verbänden oder in medizinischen Einrichtungen, ob Videoüberwachung, Vorratsdatenspeicherung oder die Frage nach dem Umgang mit sozialen Netzwerken – datenschutzrechtliche Themen sind in aller Munde und bewegen die Öffentlichkeit. Die von den Medien immer wieder aufgegriffenen Datenschutzskandale in Wirtschaftsunternehmen zeigen deutlich, dass der Datenschutz im privaten Bereich immer mehr in den Fokus des öffentlichen Interesses gerückt ist. Jeder Einzelne, ob als Kunde oder Arbeitnehmer, achtet mehr denn je auf einen verantwortungsvollen Umgang mit seinen Daten bei privaten Stellen. Umso wichtiger ist es für den TLfDI, dass sich auf der einen Seite die Stellen, die mit personenbezogenen Daten arbeiten, und auf der anderen Seite die Personen, um deren Daten es geht, gut beraten und betreut fühlen. Täglich kommen Anfragen über die Poststelle des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) herein, ob der TLfDI nicht mit einem „Rundum-sorglos-Paket“ für Datenschutz an Materialien und Referenten die eine oder andere bereits geplante Veranstaltung durch seine Vorträge unterstützen kann. Der TLfDI selbst und seine Mitarbeiter haben im Berichtszeitraum abermals an mehr als 50 (!) Diskussions- und Vortragsveranstaltungen teilgenommen und dabei über datenschutzrechtliche Themen referiert. Eine Auswahl der Vorträge im nicht-öffentlichen Bereich finden Sie auf den nächsten Seiten.

Intelligente Netze und Mess-Systeme
-
Smart Metering als Baustein für Energiewende
und Energieeffizienz ?

FSU Jena

21. Januar 2016



Inhalt:

Rechtliche Rahmenbedingungen in Deutschland
Strommarkt 2.0

Daten-Selbstschutz

Veranstaltung FH Erfurt – Medienscout

27. Januar 2016



Inhalt:

Rechtliche Grundlagen
Bedrohungen des Grundrechts der informationellen Selbstbestimmung
Privatsphäre – Warum?
Selbstschutz
Schutz des Grundrechts
Digitale Selbstverteidigung – Broschüre mit Hinweisen zum Selbstdatenschutz

"Daten-Selbstschutz"

2. Datenschutztag Karl-Volkmar-Stoy-Schule Jena

2. März 2016



Inhalt:

Rechtliche Grundlagen
Bedrohungen des Grundrechts der informationellen Selbstbestimmung
Privatsphäre – Warum?
Selbstschutz
Schutz des Grundrechts
Digitale Selbstverteidigung – Broschüre mit Hinweisen zum Selbstdatenschutz

2. Digitalisierungskonferenz EU-DSGVO

25. August 2016



Inhalt:

Europarechtliche Vorgaben
Ein wenig Dogmatik am Anfang – Typologie der Öffnungsklauseln
Sechs Beispiele für Öffnungsklauseln der DSGVO
Weitere Regelungsbedarfe aufgrund der DSGVO

„Beratungsaufgabe und Sanktionsrisiko“

Referatsleiter Referat 4
Johannes Matzke

Thüringer Zentrum für Existenzgründungen und Unternehmertum (ThEx)
29. September 2016



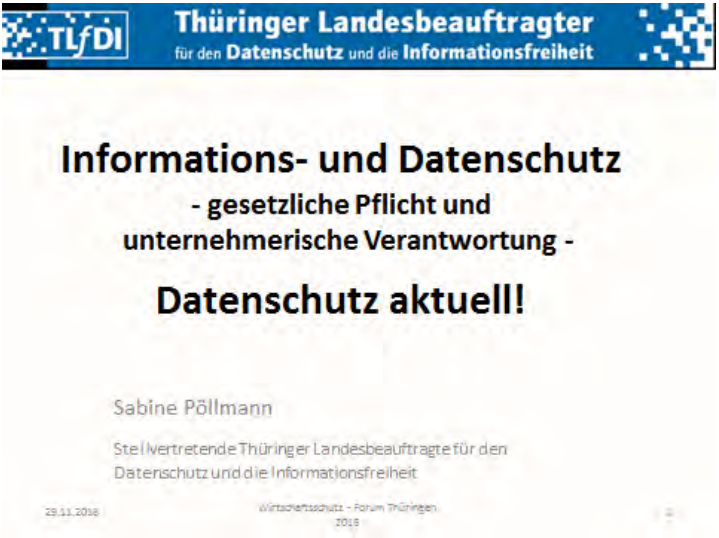
Inhalt:

- Europäische Datenschutzgrundverordnung (EU-DSGVO)
- Unterschiede der DSGVO im Vergleich zum Bundesdatenschutzgesetz (BDSG) für Unternehmen
  Betrieblicher Datenschutzbeauftragter (bDSB)
  Auftragsdatenverarbeitung und DSGVO
  Befugnisse und Sanktionsmöglichkeiten der Aufsichtsbehörde
- Ausblick
  Gesetzgebungsverfahren Bund zum BDSG und Thüringen zum Thüringer Datenschutzgesetz (ThürDSG)

Informations- und Datenschutz
-gesetzliche Pflicht und
unternehmerische Verantwortung-
Datenschutz aktuell!

Wirtschaftsschutz - Forum Thüringen 2016

29. November 2016



Inhalt:

Historischer Hintergrund
IT-Sicherheit vs. Datenschutz: Gemeinsamkeiten und Unterschiede
Was ist das “Internet”?
Gefahren / Angriffsmethoden im Internet
Wie kann ich vorsorgen?

Datenschutz im Krankenhaus

Vortrag im Helios Klinikum Gotha
12. April 2017



Inhalt:

Der TLfDI!
Was ist Datenschutz?
Datenschutz in der Medizin – wichtig, weil:
Datenschutzrecht:
Gesetzliche Pflicht – Was sind die Vorgaben?
Abgrenzung zur Schweigepflichtentbindung
Thüringer Krankenhausgesetz
Technische und organisatorische Maßnahmen, § 9 BDSG
Datenschutz- Grundverordnung (DS-GVO)
Was ändert sich?

Safe-Harbor, die EuGH-Entscheidung vom 06.10.2015 und

Privacy–Shield – was ist da los?

26. April 2017



Inhalt:

Einführung – Datenübermittlung in die USA
Die Safe-Harbor-Entscheidung der EU-Kommission
Standardvertragsklauseln und Binding-Corporate-Rules als Alternativen zu Safe-Harbor
Die Enthüllungen Edward Snowdens und die Folgen
Die EuGH-Entscheidung vom 06.10.2015
Privacy–Shield – alter Wein in neuen Schläuchen?
Ausblick

Datenschutz in der Apotheke
– ein Auszug –

Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit

Apothekertag 2017, Erfurt,
10. Juni 2017



Inhalt:

Datenschutz – Die Aufsicht
Datenschutz – Das Juristische
Datenschutz – Die Problemfelder

„DS-GVO – Neuland?“

GSE Gruppe, MSECD – Datenschutzveranstaltung – Tabarz

20. September 2017



Inhalt:

Einführung – die DS-GVO
Profiling nach Art. 22 DS-GVO
Profiling mit Algorithmen – connected cars
Sensibilisierung von Betroffenen

Datenschutz und Fahrzeug?
Sie fahren gerade Ihrer Privatsphäre davon!

Tagung Autorecht Uni Bielefeld

5. Oktober 2017



Inhalt:

Informationsflüsse im Auto
Rechtsgrundlagen des Datenschutzes
Rechtliche Problemfelder und die Sicht des Datenschutzes

Die Neuerungen der DS-GVO
Im Hinblick auf vereinsrelevante Themen

Fortbildungsveranstaltung beim Landessportbund e. V. Erfurt

28. Oktober 2017



Inhalt:

Rechtsgrundlagen des Datenschutzes
Allgemeines zur DS-GVO
Rechtsnatur der DS-GVO
Definition personenbezogener Daten, Art. 4 DS-GVO
Grundsätze für die Verarbeitung Art. 5 DS-GVO
Rechtmäßigkeit der Verarbeitung personenbezogener Daten, Art. 6 DS-GVO
Rechtmäßigkeit der Verarbeitung personenbezogener Daten, Art. 9 DS-GVO
Betroffenenrechte
Pflichten des Verantwortlichen
Effektive Durchsetzung
Fazit

Anlagen

Anlage 1

Beschluss der obersten Aufsichtsbehörden im Datenschutz im nicht-öffentlichen Bereich

(Düsseldorfer Kreis am 13./14. September 2016)

Fortgeltung bisher erteilter Einwilligungen unter der Datenschutz-Grundverordnung

Bisher erteilte Einwilligungen gelten fort, sofern sie der Art nach den Bedingungen der Datenschutz-Grundverordnung entsprechen (Erwägungsgrund 171, Satz 3 Datenschutz-Grundverordnung).

Bisher rechtswirksame Einwilligungen erfüllen grundsätzlich diese Bedingungen.

Informationspflichten nach Artikel 13 Datenschutz-Grundverordnung müssen dafür nicht erfüllt sein, da sie keine Bedingungen im Sinne des genannten Erwägungsgrundes sind.

Besondere Beachtung verdienen allerdings die folgenden Bedingungen der Datenschutz-Grundverordnung; sind diese Bedingungen nicht erfüllt, gelten bisher erteilte Einwilligungen nicht fort:

- Freiwilligkeit („Kopplungsverbot“, Artikel 7 Absatz 4 in Verbindung mit Erwägungsgrund 43 Datenschutz-Grundverordnung),

- Altersgrenze: 16 Jahre (soweit im nationalen Recht nichts anderes bestimmt wird; Schutz des Kindeswohls, Artikel 8 Absatz 1 in Verbindung mit Erwägungsgrund 38 Datenschutz-Grundverordnung).

Anlage 2

Entschließung
der 91. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 6./7. April 2016 in Schwerin

Wearables und Gesundheits-Apps –
Sensible Gesundheitsdaten effektiv schützen!

Die Datenschutzkonferenz tritt für einen effektiven Schutz der Persönlichkeitsrechte der Nutzerinnen und Nutzer von Wearables und Gesundheits-Apps ein. Einer repräsentativen Umfrage zufolge soll bereits knapp ein Drittel der Bevölkerung ab 14 Jahren sogenannte Fitness-Tracker zur Aufzeichnung von Gesundheitswerten und persönlichen Verhaltensweisen nutzen. Am Körper getragene Kleincomputer (sog. Wearables) und auf mobilen Endgeräten installierte Anwendungsprogramme (sog. Gesundheits-Apps) sammeln und dokumentieren auswertungsfähige Körperdaten. In der Regel werden diese Daten über das Internet an Hersteller, Internetanbieter und sonstige Dritte weitergeleitet.

Die digitale Sammlung und Auswertung der eigenen gesundheitsbezogenen Daten können durchaus interessante Informationen für Einzelne bieten, die zu einer besseren Gesundheitsversorgung und einem Zugewinn an persönlicher Lebensqualität beitragen können.

Allerdings stehen diesen Chancen auch Risiken, insbesondere für das Persönlichkeitsrecht, gegenüber. Zahlreiche Wearables und Gesundheits-Apps geben die aufgezeichneten Daten an andere Personen oder Stellen weiter, ohne dass die betroffenen Personen hiervon wissen oder dazu eine bewusste Entscheidung treffen. Darüber hinaus können Bedienungsfehler oder unzureichende technische Funktionalitäten dazu führen, dass Gesundheitsinformationen ungewollt preisgegeben werden. Einige Angebote weisen erhebliche Sicherheitsdefizite auf, so dass auch Unbefugte sich Zugriff auf die Gesundheitsdaten verschaffen können. Für bestimmte Situationen besteht überdies das Risiko, dass Einzelne aufgrund massiver gesellschaftlicher, sozialer oder ökonomischer Zwänge nicht frei über die Nutzung derartiger Technologien entscheiden können. Zum notwen-

digen Schutz von Gesundheitsdaten bei Wearables und Gesundheits-Apps weist die Datenschutzkonferenz auf folgende Gesichtspunkte hin:

Die Grundsätze der Datenvermeidung und Datensparsamkeit sind zu beachten. Insbesondere Hersteller von Wearables und Gesundheits-Apps sind aufgerufen, datenschutzfreundliche Technologien und Voreinstellungen einzusetzen (Privacy by Design and Default). Hierzu gehören Möglichkeiten zur anonymen bzw. pseudonymen Datenverarbeitung. Soweit eine Weitergabe von Gesundheits- und Verhaltensdaten an Dritte nicht wegen einer medizinischen Behandlung geboten ist, sollten Betroffene sie technisch unterbinden können (lediglich lokale Speicherung).
Die Datenverarbeitungsprozesse, insbesondere die Weitergabe von Gesundheits- und Verhaltensdaten an Dritte, bedürfen einer gesetzlichen Grundlage oder einer wirksamen und informierten Einwilligung. Sie sind transparent zu gestalten. Für das Persönlichkeitsrecht riskante Datenverwendungen, insbesondere Datenflüsse an Dritte, sollten für die Nutzerinnen und Nutzer auf einen Blick erkennbar sein. Beispielsweise könnte die Anzeige des Vernetzungsstatus die aktuellen Weitergabe-Einstellungen veranschaulichen. Eine solche Verpflichtung zur erhöhten Transparenz sollte gesetzlich verankert werden.
Einwilligungserklärungen und Verträge, die unter Ausnutzung eines erheblichen Verhandlungsungleichgewichts zwischen Verwendern und den betroffenen Personen zustande kommen, sind unwirksam und liefern keine Rechtsgrundlage für Verarbeitungen. Das gilt namentlich für besonders risikoträchtige Verwendungszusammenhänge, etwa in Beschäftigungs- und Versicherungsverhältnissen.
Verbindliche gesetzliche Vorschriften zur Datensicherheit, insbesondere zur Integrität und Vertraulichkeit von Daten, können nicht durch Verträge oder durch Einwilligungserklärungen abbedungen werden.
Wer aus eigenen Geschäftsinteressen gezielt bestimmte Wearables und Gesundheits-Apps in den Umlauf bringt oder ihren Vertrieb systematisch unterstützt, trägt eine Mitverantwortlichkeit für die rechtmäßige Ausgestaltung solcher Angebote. In diesem Sinne Mitverantwortliche haben sich zu vergewissern, dass die Produkte verbindlichen Qualitätsstandards an IT-Sicherheit, Funktionsfähigkeit sowie an Transparenz der Datenverarbeitung genügen.

Die Datenschutzkonferenz fordert den Gesetzgeber auf zu prüfen, ob und inwieweit im Zusammenhang mit Wearables und Gesundheits-Apps die Möglichkeit beschränkt werden sollte, materielle Vorteile von der Einwilligung in die Verwendung von Gesundheitsdaten abhängig zu machen.

Anlage 3

Entschließung zwischen den Konferenzen 2016/2017

Novellierung des Personalausweisgesetzes – Änderungen müssen bürger- und datenschutzfreundlich realisiert werden!
(Umlaufentschließung vom 24. Januar 2017)

Die Bundesregierung plant grundlegende Änderungen des Personalausweisrechts. Nach dem vom Bundeskabinett beschlossenen Gesetzentwurf (BR-Drs. 787/16) werden das Recht auf informationelle Selbstbestimmung der Bürgerinnen und Bürger übergangen und Datenschutz sichernde Standards unterlaufen. Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder fordert daher insbesondere folgende datenschutzrechtliche Anforderungen zu berücksichtigen:

- Die obligatorische Aktivierung der eID-Funktion ist dann hinnehmbar, wenn dauerhaft sichergestellt ist, dass daraus keine verpflichtende Nutzung der eID-Funktion des Personalausweises resultiert. Die Entscheidung über die Nutzung der eID-Funktion muss allein bei den Bürgerinnen und Bürgern liegen. Deren Selbstbestimmungsrecht muss gewahrt bleiben.
- An der bisherigen Verpflichtung der Ausweisbehörden, Bürgerinnen und Bürger über die eID-Funktion des Personalausweises schriftlich zu unterrichten, sollte festgehalten werden. Nur durch eine bundesweit einheitliche Vorgabe zu einer solchen Information wird sichergestellt, dass alle Bürgerinnen und Bürger in hinreichend verständlicher Form aufgeklärt werden.
- Vor einer Datenübermittlung aus dem Personalausweis müssen die Bürgerinnen und Bürger Kenntnis über den Zweck der Übermittlung erhalten; zur Wahrnehmung des Rechts auf informationelle Selbstbestimmung müssen die Betroffenen stets - wie bislang - nachvollziehen können, in welchem konkreten Kontext ihre Identitätsdaten übermittelt werden. Zudem sollte die bisherige Möglichkeit, die Übermittlung einzelner Datenkategorien auszuschließen, beibehalten werden.
- Die Einführung von organisationsbezogenen Berechtigungszertifikaten bei Diensteanbietern wird abgelehnt. Um sicherzustellen, dass Diensteanbieter nur die für den jeweiligen Geschäftsprozess erforderlichen Angaben übermittelt bekommen, sollte an

der aktuellen Rechtslage festgehalten werden, nach der der antragstellende Diensteanbieter die Erforderlichkeit der aus der eID-Funktion des Personalausweises zu übermittelnden Angaben nachweisen muss und an den jeweils festgelegten Zweck gebunden ist.

- Berechtigungszertifikate dürfen nur an Diensteanbieter erteilt werden, die Datenschutz und Datensicherheit gewährleisten. Daher sollten antragstellende Diensteanbieter nach wie vor durch eine Selbstverpflichtung die Erfüllung dieser Anforderungen schriftlich bestätigen und nachweisen müssen.
- Die maßgeblichen Regelungen für die mit der Anlegung und Nutzung von Servicekonten einhergehende Erhebung und Verarbeitung von Identitätsdaten aus dem Personalausweis sowie die sicherheitstechnischen Rahmenbedingungen sollten im Personalausweisgesetz getroffen werden.
- Die Voraussetzungen für die Erstellung und Weitergabe von Personalausweisablichtungen sollten gesetzlich konkreter normiert werden. Insbesondere das Prinzip der Erforderlichkeit ist durch eine verpflichtende Prüfung der Notwendigkeit der Anfertigung einer Ablichtung sowie durch eine Positivliste von Erlaubnisgründen zu stärken. Die Einwilligung der Betroffenen als alleinige Voraussetzung birgt die Gefahr, dass in der Praxis Ablichtungen angefertigt werden, obwohl sie nicht erforderlich sind. Zudem dürfte fraglich sein, ob betroffene Personen in eine solche Maßnahme stets informiert und freiwillig einwilligen können.
- Die zum 1. Mai 2021 vorgesehene Einführung eines nahezu voraussetzungslosen Abrufs des Lichtbildes im automatisierten Verfahren durch die Polizeibehörden des Bundes und der Länder sowie die Verfassungsschutzbehörden und Nachrichtendienste wird abgelehnt. Bisher dürfen zur Verfolgung von Straftaten und Verkehrsordnungswidrigkeiten insbesondere die Polizei- und Ordnungsbehörden Lichtbilder automatisiert abrufen, wenn die Personalausweisbehörde nicht erreichbar ist und ein weiteres Abwarten den Ermittlungszweck gefährdet. Diese gesetzlichen Einschränkungen für das Abrufverfahren sollen nun entfallen. Zudem sollen alle Nachrichtendienste künftig voraussetzungslos Lichtbilddaten abrufen können. Die bisherige Rechtslage ist völlig ausreichend.

Anlage 4

Pressemitteilung
vom 19. Mai 2016

Gericht bestätigt: Videoüberwachung durch Private in öffentlich zugänglichen Räumen meldepflichtig!

Wie aus einer Pressemitteilung des Unabhängigen Datenschutzzentrums Saarland zu entnehmen ist, stellt ein Urteil des Verwaltungsgerichts Saarland vom 18. Mai 2016 fest, dass der Betrieb von Wildbeobachtungskameras grundsätzlich dem Anwendungsbereich des Bundesdatenschutzgesetzes (BDSG) unterfällt und das Erheben, Verarbeiten oder Nutzen der mit einer Wildkamera erstellten Aufnahmen eine automatisierte Verarbeitung darstellen, sofern hiervon personenbezogene Daten möglicherweise betroffen sind. Damit sind die Kameras gemäß § 4d Abs. 1 BDSG meldepflichtig (siehe auch: https://www.tlfdi.de/tlfdi/themen/video/).
Auch nicht-öffentliche Stellen in Thüringen, die eine solche Kamera einsetzen wollen, müssen dies zuvor dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) als zuständige Aufsichtsbehörde melden, wenn sie keinen betrieblichen Datenschutzbeauftragten haben. Der Inhalt der erforderlichen Meldepflicht ergibt sich aus § 4e BDSG. Damit bestätigt das Verwaltungsgericht die vom TLfDI vertretene Position.
Nach Auffassung des TLfDI hat das Urteil auch eine weitreichende Bedeutung für den Einsatz von **allen übrigen Videoüberwachungsanlagen** durch private Stellen, die (teilweise) öffentlich zugängliche Räume beobachten. Auch diese Stellen sind gegenüber dem TLfDI meldepflichtig.

Anlage 5

Pressemitteilung
vom 19. September 2017

Meldepflicht für (Wild-)Kameras bestätigt!

Bereits mit Urteil vom 18. Mai 2016 stellte das Verwaltungsgericht Saarland fest, dass die Videoüberwachung mittels Wildbeobachtungskameras durch nicht-öffentliche Stellen **(u. a. natürliche und juristische Personen des Privatrechts)** grundsätzlich der Meldepflicht des § 4d Abs. 1 Bundestatenschutzgesetz (BDSG) unterfällt. Die gegen das Urteil eingelegte Berufung von drei Jägern wurde mit Urteil vom 14. September 2017 durch das **Oberverwaltungsgericht Saarland** abgewiesen und die **Meldepflicht für Wildtierkameras bestätigt**. Die Revision gegen das Urteil wurde nicht zugelassen.

Auch der TLfDI vertritt, wie schon seit seiner Pressemitteilung vom 19. Mai 2016, die Auffassung, dass Wildtierkameras der Meldepflicht unterfallen.

Was allerdings für Wildkameras gilt, muss für alle anderen Kameras erst recht gelten:
Nicht-Öffentliche Stellen in Thüringen müssen Kameras vor dem Einsatz dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) als zuständige Aufsichtsbehörde melden, sofern sie keinen betrieblichen Datenschutzbeauftragten bestellt haben. Der Inhalt der Meldung ergibt sich aus § 4e BDSG. Der TLfDI stellt auf seiner Website entsprechende Meldeformulare zur Verfügung:
(https://www.tlfdi.de/mam/tlfdi/datenschutz/video/tlfdi_meldeformular_v_.pdf).

„Bürgerinnen und Bürger sowie Unternehmen sollten dieser bußgeldbewehrten Meldepflicht rechtsbewusst nachkommen – für Fragen /Informationen stehe ich natürlich jederzeit zur Verfügung!“ – so Dr. Lutz Hasse.

Anlage 6

Pressemitteilung
vom 24. November 2017

Microsoft trifft TLfDI
-Wirtschaft und Datenschutzaufsicht – geht das zusammen?-

Der TLfDI, Dr. Lutz Hasse, ist Bundesvorsitzender des Arbeitskreises Datenschutz und Bildung aller Landesdatenschutzbeauftragten. In diesem Kreis werden derzeit bundesweite Lösungen etwa für Fragen erarbeitet, die sich im Zusammenhang mit Medienkompetenz von Lehrern und Schülern, aber auch mit Lernplattformen und digitalen „Schul-Büchern“ aufdrängen. Einer der großen Akteure in diesem Segment ist Microsoft, z. B. als bedeutender Cloud-Anbieter. In einem von der Wirtschaft und Politik aufmerksam beobachteten Prozess gehen der Global Player und die Datenschutzaufsichtsbehörden in Erfurt aufeinander zu, um gemeinsam datenschutzkonforme Lösungen zu finden.

Dr. Lutz Hasse: „Wir praktizieren ein neues Modell des Umgangs. Wir agieren nicht als Gegenspieler, sondern richten gemeinsam Wirtschaftsinteressen am Datenschutzrecht aus. Ohne gegenseitiges Vertrauen ist das nicht möglich – Microsoft ist hier zukunftsweisende Schritte gegangen, die Nachahmung finden sollten. Win-win für alle Beteiligten!“

Anlage 7

Pressemitteilung
vom 27. November 2017

Immelborn – AdActa

Seit kurzem liegt er vor: der **Zwischenbericht** des Untersuchungsausschusses 6/2 „Aktenlager Immelborn“ (Drucksache 6/4641). Beim Versuch, den Wertungsteil des Zwischenberichts zu verhindern, scheiterte die CDU-Fraktion vor dem Thüringer Verfassungsgerichtshof. Die Hauptfrage der Untersuchung lautete, ob der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) das damalige Thüringer Innenministerium (TIM) auf Amtshilfe zur Beräumung des Aktendepots verklagt habe, um dem damaligen Innenminister Geibert zu schaden. Das **Fazit** des **Zwischenberichtes** lautet: „Der dem Auftrag des Untersuchungsausschusses zugrunde liegende **Verdacht**, der TLfDI habe die Klage erhoben, um im damals anstehenden Wahlkampf dem politischen Konkurrenten in Gestalt des von ihm geführten TIM schaden zu wollen, konnte durch die die bisherige Beweisaufnahme **nicht erhärtet** werden.“
Ferner förderte der Zwischenbericht auch **andere wichtige Tatsachen und Feststellungen** ans Licht:
1. Die Zustellung der Bescheide des TLfDI durch **öffentliche Bekanntmachung** war **rechtmäßig** und erfolgte an den **richtigen Adressaten**.
2. Die getroffenen Maßnahmen des TLfDI waren **verhältnismäßig**.
3. Die **Ersatzvornahme** durch den TLfDI wird von der **Fachliteratur gestützt**.
4. Die **Polizei wollte** dem TLfDI **helfen**, wurde durch **Einwirkung der Hausleitung des TIM indes daran gehindert**.
5. Die Hausleitung des TIM **ließ gezielt Ablehnungsgründe gegen das Amtshilfegesuch generieren**, etwa: statt der vom TLfDI geforderten 10 Mann für 10 Tage, ließ die Hausleitung des TIM bei der Polizei anfragen, ob denn **100 Mann für 30 Tage** leistbar wären, **um dort eine ablehnende Haltung hervorzurufen**.
6. Das **TIM verweigerte dem TLfDI einen konstruktiven Dialog** völlig.
7. Das **Amtshilfeersuchen des TLfDI war zulässig und begründet**.

8. Der TLfDI durfte **nicht auf Private verwiesen** werden und die **Erfüllung polizeilicher Aufgaben** wäre durch die Amtshilfe **nicht gefährdet** gewesen.
9. Die **Bestellung des Nachtragsliquidators erfolgte zügig und rechtskonform**.
10. Für die **Beräumung des Aktenlagers entstanden dem Freistaat keine Kosten**.

Anlage 8

Kurzpapier Nr. 1
Verzeichnis von Verarbeitungstätigkeiten –Art. 30 DS-GVO

Dieses Kurzpapier der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz –DSK) dient als erste Orientierung insbesondere für den nicht-öffentlichen Bereich, wie nach Auffassung der DSK die Datenschutz-Grundverordnung (DS-GVO) im praktischen Vollzug angewendet werden sollte. Diese Auffassung steht unter dem Vorbehalt einer zukünftigen – möglicherweise abweichenden – Auslegung des Europäischen Datenschutzausschusses.

Altes Recht = neues Recht?
Das aus dem BDSG bekannte Verfahrensverzeichnis (§ 4g Abs. 2 und 2a BDSG; dort „Übersicht" genannt) wird mit der DS-GVO abgelöst durch ein (schriftliches oder elektronisches) Verzeichnis aller Verarbeitungstätigkeiten mit personenbezogenen Daten. Dieses Verzeichnis betrifft sämtliche – auch teilweise – automatisierte Verarbeitungen sowie nichtautomatisierte Verarbeitungen personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Grundsätzlich ist jeder Verantwortliche (z. B. Unternehmen, Freiberufler, Verein) und – neu – auch jeder Auftragsverarbeiter zur Erstellung und Führung eines solchen Verzeichnisses verpflichtet. Es wird in der Praxis wegen der Unterschiede bei den eingesetzten Verfahren notwendigerweise oft aus einer Reihe von Einzelbeiträgen bestehen müssen. Das Verfahrensverzeichnis wird somit die Summe der einzelnen Verfahrensbeschreibungen sein.

Stellen mit weniger als 250 Mitarbeitern
Unternehmen und Einrichtungen mit weniger als 250 Mitarbeitern müssen kein Verzeichnis von Verarbeitungstätigkeiten führen, es sei denn, der Verantwortliche bzw. Auftragsverarbeiter führt Verarbeitungen personenbezogener Daten durch,

- die ein Risiko für die Rechte und Freiheiten der betroffenen Personen bergen (dazu gehören regelmäßig Fälle von Scoring und Überwachungsmaßnahmen) oder
- die nicht nur gelegentlich erfolgen (z. B. die regelmäßige Verarbeitung von Kunden- oder Beschäftigtendaten) oder

- die besondere Datenkategorien gemäß Art. 9 Abs. 1 DS-GVO (Religionsdaten, Gesundheitsdaten, usw.) oder strafrechtliche Verurteilungen und Straftaten im Sinne des Art. 10 DS-GVO betreffen.

Die Pflicht zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten besteht also bereits dann, wenn mindestens eine der genannten Fallgruppen erfüllt ist. Da es anders als in Art. 35 DS-GVO (Datenschutz-Folgenabschätzung) nicht darauf ankommt, dass es sich voraussichtlich um ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen handelt, sondern jedes Risiko für die Rechte und Freiheiten bezüglich der Verarbeitung zu betrachten ist, wird vielfach das Erstellen eines Verzeichnisses von Verarbeitungstätigkeiten geboten sein.

Kein öffentliches Verzeichnis und keine Meldepflicht mehr

Anders als im bisherigen BDSG ist eine Möglichkeit für jedermann, in das Verzeichnis von Verarbeitungstätigkeiten Einsicht zu nehmen, nach der DS-GVO nicht vorgesehen. Ebenso entfallen mit der DS-GVO die bisher in § 4d und § 4e BDSG geregelten Meldepflichten von manchen Unternehmen an die Aufsichtsbehörde. Erstellt und vorgehalten werden müssen die Verzeichnisse dennoch, da sie den Aufsichtsbehörden jederzeit auf Anfrage zur Verfügung zu stellen sind (siehe Art. 30 Abs. 4 DS-GVO und ErwGr. 82).

Inhalt des Verzeichnisses für Verantwortliche (Art. 30 Abs. 1 DS-GVO)

Das Verzeichnis der Verantwortlichen muss nach Art. 30 Abs. 1 DS-GVO wesentliche Angaben zur Verarbeitung beinhalten wie z. B. die Zwecke der Verarbeitung und eine Beschreibung der Kategorien der personenbezogenen Daten, der betroffenen Personen und der Empfänger. Verantwortliche Stellen, die bereits jetzt über ein strukturiertes Verfahrensverzeichnis oder eine strukturierte Datenschutzdokumentation zu den Verfahren verfügen, sollten mit den geforderten Pflichtangaben des neuen Artikels aus der DS-GVO keine Probleme haben.

Inhalt des Verzeichnisses für Auftragsverarbeiter (Art. 30 Abs. 2 DS-GVO)

Ein Verzeichnis beim Auftragsverarbeiter zu allen Kategorien der von ihm im Auftrag eines Verantwortlichen durchgeführten Tätig-

keiten der Verarbeitung war vom BDSG bislang nicht vorgeschrieben. Nach Art. 30 Abs. 2 DS-GVO ist ein solches Verzeichnis jedoch künftig zu erstellen. Auch hier sind die Pflichtangaben überschaubar, so dass der Aufwand, dieses Verzeichnis zu erstellen, als eher gering einzustufen sein wird.

Beschreibung technischer und organisatorischer Maßnahmen
Art. 30 Abs. 1 lit. g und Art. 30 Abs. 2 lit. d DS-GVO geben vor, dass das Verzeichnis, wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1 DS-GVO enthalten soll. Wie detailliert diese Beschreibung sein muss, lässt sich der DS-GVO nicht unmittelbar entnehmen. Jedenfalls sollte die Beschreibung der Maßnahmen nach Art. 32 DS-GVO so konkret erfolgen, dass die Aufsichtsbehörden eine erste Rechtmäßigkeitsüberprüfung vornehmen können.

Rechtsfolgen bei Verstoß
Verstöße durch eine fehlende oder nicht vollständige Führung eines Verzeichnisses oder das Nichtvorlegen des Verzeichnisses nach Aufforderung durch die Aufsichtsbehörde können nach Art. 83 Abs. 4 lit. a DS-GVO mit einer Geldbuße sanktioniert werden.

Das Verzeichnis als Teil der Rechenschaftspflicht
Mit der Erstellung des Verzeichnisses der Verarbeitungstätigkeiten sind keinesfalls alle von der DS-GVO geforderten Dokumentationspflichten erfüllt. Das Verzeichnis ist nur ein Baustein, um der in Art. 5 Abs. 2 normierten Rechenschaftspflicht zu genügen. So müssen beispielsweise auch das Vorhandensein von Einwilligungen (Art. 7 Abs. 1), die Ordnungsmäßigkeit der gesamten Verarbeitung (Art. 24 Abs. 1) und das Ergebnis von Datenschutz-Folgenabschätzungen (Art. 35 Abs. 7) durch entsprechende Dokumentationen nachgewiesen werden.

Ausblick: Wesentliche Rolle des Verzeichnisses und Muster-Vorlage der Datenschutzaufsichtsbehörden
Das Verzeichnis von Verarbeitungstätigkeiten nach der DS-GVO wird wie die bisherigen internen Verfahrensverzeichnisse eine wesentliche Rolle spielen, um datenschutzrechtliche Vorgaben überhaupt einhalten zu können. Nur wer die eigenen Verarbeitungsprozesse kennt, kann gezielt Maßnahmen ergreifen, um eine rechtmäßi-

ge Verarbeitung personenbezogener Daten sicherstellen zu können. Die deutschen Aufsichtsbehörden werden im Jahr 2017 eine Muster-Vorlage sowie weitere Hinweise für ein Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 DS-GVO bereitstellen.

Unsere Empfehlung
Es ist ratsam, rechtzeitig im eigenen Interesse ein vollständiges Verzeichnis von Verarbeitungstätigkeiten zu erstellen. Das Verzeichnis von Verarbeitungstätigkeiten dient als wesentliche Grundlage für eine strukturierte Datenschutzdokumentation und hilft dem Verantwortlichen dabei, gemäß Art. 5 Abs. 2 DS-GVO nachzuweisen, dass die Vorgaben aus der DS-GVO eingehalten werden (Rechenschaftspflicht). Die Übergangszeit bis zur Geltung der DS-GVO am 25. Mai 2018 sollte dazu genutzt werden, die bereits bestehende Verfahrensdokumentation an die neu-en Anforderungen anzupassen.

Anlage 9

Kurzpapier Nr. 2
Aufsichtsbefugnisse/Sanktionen

Dieses Kurzpapier der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz –DSK) dient als erste Orientierung insbesondere für den nicht-öffentlichen Bereich, wie nach Auffassung der DSK die Datenschutz-Grundverordnung (DS-GVO) im praktischen Vollzug angewendet werden sollte. Diese Auffassung steht unter dem Vorbehalt einer zukünftigen – möglicherweise abweichenden – Auslegung des Europäischen Datenschutzausschusses.

Die DS-GVO stellt den Aufsichtsbehörden einen umfassenden Katalog von Untersuchungs-und Abhilfebefugnissen zur Verfügung, um die Einhaltung datenschutzrechtlicher Bestimmungen durchzusetzen. Neben diesen verwaltungsrechtlichen Maßnahmen können Verstöße auch mit hohen Geldbußen sanktioniert werden.

Untersuchungs- und Abhilfebefugnisse im Verwaltungsverfahren (Art. 58 -GVO)

Gegenüber Verantwortlichen und Auftragsverarbeitern können vorsorgliche Warnungen ausgesprochen werden, wenn diese Datenverarbeitungen beabsichtigen, die voraussichtlich einen Verstoß gegen die Grundverordnung darstellen, bzw. Verwarnungen, wenn mit Datenverarbeitungen bereits gegen die Grundverordnung verstoßen wurde. Darüber hinaus können Verantwortliche und Auftragsverarbeiter künftig im Rahmen eines förmlichen Verwaltungsaktes von den Aufsichtsbehörden angewiesen werden, Betroffenenrechten zu entsprechen, Datenverarbeitungen mit der Grundverordnung in Einklang zu bringen sowie von einem Datenschutzverstoß betroffene Personen entsprechend zu benachrichtigen. Des Weiteren ist künftig auch die Anordnung der Aussetzung der Übermittlung von Daten an einen Empfänger in einem Drittland oder an eine internationale Organisation möglich. Die Befugnis der Aufsichtsbehörden, Beschränkungen und Verbote von Datenverarbeitungen und die Berichtigung oder Löschung bestimmter Daten sowie eine Einschränkung der Verarbeitung solcher Daten anzuordnen, bleibt unbe-

rührt. Nicht zuletzt können mit Inkrafttreten der Grundverordnung Zertifizierungen seitens der Aufsichtsbehörden selbst widerrufen oder Zertifizierungsstellen angewiesen werden, erteilte Zertifizierungen zu widerrufen oder neue Zertifizierungen nicht zu erteilen. Zusätzlich zu oder anstelle all dieser Maßnahmen können Verstöße gegen die Grundverordnung mit Geldbußen geahndet werden. Zu beachten ist, dass sich die genannten behördlichen Maßnahmen zukünftig nicht nur gegen den Verantwortlichen selbst, sondern auch gegen Auftragsverarbeiter richten können. Die Aufsichtsbehörden haben umfassende Untersuchungsbefugnisse, wobei den Verantwortlichen und auch Auftragsverarbeiter Mitwirkungspflichten treffen. Insbesondere können die Aufsichtsbehörden den Verantwortlichen und Auftragsverarbeiter sowie deren Vertreter anweisen, alle Informationen bereitzustellen, die für die Erfüllung der Aufgaben der Aufsichtsbehörde erforderlich sind. Alle Anordnungen können mit Zwangsmitteln, wie Zwangsgeldern, durchgesetzt werden. Rechtsschutz bei Zweifeln an der Rechtmäßigkeit der Anordnungen der Aufsichtsbehörde ist wie bisher auch im verwaltungsgerichtlichen Verfahren gewahrt.

Verhängung von Geldbußen (Art. 83 DS-GVO)

Zusätzlich zu oder anstelle all dieser Maßnahmen können Verstöße gegen die Grundverordnung mit Geldbußen geahndet werden. Der Rahmen für die Geldbußen wird mit der DS-GVO deutlich erhöht. Dies trägt der gestiegenen Bedeutung des Datenschutzes Rechnung. So können Geldbußen von bis zu 10.000.000 € bzw. bei Unternehmen bis zu 2% des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres verhängt werden (z. B. ist eine weitere erwähnenswerte Neuerung gegenüber der aktuellen Rechtslage, dass unter dem Regime der DS-GVO auch ein Verstoß gegen die Pflicht zur Ergreifung geeigneter und angemessener technischer und organisatorischer Maßnahmen zum Schutz personenbezogener Daten mit einer Geldbuße geahndet werden kann). Bei bestimmten, besonders schwerwiegenden Verstößen, darunter Verstöße gegen die Datenverarbeitungsgrundsätze und gegen die Betroffenenrechte oder im Falle einer Verarbeitung ohne Rechtsgrundlage, sind Geldbußen von bis zu 20.000.000 € möglich. Gegen Unternehmen kann diese Grenze sogar noch überschritten werden, nämlich bis zu 4% des weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres.

Für den Fall der Nichtbefolgung einer Anweisung der Aufsichtsbehörde nach Art. 58 Abs. 2 DS-GVO ist ebenfalls die Verhängung einer Geldbuße von bis zu 20.000.000 € oder im Fall eines Unternehmens von bis zu 4% seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres vorgesehen. In allen drei Fallgestaltungen richtet sich die maximale Obergrenze für die Geldbuße danach, welcher der Beträge höher ist.
Hierbei geht die DS-GVO von einem gegenüber Art. 4 Nr. 18 DS-GVO erweiterten Unternehmensbegriff aus. Wie der Begriff „Unternehmen“ im Zusammenhang mit dem Bußgeldverfahren zu verstehen ist, ist Erwägungsgrund (ErwGr.) 150 der DS-GVO zu entnehmen. Danach gilt der aus dem Kartellrecht entlehnte weite, funktionale Unternehmensbegriff nach Art. 101 und 102 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV). Dies hat zur Folge, dass Mutter- und Tochtergesellschaften als wirtschaftliche Einheit betrachtet werden, so dass bei der Bemessung des Bußgeldes der Gesamtumsatz der Unternehmensgruppe zu Grunde gelegt wird. Nach dem Wortlaut der DS-GVO reicht es für die Zurechnung eines Verstoßes zu einem Unternehmen aus, dass ein Beschäftigter des Unternehmens oder auch ein für das Unternehmen agierender externer Beauftragter gehandelt hat. Die Zurechnung ist damit nicht mehr wie bisher (vgl. § 30 OWiG) auf Handlungen gesetzlicher Vertreter oder anderer Leitungspersonen des Unternehmens begrenzt. Für die Zumessung der Geldbußen gilt zuvörderst der Grundsatz, dass die Geldbußen wirksam, verhältnismäßig und abschreckend sein müssen. Art. 83 Abs. 2 S. 2 DS-GVO enthält eine Auflistung von Kriterien, die bei der Entscheidung über die Verhängung und die Höhe einer Geldbuße (ggf. auch einem Absehen davon, vgl. ErwGr. 148) gebührend im Einzelfall berücksichtigt werden sollen. Neben Art, Schwere und Dauer des Verstoßes ist unter anderem auch zu berücksichtigen, welche Art von Daten verarbeitet wurde sowie ob früher angeordnete Maßnahmen vom Verantwortlichen eingehalten wurden. Zu berücksichtigen ist künftig auch die Art und Weise, wie der Verstoß der Aufsichtsbehörde bekannt wurde, insbesondere, ob und wie die Verantwortlichen mit den Aufsichtsbehörden zusammen gearbeitet haben, um Verstößen abzuhelfen und ihre möglichen nachteiligen Auswirkungen zu mindern, und ob sie die Verstöße eigenständig mitgeteilt haben. Ferner ist auch der Grad der Verantwortung des Verantwortlichen bzw. Auftragsverarbeiters unter Berücksichtigung der von ihm getroffenen technischen und organisatorischen Maß-

nahmen ein zu berücksichtigendes Kriterium. Mithin wird im Einzelfall zu überprüfen sein, inwieweit ein Unternehmen im Rahmen seiner internen Organisation, etwa durch Ausgestaltung seiner Strukturen, Arbeitsprozesse und Kontrollmechanismen, Vorkehrungen getroffen hat, die dazu dienen, die Einhaltung der datenschutzrechtlichen Anforderungen sicherzustellen, bzw. inwieweit die interne Organisation diesbezüglich Mängel aufweist. Zudem können jegliche anderen erschwerenden oder mildernden Umstände im jeweiligen Fall, wie unmittelbar oder mittelbar durch den Verstoß erlangte finanzielle Vorteile oder vermiedene Verluste, Berücksichtigung finden. Abzuwarten bleibt, in welcher Form der Europäische Datenschutzausschuss seinen Auftrag aus Art. 70 Abs. 1 lit. k DS-GVO umsetzen wird. Danach obliegt ihm die Aufgabe, Leitlinien für die Aufsichtsbehörden in Bezug auf die Anwendung von Maßnahmen nach Art. 58 Abs. 1, 2 und 3 DS-GVO und die Festsetzung von Geldbußen gemäß Art. 83 DS-GVO zu erlassen.

Anlage 10

Kurzpapier Nr. 3
Verarbeitung personenbezogener Daten für Werbung

Dieses Kurzpapier der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) dient als erste Orientierung insbesondere für den nicht-öffentlichen Bereich, wie nach Auffassung der DSK die Datenschutz-Grundverordnung (DS-GVO) im praktischen Vollzug angewendet werden sollte. Diese Auffassung steht unter dem Vorbehalt einer zukünftigen – möglicherweise abweichenden – Auslegung des Europäischen Datenschutzausschusses.

Keine Detailregelung für Werbung
Mit der DS-GVO fallen alle detaillierten Regelungen des Bundesdatenschutzgesetzes (BDSG) zur Verarbeitung personenbezogener Daten für werbliche Zwecke weg.

Werbung nach Interessenabwägung
Grundlage für die Beurteilung der Zulässigkeit von Werbung ist in Zukunft, abgesehen von einer Einwilligung, eine Interessenabwägung nach Art. 6 Abs. 1 lit. f DS-GVO. Ausgangspunkt für die zu treffende Abwägungsentscheidung ist Erwägungsgrund (ErwGr.) 47 DS-GVO, der u. a. ausführt: „Die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung kann als eine einem berechtigten Interesse dienende Verarbeitung betrachtet werden.“ Ferner gibt ErwGr. 47 DS-GVO im Rahmen der durchzuführenden Interessenabwägung vor, die „vernünftigen Erwartungen der betroffenen Person“, die auf ihrer Beziehung zu dem Verantwortlichen beruhen, in den Abwägungsprozess einzubeziehen. Wann diese Voraussetzungen vorliegen, ist derzeit noch nicht abschließend geklärt. Dem Working Paper der Art. 29 Datenschutzgruppe (WP 217, S. 51), das sich allerdings auf die Datenschutzrichtlinie 95/46/EG bezieht, können insoweit erste Interpretationshinweise entnommen werden. Die vernünftigen Erwartungen der betroffenen Person werden bei Maßnahmen zur werblichen Ansprache maßgebend durch die Informationen nach Art. 13, 14 DS-GVO zu den Zwecken der Datenverarbeitung bestimmt werden. Informiert der Verantwortliche transparent und umfassend über eine vorgesehene werbliche Nutzung der Daten,

geht die Erwartung der betroffenen Person in aller Regel auch dahin, dass ihre Kundendaten entsprechend genutzt werden. Insoweit ist im Rahmen der Interessenabwägung zu berücksichtigen, dass die von Werbung betroffenen Personen ein jederzeitiges und umfassendes Widerspruchsrecht haben (Art. 21 Abs. 2 DS-GV0), auf das sie ausdrücklich hinzuweisen sind (Art. 21 Abs. 4 DS-GVO). Der Werbewiderspruch hat nach Art. 21 Abs. 3 DS-GVO zur Folge, dass personenbezogene Daten für Werbezwecke nicht mehr verarbeitet, insbes. verwendet werden dürfen. Im Übrigen ist zu berücksichtigen, ob die betroffene Person bereits Kunde des Verantwortlichen ist oder dessen Dienste nutzt (ErwGr. 47 DS-GVO). Ferner sind bei der Interessenabwägung auch die allgemeinen Grundsätze aus Art. 5 Abs. 1 DS-GVO zu berücksichtigen, also insbesondere:

- faire Verfahrensweise
- dem Verarbeitungszweck angemessen
- in einer für die betroffene Person nachvollziehbaren Weise (insbesondere Nennung der Quelle der Daten)

Diese Grundsätze sprechen jedenfalls dagegen, Profile zur werblichen Ansprache (Werbescores) zu erstellen, die z. B. Informationen aus sozialen Netzwerken berücksichtigen. Eingriffsintensivere Maßnahmen wie Profilbildung sprechen eher dafür, dass ein Interesse der betroffenen Person am Ausschluss der Datenverarbeitung überwiegt. Unabhängig von der Interessenabwägung müssen die Informationspflichten nach den Art. 13, 14 DS-GVO eingehalten werden.

Ohne Einwilligung keine werbliche Nutzung besonderer Datenkategorien

Art. 9 DS-GVO enthält keine Erlaubnisnorm für die Verarbeitung besonderer Kategorien personenbezogener Daten für Zwecke der Werbung. Dies ist nur bei Vorliegen einer ausdrücklichen Einwilligung der betroffenen Person zulässig. Von Relevanz ist dies z. B. für Unternehmen und Berufe des Gesundheitswesens (Apotheken, Sanitätshäuser, Optiker, Orthopäden usw.).

Besondere Grenzen aus § 7 UWG

Auch nach neuem Recht wird die Interessenabwägung bei der Nutzung der Kontaktdaten von Verbrauchern für Telefon- und Faxwerbung dazu führen, dass diese weiterhin nur mit einer vorherigen ausdrücklichen Einwilligung erlaubt ist. Alles andere wäre im Hinblick auf die klaren Regelungen in § 7 des Gesetzes gegen den un-

lauteren Wettbewerb (UWG) mit den vernünftigen Erwartungen der Betroffenen (ErwGr. 47 DS-GVO) nicht zu vereinbaren. Ebenso ist eine Kontaktdatennutzung für E-Mail-und SMS-Werbung außerhalb einer Einwilligung nur im Fall der Eigenwerbung bei Bestandskunden unter den Maßgaben von § 7 Abs. 3 UWG zulässig. Im Übrigen bleibt abzuwarten, inwieweit die geplante neue ePrivacy-Verordnung im Bereich der elektronischen Werbung konkrete Regelungen (z. B. ausschließliche Opt-in-Lösung) für werbliche Ansprachen enthalten wird.

Fortgeltung von Einwilligungen
Bisher erteilte Einwilligungen wirken nach Erwägungsgrund 171 der DS-GVO fort, sofern sie der Art nach den Bedingungen der Datenschutz-Grundverordnung entsprechen. Die im Wirtschafts-leben EU-weit vorhandenen Einwilligungen sind auf ihre Wirksamkeit hin zu überprüfen. Dabei ist u. a. von Bedeutung, ob auf Grundlage der neuen Anforderungen nach Art. 7 Abs. 4 der DS-GVO eine freiwillige Erklärung abgegeben und dass die Altersgrenze für die Einwilligungsfähigkeit bei Inanspruchnahme von Diensten der Informationsgesellschaft nach Art. 8 Abs. 1 der DS-GVO berücksichtigt wurde.

„Koppelungsverbot“ bei Einwilligungen für Werbung
Das bisher schon bestehende Koppelungsverbot für Werbung findet sich auch in der DS-GVO wieder, ist aber nicht mehr davon abhängig, ob ein anderer Zugang zu gleichwertigen vertraglichen Leistungen möglich ist. Bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, ist dem Umstand in größtmöglichem Umfang Rechnung zu tragen, ob unter anderem die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrages nicht erforderlich ist (Art. 7 Abs. 4 DS-GVO). Bei „kostenlosen“ Dienstleistungsangeboten, die die Nutzer mit der Zustimmung für eine werbliche Nutzung ihrer Daten „bezahlen“ (z. B. kostenloser E-Mail-Account gegen Zustimmung für Newsletter-Zusendung als „Gegenfinanzierung“), muss diese vertraglich ausbedungene Gegenleistung des Nutzers bei Vertragsabschluss klar und verständlich dargestellt werden. Nur dann besteht keine Notwendigkeit mehr für eine Einwilligung.

Ausblick für den künftigen Umgang mit personenbezogenen Daten für Werbung

Soweit Werbung nicht auf einer wirksamen Einwilligung der betroffenen Person beruht, wird für die Zulässigkeit von Werbung in Zukunft fast ausschließlich die nach Art. 6 Abs. 1 lit. f DS-GVO vorgeschriebene Interessenabwägung maßgeblich sein. Inwieweit es in Europa gelingen wird, die in Deutschland entwickelten Maßstäbe auch unter Geltung der DS-GVO aufrechtzuerhalten, wird sich zeigen. Anzustreben sind für diesen Bereich möglichst EU-weite Verhaltensregeln. Sollte das nicht für die wesentlichen Bereiche der Werbung gelingen, wird mit Leitlinien des Europäischen Datenschutzausschusses auch zu diesem Thema zu rechnen sein.

Anlage 11

Kurzpapier Nr. 4
Datenübermittlung in Drittländer

Dieses Kurzpapier der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) dient als erste Orientierung insbesondere für den nicht-öffentlichen Bereich, wie nach Auffassung der DSK die Datenschutz-Grundverordnung (DS-GVO) im praktischen Vollzug angewendet werden sollte. Diese Auffassung steht unter dem Vorbehalt einer zukünftigen – möglicherweise abweichenden – Auslegung des Europäischen Datenschutzausschusses.

Die DS-GVO sieht für die Übermittlung personenbezogener Daten in ein Land außerhalb der EU/des EWR besondere Regelungen vor: Art. 44 – 49. Länder außerhalb der EU/des EWR werden in der DS-GVO als „Drittländer" bezeichnet, in der Praxis wird auch der Begriff „Drittstaat" verwendet. Bei der Datenübermittlung in ein Drittland muss zunächst überprüft werden, ob unabhängig von den in den Art. 45 ff. geregelten spezifischen Anforderungen an Datenübermittlungen in Drittländer auch alle übrigen Anforderungen der DS-GVO (z. B. Art. 9 Abs. 3) an die in Rede stehende Datenverarbeitung eingehalten werden (1 Stufe). Steht nach diesem Prüfungsschritt einer Verarbeitung nichts entgegen, müssen gemäß Art. 44 zusätzlich die spezifischen Anforderungen der Art. 45 ff. an die Übermittlung in Drittländer beachtet werden (2. Stufe; „2-Stufen-Prüfung"). Dies gilt auch bei einer Weiterübermittlung der personenbezogenen Daten durch die empfangende Stelle im Drittland (Art. 44 S. 1 2. HS (siehe auch Erwägungsgrund (ErwGr.) 101)). Die DS-GVO sieht für Datentransfers in Drittländer folgende Möglichkeiten vor (für öffentliche Stellen gelten im Einzelfall ergänzende Regelungen):

- **Feststellung der Angemessenheit des Datenschutzniveaus im Drittland durch die EU-Kommission (Art. 45 DS-GVO)**
- **Vorliegen geeigneter Garantien (Art. 46 DS-GVO) oder**
- **Ausnahmen für bestimmte Fälle (Art. 49 DS-GVO).**

1. Feststellung der Angemessenheit des Datenschutzniveaus im Drittstaat durch die Kommission (Art. 45 DS-GVO)

Die Kommission hat die Möglichkeit, nach entsprechender Prüfung das Bestehen eines angemessenen Schutzniveaus in einem bestimmten Drittland festzustellen. Die Feststellung kann auch auf ein bestimmtes Gebiet oder einen bestimmten Sektor in dem Drittland oder auch auf bestimmte Datenkategorien beschränkt sein. Ein angemessenes Schutzniveau besteht dann, wenn in dem Drittland auf Grundlage seiner innerstaatlichen Rechtsvorschriften und deren Anwendung, der Existenz und der wirksamen Funktionsweise einer oder mehrerer unabhängiger Aufsichtsbehörden sowie seiner eingegangenen internationalen Verpflichtungen ein Schutzniveau existiert, welches dem in der DS-GVO gewährten Schutzniveau gleichwertig ist. Eine Datenübermittlung auf Grundlage eines solchen Angemessenheitsbeschlusses bedarf keiner weiteren Genehmigung durch die für den Verantwortlichen oder Auftragsverarbeiter zuständige nationale Aufsichtsbehörde. Die DS-GVO sieht eine Fortgeltung der bereits erlassenen Angemessenheitsbeschlüsse vor (Art. 46 Abs. 5 S. 2). Für den EU-US Privacy Shield hat die Kommission die Angemessenheit des Datenschutzniveaus festgestellt (C(2016) 4176 final)).

2. Vorliegen geeigneter Garantien (Art. 46 DS-GVO)

Eine Datenübermittlung in ein Drittland ist weiter zulässig, wenn der Verantwortliche oder Auftragsverarbeiter geeignete Garantien zur Gewähr-leistung eines angemessenen Schutzniveaus vorgesehen hat. Folgende Garantien kommen in Betracht:

a) Verbindliche interne Datenschutzvorschriften (Binding Corporate Rules) (Art. 46 Abs. 2 lit. b, Art. 47)

Verbindliche interne Datenschutzvorschriften (BCR) wurden schon bisher in der Praxis verwendet und sind nun in der DS-GVO (anders als in der noch geltenden EU-Datenschutzrichtlinie 95/46/EG) ausdrücklich als Möglichkeit zur Erbringung „geeigneter Garantien“ für Datenübermittlungen in Drittländer geregelt. Sie können vor allem bei international tätigen Konzernen mit internem Datenfluss (auch) in Drittländer empfehlenswert sein. Dabei legt das Unternehmen Regelungen für den Umgang mit personenbezogenen Daten auch in Drittländern fest. Die BCR müssen einen Schutz bieten, der im Wesentlichen der DS-GVO entspricht. Der Mindest-Inhalt ist in Art. 47 Abs. 2 festgelegt. Zudem müssen die BCR für alle betreffenden Mitglieder der Unternehmensgruppe rechtlich bindend sein und den betroffenen Personen durchsetzbare Rechte gewähren (Art. 47 Abs. 1

lit. a und b). Die Genehmigung der BCR erfolgt gemäß dem Kohärenzverfahren durch die zuständige Aufsichtsbehörde (Art. 47 Abs. 1). Die konkreten Datenübermittlungen auf Grundlage der BCR werden dann nicht mehr einzeln genehmigt.

b) Standarddatenschutzklauseln der Kommission oder einer Aufsichtsbehörde (Art. 46 Abs. 2 lit. c und d)

Schließen der Datenexporteur und der Datenimporteur einen Vertrag unter Verwendung der Standarddatenschutzklauseln der Kommission, ist der darauf basierende Datentransfer ohne weitere Genehmigung durch die Aufsichtsbehörde zulässig (vorbehaltlich der weiteren Anforderungen nach der DS-GVO). Auch den Aufsichtsbehörden ist es möglich, eigene Standarddatenschutzklauseln zu entwerfen. Diese bedürfen der Abstimmung im Kohärenzverfahren und sind anschließend von der Kommission förmlich zu genehmigen.

Die bereits bestehenden EU-Standardvertrags-klauseln gelten gemäß Art. 46 Abs. 5 S. 2 ausdrücklich fort. Sofern die Standarddatenschutzklauseln in unveränderter Form verwendet werden, sind die Datenübermittlungen genehmigungsfrei. Dies gilt auch noch dann, wenn ihnen weitere Klauseln oder zusätzliche Garantien hinzugefügt werden, solange diese weder mittelbar noch unmittelbar im Widerspruch zu den Standarddatenschutzklauseln stehen und die Grundrechte und Grundfreiheiten der betroffenen Personen nicht beschneiden (ErwGr. 109). Bei solchen Hinzufügungen sollten Unternehmen jedoch eine gewisse Vorsicht walten lassen, da im Falle eines inhaltlichen Widerspruchs zu den Standarddatenschutzklauseln die Übermittlung nicht mehr genehmigungsfrei ist.

c) Genehmigte Verhaltensregeln und genehmigter Zertifizierungsmechanismus (Art. 46 Abs. 2 lit. e und f)

Neu hinzugekommen ist die Möglichkeit, Datenübermittlungen auf Grundlage von branchenspezifischen Verhaltensregeln gemäß Art. 40 zu legitimieren, sofern diese mit rechtsverbindlichen und durchsetzbaren Verpflichtungen des Verantwortlichen oder des Auftragsverarbeiters versehen sind und von der zuständigen Aufsichtsbehörde genehmigt worden sind.

Auch Zertifizierungen nach Art. 42 können nun zusammen mit rechtsverbindlichen und durchsetzbaren Verpflichtungen des Verantwortlichen oder des Auftragsverarbeiters als rechtliche Grundlage für einen Datentransfers in ein Drittland herangezogen werden, wenn die Zertifizierungsmechanismen zuvor genehmigt worden sind.

Die europäischen Aufsichtsbehörden werden in der Folgezeit die für eine praktische Anwendung dieser Instrumente notwendigen weiteren Einzelheiten im Hinblick auf rechtliche Rahmenbedingungen und Verfahrensfragen erarbeiten.

d) Einzeln ausgehandelte Vertragsklauseln (Art. 46 Abs. 3)

Ebenso können einzeln ausgehandelte individuelle Vertragsklauseln eine Datenübermittlung in ein Drittland legitimieren, allerdings nur nach Genehmigung der Aufsichtsbehörde und Durchführung des Kohärenzverfahrens nach Art. 63.

e) Rechte der betroffenen Personen

Gemäß Art. 46 Abs. 1 a. E. ist es bei allen in Betracht kommenden geeigneten Garantien im Sinne von Art. 46 zusätzlich erforderlich, den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe einzuräumen.

3. Ausnahmen für bestimmte Fälle (Art. 49 DS-GVO)

Eine Datenübermittlung kann in einer Reihe besonderer, vom Gesetz explizit genannter und abschließender Fälle, auch zulässig sein, wenn weder ein Angemessenheitsbeschluss der Kommission noch geeignete Garantien vorliegen. Die hierfür von der DS-GVO definierten Ausnahmetatbestände sind gemäß ihrem Ausnahmecharakter eng auszulegen.

a) Einwilligung (Art. 49 Abs. 1 UAbs. 1 lit. a)

Eine wirksame Einwilligung der betroffenen Person in die Datenübermittlung in ein Drittland setzt zunächst eine ausdrückliche Einwilligung in die Weitergabe ihrer Daten für den konkreten Fall voraus. Weiter ist die betroffene Person vorher explizit über bestehende mögliche Risiken derartiger Datenübermittlungen aufzuklären, d.h. insbesondere darüber, dass kein angemessenes Datenschutzniveau gegeben ist und Betroffenenrechte ggf. nicht durchgesetzt werden können. Auch ist die betroffene Person darauf hinzuweisen, dass sie die Einwilligung jederzeit widerrufen kann (Art. 7 Abs. 3).

b) Erforderlichkeit zur Vertragserfüllung (Art. 49 Abs. 1 UAbs. 1 lit. b und c)

Eine Datenübermittlung in ein Drittland ist (vorbehaltlich der weiteren Anforderungen der DS-GVO) zulässig, wenn und soweit die Übermittlung zur Erfüllung eines Vertrages mit der betroffenen Person oder zum Abschluss oder zur Erfüllung eines Vertrages im Interesse der betroffenen Person erforderlich ist. Wesentlich ist hier

jeweils die strikte Erforderlichkeit gerade dieser Datenübermittlung zur Erfüllung des Vertragszwecks.

c) Wichtige Gründe des öffentlichen Interesses (Art. 49 Abs. 1 UAbs. 1 lit. d)

Die Übermittlung kann auch zulässig sein, wenn sie aus wichtigen Gründen des öffentlichen Interesses notwendig ist. In Betracht kommen nur wichtige öffentliche Interessen, die im Recht der Europäischen Union oder des Mitgliedstaates, dem der Verantwortliche unterliegt, anerkannt sind (Art. 49 Abs. 4). Wie aus Erwägungsgrund 112 hervorgeht, hatte der Gesetzgeber insoweit insbesondere Datentransfers im Rahmen der internationalen behördlichen Zusammenarbeit im Auge, etwa zwischen Wettbewerbs-, Steuer- oder Zollbehörden.

d) Verfolgung von Rechtsansprüchen (Art. 49 Abs. 1 UAbs. 1 lit. e)

Auch die Verfolgung von Rechtsansprüchen kann eine Datenübermittlung legitimieren, wenn die Datenübermittlung hierzu erforderlich ist. In Erweiterung der bisherigen Regelung im BDSG kommt auch die Geltendmachung von Rechtsansprüchen in außergerichtlichen Verfahren in Betracht (ErwGr. 111).

e) Schutz lebenswichtiger Interessen (Art. 49 Abs. 1 UAbs. 1 lit. f)

Ist die betroffene Person aus physischen oder rechtlichen Gründen nicht in der Lage, ihre Einwilligung zu erteilen, darf die Datenübermittlung dennoch durchgeführt werden, soweit dies zum Schutz ihrer lebenswichtigen Interessen oder derjenigen anderer Personen erforderlich ist.

f) Wahrung zwingender berechtigter Interessen (Art. 49 Abs. 1 UAbs. 2 S. 1)

Im Einzelfall kann eine Datenübermittlung in ein Drittland legitimiert sein, wenn ein zwingendes berechtigtes Interesse des Verantwortlichen an der Übermittlung besteht, die Übermittlung nicht wiederholt erfolgt, nur eine begrenzte Anzahl von Personen betrifft und keine überwiegenden schutzwürdigen Interessen oder Rechte und Freiheiten der betroffenen Person entgegenstehen und der Verantwortliche durch geeignete Garantien den Schutz personenbezogener Daten gewährleistet. Voraussetzung für diese Übermittlungserlaubnis ist ein zwingendes berechtigtes Interesse des Verantwortlichen an der Übermittlung, dem eine heraus-gehobene und besondere Bedeutung zukommt. Zudem muss die Übermittlung unbedingt erforderlich

sein zur Verfolgung dieses berechtigten Interesses. Die Übermittlung darf sich nicht bereits auf einen der oben genannten Erlaubnistatbestände stützen lassen. Wird eine Übermittlung in ein Drittland auf Grundlage eines zwingenden berechtigten Interesses in einem absoluten Einzelfall durchgeführt, ist sowohl die Aufsichtsbehörde als auch die betroffene Person hierüber zu informieren (Art. 49 Abs. 1 UAbs. 2 S. 2 und 3).

Anlage 12

Kurzpapier Nr. 5
Datenschutz-Folgenabschätzung, Art. 35 DS-GVO

Dieses Kurzpapier der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) dient als erste Orientierung, wie nach Auffassung der DSK die Datenschutz-Grundverordnung (DS-GVO) im praktischen Vollzug angewendet werden sollte. Diese Auffassung steht unter dem Vorbehalt einer zukünftigen – möglicherweise abweichenden – Auslegung des Europäischen Datenschutzausschusses.

Auch bei einer rechtmäßigen Verarbeitung personenbezogener Daten entstehen Risiken für die betroffenen Personen. Deswegen sieht die DS-GVO unabhängig von sonstigen Voraussetzungen für die Verarbeitung vor, dass durch geeignete Abhilfemaßnahmen (insbesondere durch technische und organisatorische Maßnahmen (TOMs)) diese Risiken eingedämmt werden. Das Instrument einer Datenschutz-Folgenabschätzung (DSFA) kann hierfür systematisch eingesetzt werden.

Was ist eine Datenschutz-Folgenabschätzung nach DS-GVO?
Eine DSFA ist ein spezielles Instrument zur Beschreibung, Bewertung und Eindämmung von Risiken für die Rechte und Freiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten. Die DSFA ist durchzuführen, wenn die Form der Verarbeitung, insbesondere bei der Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko zur Folge hat. Sie befasst sich insbesondere mit Abhilfemaßnahmen durch die der Schutz personenbezogener Daten sichergestellt und die Einhaltung der Verordnung nachgewiesen werden kann (Art. 35 Abs. 1, 7 DS-GVO sowie ErwGr. 84, 90). Zum Begriff des Risikos, der ein zentrales Konzept der DS-GVO ist, wird es ein eigenes Kurzpapier geben.

Verarbeitungsvorgang als Ankerpunkt
Eine DSFA bezieht sich auf einzelne, konkrete Verarbeitungsvorgänge. Unter Verarbeitungsvorgängen ist die Summe von Daten, Systemen (Hard- und Software) und Prozessen zu verstehen.

Sofern mehrere ähnliche Verarbeitungsvorgänge voraussichtlich ein ähnliches Risiko aufweisen, können diese zusammen bewertet werden (Art. 35 Abs. 1 DS-GVO). Ähnliche Risiken können beispielsweise dann gegeben sein, wenn ähnliche Technologien zur Verarbeitung vergleichbarer Daten(-kategorien) zu gleichen Zwecken eingesetzt werden (vgl. auch ErwGr. 92 DS-GVO). Bei einer gemeinsamen Bewertung von ähnlichen Verarbeitungsvorgängen sind die im Folgenden dargestellten Vorgehensweisen ggf. anzupassen.

Erforderlichkeit einer DSFA

Ob eine DSFA durchzuführen ist, ergibt sich aus einer Abschätzung der Risiken der Verarbeitungsvorgänge („Schwellwertanalyse"). Ergibt diese ein voraussichtlich hohes Risiko, dann ist eine DSFA durchzuführen. Wird festgestellt, dass der Verarbeitungsvorgang kein hohes Risiko aufweist, dann ist eine DSFA nicht zwingend erforderlich. In jedem Fall ist die Entscheidung über die Durchführung oder Nichtdurchführung der DSFA mit Angabe der maßgeblichen Gründe für den konkreten Verarbeitungsvorgang schriftlich zu dokumentieren.

Art. 35 Abs. 3 DS-GVO benennt einige Faktoren, die wahrscheinlich zu einem hohen Risiko i. S. d. Art. 35 Abs. 1 DS-GVO führen. Aufbauend auf den Leitlinien der Artikel-29-Datenschutzgruppe werden die Datenschutzaufsichtsbehörden eine nicht-abschließende Liste mit Verarbeitungstätigkeiten, bei denen eine DSFA durchzuführen ist, veröffentlichen. Auch zur Durchführung der Schwellwertanalyse werden künftig Hinweise zur Verfügung gestellt.

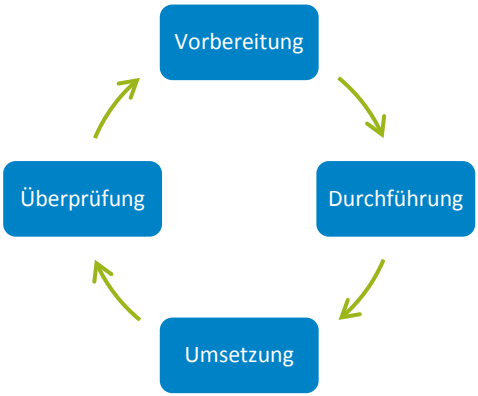
Zeitpunkt der Durchführung einer DSFA

Eine DSFA ist vor der Aufnahme der zu betrachtenden Verarbeitungsvorgänge durchzuführen. Auch bereits bestehende Verarbeitungsvorgänge können unter die Pflicht einer DSFA fallen. Da eine DSFA meist nicht ad hoc in wenigen Tagen erstellt werden kann, muss sie rechtzeitig, beispielsweise unterstützt durch ein allgemeines Datenschutz-Managementsystem, auf den Weg gebracht werden.

Wie kann eine DSFA durchgeführt werden?

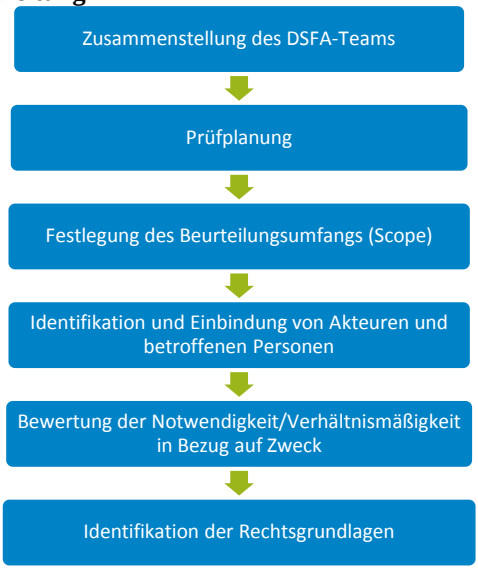
Die formellen Anforderungen an die Durchführung einer DSFA ergeben sich aus der DS-GVO, speziell aus Art. 35 sowie den Erwägungsgründen 84, 90, 91, 92 und 93. Bei der verwendeten Methode wird dem Verantwortlichen mehr Spielraum gelassen. Werden be-

stehende Methoden oder Standards eingesetzt, ist zu beachten, dass die Anforderungen der DS-GVO immer vorrangig zu behandeln sind.
Eine DSFA ist kein einmaliger Vorgang. Sollten sich z .B. neue Risiken ergeben, die Bewertung bereits erkannter Risiken ändern oder wesentliche Änderungen im Verfahren ergeben, die in der DSFA bisher nicht berücksichtigt wurden, so ist die DSFA zu überprüfen und ebenso anzupassen. Um dies zu garantieren, wird ein stetiger, iterativer Prozess der Überprüfung und Anpassung empfohlen:



Die Bestandteile der Hauptprozessschritte werden im Einzelnen nachfolgend dargestellt.

Vorbereitung



1. Zusammenstellung des DSFA-Teams

Eine DSFA kann im Allgemeinen nur von einem interdisziplinären Team erstellt werden, das Kompetenzen im Bereich Datenschutz, Risikoermittlung und Fachprozesse mitbringt. Der Datenschutzbeauftragte steht diesem während des gesamten Prozesses beratend zur Seite. Es kann sinnvoll oder notwendig sein, z. B. Auftragsverarbeiter oder Hersteller von IT-Systemen ebenfalls mit einzubeziehen.

2. Prüfplanung

Da eine DSFA meist ein komplexer Prozess ist, der viele Mitwirkende einbindet, ist eine Prüfplanung (z. B. mit Methoden des Projektmanagements) empfehlenswert.

3. Festlegung des Beurteilungsumfangs (Scope)

Die betrachteten Verarbeitungsvorgänge sind von anderen (Geschäfts-)Prozessen abzugrenzen und ausführlich und abschließend mit allen Datenflüssen zu beschreiben. Wesentlich ist es, die beabsichtigten Zwecke der Verarbeitungsvorgänge festzuhalten.

4. Identifikation und Einbindung von Akteuren und betroffenen Personen

Die Akteure und betroffenen Personen sind zu identifizieren. Bei der Durchführung der DSFA zieht der Verantwortliche den Datenschutzbeauftragten zurate (Art. 35 Abs. 2 DS-GVO). Ggf. holt der Verantwortliche den Standpunkt der betroffenen Personen oder ihrer Vertreter zu der beabsichtigten Verarbeitung ein (Art. 35 Abs. 9 DS-GVO). Dies umfasst beispielsweise die Einbindung von Gremien der Mitbestimmung, z. B. von Betriebsräten.

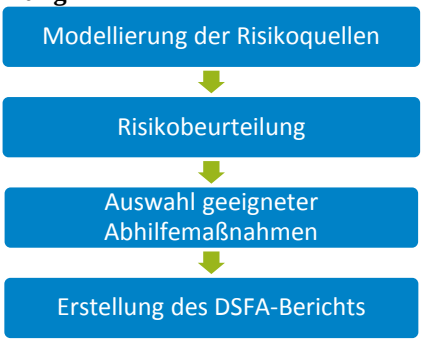
5. Bewertung der Notwendigkeit/Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf ihren Zweck

Die im vorigen Schritt beschriebenen Verarbeitungsvorgänge werden ausgehend von den mit ihnen verfolgten Zwecken daraufhin bewertet, ob der durch sie bewirkte Eingriff in die Rechte und Freiheiten der Betroffenen im Verhältnis zu dem angestrebten Zweck steht, ob sie zum Erreichen der Zwecke tatsächlich notwendig sind oder ob alternative Vorgehensweisen zur Verfügung stehen, die in die Rechte und Freiheiten der Betroffenen weniger stark eingreifen. Ggf. nimmt der Verantwortliche eine Anpassung der Verarbeitungsvorgänge vor, z. B. durch Beschränkung der zu verarbeitenden Daten oder durch Änderung der beteiligten Akteure oder eingesetzten Technologien.

6. Identifikation der Rechtsgrundlagen

Aufbauend auf dem vorigen Schritt können sodann die Rechtsgrundlagen für die zu bewertenden Verarbeitungsvorgänge bestimmt und dokumentiert werden.

Durchführung



7. Modellierung der Risikoquellen

Die Quellen des Risikos für die Rechte und Freiheiten natürlicher Personen müssen identifiziert werden. Insbesondere ist zu bestimmen, welche Personen motiviert sein könnten, die Verarbeitungsvorgänge und die hierin verarbeiteten Daten in unrechtmäßiger Weise zu nutzen, und welches ihre Beweggründe und möglichen Ziele sein können. Anhand dessen können die damit zusammenhängenden Eintrittswahrscheinlichkeiten ermittelt werden.

8. Risikobeurteilung

Aufbauend auf den vorherigen Schritten wird bestimmt, ob in Bezug auf die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen besteht. Potenzielle Schäden können physischer, materieller oder immaterieller Art sein. Ihre Schwere sowie die jeweilige Eintrittswahrscheinlichkeit sind dabei zu berücksichtigen (ErwGr. 75 f.).

9. Auswahl geeigneter Abhilfemaßnahmen

Die ermittelten Risiken müssen durch geeignete Abhilfemaßnahmen (insbesondere durch TOMs) eingedämmt werden. Eine Auswahl sowie Planung der Umsetzung der Maßnahmen findet statt. Dabei wird den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen. Verbleibende Restrisiken werden ermittelt und dokumentiert.

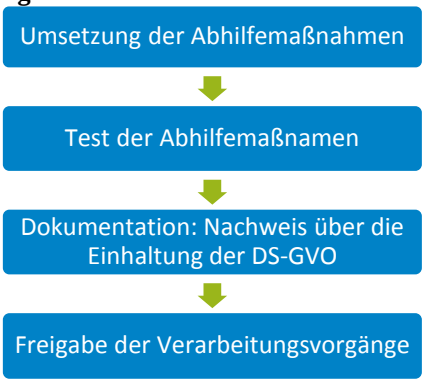
10. Erstellung des DSFA-Berichts

Der DSFA-Bericht enthält gem. Art. 35 Abs. 7 DS-GVO jedenfalls die systematische Beschreibung der geplanten Verarbeitungsvorgänge und ihrer Zwecke, die Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitung, die Beschreibung und Beurteilung der Risiken sowie der Abhilfemaßnahmen zur Risikoeindämmung. Der Bericht ist um eine Darstellung der Restrisiken samt Entscheidung über den Umgang mit diesen zu ergänzen. Er kann sich dabei an den hier dargestellten Phasen orientieren. Der DSFA-Bericht dient ferner als Baustein einer umfassenden Dokumentation zur Umsetzung der in Art. 5 Abs. 2 DS-GVO normierten Rechenschaftspflicht. Es ist zu prüfen, inwieweit Teile des DSFA-Berichts im Sinne einer erhöhten Transparenz für die betroffenen Personen veröffentlicht werden sollen.

Weitere Schritte nach Durchführung der DSFA

Die folgenden Schritte dienen der Implementierung der Abhilfemaßnahmen und sollten nicht lediglich linear durchlaufen werden, sondern eine Rückkoppelung der jeweiligen Ergebnisse im Sinne eines iterativen Vorgehens ermöglichen. Beispielsweise können durch eine Maßnahme weitere Verarbeitungsvorgänge nötig werden, für die wiederum etwaige Risiken zu betrachten sind.

Umsetzung



11. Umsetzung der Abhilfemaßnahmen

Bevor die geplante Datenverarbeitung eingesetzt wird, müssen die für die Eindämmung des Risikos geeigneten Abhilfemaßnahmen

(insbesondere TOMs) umgesetzt sein. Vorher darf die Verarbeitung personenbezogener Daten nicht stattfinden. Sofern sich bei der Umsetzung herausstellt, dass geplante Maßnahmen nicht (wirksam) realisiert werden können, müssen andere geeignete Maßnahmen ausgewählt, die Restrisikobewertung angepasst oder die Verarbeitungsvorgänge insgesamt angepasst werden, so dass sie den Anforderungen der DS-GVO genügen.

12. Test der Abhilfemaßnahmen
Nachdem Abhilfemaßnahmen umgesetzt wurden, müssen sie auf ihre Wirksamkeit getestet werden. Möglicherweise zeigt sich bei der Umsetzung der Maßnahmen, dass weitere Risiken bestehen, die ebenfalls zu behandeln sind.

13. Dokumentation: Nachweis über die Einhaltung der DS-GVO
Gem. Art. 5 Abs. 2 DS-GVO hat der Verantwortliche eine umfassende Dokumentations- und Rechenschaftspflicht, durch die die Einhaltung der DS-GVO insgesamt nachgewiesen werden soll. Der DSFA-Bericht und eine Bestätigung der Wirksamkeit der umgesetzten Maßnahmen dienen als Bausteine zur Erfüllung dieser Pflicht.

14. Freigabe der Verarbeitungsvorgänge
Im Anschluss und mit Vorliegen der vollständigen Dokumentation können die Verarbeitungsvorgänge formal durch den Verantwortlichen freigegeben werden.

Überprüfung



15. Ggf. Überprüfung und Audit der DSFA
Um eine ordnungsgemäße Durchführung sicherzustellen, kann es sinnvoll sein, den DSFA-Bericht von einem unabhängigen Dritten überprüfen zu lassen. Auch könnte der Datenschutzbeauftragte, der gemäß Art. 35 Abs. 2 DS-GVO sowieso einzubeziehen ist, die DSFA abschließend prüfen und das Ergebnis der Leitungsebene des Verantwortlichen mitteilen.

16. Fortschreibung

Die DSFA ist kein strikt linearer oder abgeschlossener Prozess. Vielmehr muss die Einhaltung der DS-GVO während der gesamten Dauer der Verarbeitungsvorgänge fortlaufend überwacht werden. Hierfür bietet sich ein Datenschutz-Managementsystem an. Spätestens wenn sich das mit der Verarbeitung verbundene Risiko ändert, muss erneut eine DSFA durchgeführt werden.

Umgang mit hohen Restrisiken

Ergibt eine DSFA, dass trotz technischer und organisatorischer Maßnahmen zur Risikoeindämmung weiterhin ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen besteht (Restrisiko), muss nach Art. 36 DS-GVO der Verantwortliche die zuständige Aufsichtsbehörde konsultieren. Er trifft unter Berücksichtigung der Empfehlungen der Aufsichtsbehörde eine Entscheidung, ob die Verarbeitungsvorgänge angesichts der verbleibenden Restrisiken durchgeführt werden können und ggf. welche zusätzlichen Abhilfemaßnahmen in diesem Fall zum Einsatz kommen sollen. Die Aufsichtsbehörde kann ihrerseits die in Art. 58 DS-GVO genannten Befugnisse ausüben und z. B. eine Warnung, Anweisung oder Untersagung aussprechen.

Fazit

Die Datenschutz-Folgenabschätzung ist ein sinnvolles Instrument zur systematischen Risikoeindämmung und stellt eine der wichtigsten Neuerungen der DS-GVO gegenüber dem BDSG dar. Rechtzeitig auf den Weg gebracht hilft sie nicht nur, die eigenen Prozesse bei der Verarbeitung personenbezogener Daten besser zu verstehen, sondern auch die Pflichten nach der Grundverordnung umzusetzen.

Anlage 13

Kurzpapier Nr. 6
Auskunftsrecht der betroffenen Person, Art. 15 DS-GVO

Dieses Kurzpapier der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) dient als erste Orientierung insbesondere für den nicht-öffentlichen Bereich, wie nach Auffassung der DSK die Datenschutz-Grundverordnung (DS-GVO) im praktischen Vollzug angewendet werden sollte. Diese Auffassung steht unter dem Vorbehalt einer zukünftigen – möglicherweise abweichenden – Auslegung des Europäischen Datenschutzausschusses.

Auskunftsrecht als zentrales Recht zur Schaffung von Transparenz

Wie schon nach der bisherigen Rechtslage haben betroffene Personen das Recht mit formlosem Antrag und ohne Begründung von einem Verantwortlichen Auskunft über dort gespeicherte personenbezogene Daten zu verlangen. Die Auskünfte können es beispielsweise erleichtern, gezielt weitere Rechte, wie auf Berichtigung, Löschung oder Einschränkung der Verarbeitung („Sperrung“), geltend zu machen.

Umfang des Auskunftsrechts

Nach Art. 15 Abs. 1 DS-GVO steht der betroffenen Person ein abgestuftes Auskunftsrecht zu.

Zum einen kann die betroffene Person von dem Verantwortlichen eine Bestätigung darüber verlangen, ob dort sie betreffende personenbezogene Daten verarbeitet werden. Auch eine Negativauskunft ist erforderlich, wenn der Verantwortliche entweder keine Daten zu dieser Person verarbeitet oder personenbezogene Daten unumkehrbar anonymisiert hat.

Zum anderen kann die betroffene Person ganz konkret Auskunft darüber verlangen, welche personenbezogenen Daten vom Verantwortlichen verarbeitet werden (z. B. Name, Vorname, Anschrift, Geburtsdatum, Beruf, medizinische Befunde).

Weiterhin sind bei der Datenauskunft vom Verantwortlichen nach Art. 15 Abs. 1 DS-GVO vor allem noch folgende Informationen mitzuteilen:

- Verarbeitungszwecke,
- Kategorien personenbezogener Daten, die verarbeitet werden (mit Gruppenbezeichnungen wie Gesundheitsdaten, Bonitätsdaten usw.),
- Empfänger bzw. Kategorien von Empfängern, die diese Daten bereits erhalten haben oder künftig noch erhalten werden,
- geplante Speicherdauer falls möglich, andern-falls die Kriterien für die Festlegung der Speicherdauer,
- Rechte auf Berichtigung, Löschung oder Einschränkung der Verarbeitung,
- Widerspruchsrecht gegen diese Verarbeitung nach Art. 21 DS-GVO,
- Beschwerderecht für die betroffene Person bei der Aufsichtsbehörde,
- Herkunft der Daten, soweit diese nicht bei der betroffenen Person selbst erhoben wurden, und
- das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling mit aussagekräftigen Informationen über die dabei involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen solcher Verfahren.

Im Falle der Datenübermittlung in Drittländer ist über die insoweit gegebenen Garantien gemäß Art. 46 DS-GVO zu informieren (z. B. vereinbarte Standard-Datenschutzklauseln, verbindliche interne Datenschutzvorschriften, d. h. BCR). Keine Drittländer sind die EU-Mitgliedsstaaten

Form der Auskunftserteilung
Die Auskunftserteilung an die betroffene Person kann nach Art. 12 Abs. 1 Sätze 2 und 3 DS-GVO je nach Sachverhalt schriftlich, elektronisch oder – auf Wunsch der betroffenen Person – mündlich erfolgen. Der Verantwortliche stellt eine Kopie der Daten zur Verfügung (Art. 15 Abs. 3 Satz 1 DS-GVO). Stellt die betroffene Person ihren Auskunftsantrag elektronisch, ist die Auskunft nach Art. 15 Abs. 3 Satz 2 DS-GVO in einem gängigen elektronischen Format zur Verfügung zu stellen (z. B. im PDF-Format). Als datenschutzfreundlichste Gestaltung wird in Erwägungsgrund (ErwGr.) 63 Satz 4 ein vom Verantwortlichen eingerichteter Fernzugriff der betroffenen

Person auf ihre eigenen Daten bezeichnet. Alle Kommunikationswege müssen angemessene Sicherheitsanforderungen erfüllen.

Frist für die Auskunftserteilung
Auskunftserteilungen müssen gemäß Art. 12 Abs. 3 DS-GVO unverzüglich erfolgen, spätestens aber innerhalb eines Monats; nur in begründeten Ausnahmefällen kann die Monatsfrist überschritten werden, worüber die betroffene Person zu informieren ist (Art. 12 Abs. 3 Satz 3 DS-GVO). Der Verantwortliche muss (vorbereitend) geeignete organisatorische Maßnahmen treffen, damit die betroffene Person eine beantragte Auskunft zeitnah und in verständlicher Form erhalten kann (Art. 12 Abs. 1 Satz 1 und Art. 5 Abs. 2 DS-GVO).

Kosten der Auskunftserteilung
Die Auskunftserteilung an die betroffene Person (z. B. als Kopie) muss durch den Verantwortlichen regelmäßig unentgeltlich erfolgen, Art. 12 Abs. 5 Satz 1 DS-GVO. Für weitere Kopien kann er ein angemessenes Entgelt fordern. Außerdem kann bei offenkundig unbegründeten oder exzessiven Anträgen ein angemessenes Entgelt für die Auskunft verlangt werden (Art. 12 Abs. 5 Satz 2, ErwGr. 63).

Identitätsprüfung
Es muss sichergestellt werden, dass die zu beauskunftenden Daten nicht unbefugten Dritten zur Verfügung gestellt werden. Hierauf ist auch insbesondere bei mündlicher oder elektronischer Auskunftserteilung zu achten. Hat der Verantwortliche begründete Zweifel an der Identität eines Antragstellers auf Datenauskunft, so kann er nach Art. 12 Abs. 6 DS-GVO zusätzliche Informationen zur Bestätigung der Identität nachfordern (z. B. eine Postadresse bei elektronischem Auskunftsantrag).

Grenzen des Auskunftsrechts
Bei einer großen Menge von gespeicherten Informationen über die betroffene Person kann der Verantwortliche verlangen, dass präzisiert wird, auf welche Informationen oder Verarbeitungsvorgänge sich das Auskunftsersuchen konkret bezieht (ErwGr. 63 Satz 7). Das kann z. B. bei Banken oder Versicherungen mit umfangreichen Vertragsbeziehungen zu der betroffenen Person der Fall sein.
Offenkundig unbegründete oder exzessive Anträge einer betroffenen Person können zur Ablehnung oder zu einer Kostenerstattungspflicht

führen (Art. 12 Abs. 5 S. 2 DS-GVO). Die betroffene Person muss jedoch (und zwar kostenfrei) ihr Recht in angemessenen Abständen wahrnehmen können, um sich der Verarbeitung bewusst zu sein und deren Rechtmäßigkeit überprüfen zu können (ErwGr. 63). Eine Ablehnung oder Kostenerstattung kommt daher nur in Ausnahmefällen in Betracht. Der Verantwortliche trägt die Beweislast für das Vorliegen eines unbegründeten oder exzessiven Antrags (Art. 12 Abs. 5 Satz 3 DS-GVO). Er muss der betroffenen Person in der Regel die Gründe für die Verweigerung der Auskunft mitteilen und sie über Rechtsschutzmöglichkeiten informieren (Art. 12 Abs. 4 DS-GVO).
Das BDSG-neu enthält in § 34 noch weitere Eingrenzungen des Auskunftsrechts, insbesondere für Archivdaten und Protokollierungsdaten.
Ob und wenn ja wie weit die Regelungen des BDSG-neu zur Einschränkung der Betroffenenrechte wegen des bestehenden Anwendungsvorrangs der DS-GVO angewendet werden können, bleibt eine Entscheidung im jeweiligen konkreten Einzelfall vorbehalten.

Beachtung Rechte Dritter
Die Auskunftserteilung an die betroffene Person darf nach Art. 15 Abs. 4 DS-GVO sowie ErwGr. 63 Satz 5 die Rechte des Verantwortlichen oder anderer Personen nicht beeinträchtigen, was bei Geschäftsgeheimnissen oder bei Daten mit Bezug auch auf andere Personen der Fall sein kann. Dies darf im Ergebnis aber nicht dazu führen, dass jegliche Auskunft verweigert wird.

Rechtfolgen bei Verstoß
Unterlassene oder nicht vollständige Auskunftserteilungen an betroffene Personen sind nach Art. 83 Abs. 5 lit. b DS-GVO mit einer hohen Geldbuße bedroht.

Empfehlung
Es ist für Verantwortliche ratsam, rechtzeitig im eigenen Interesse organisatorische Vorkehrungen für zügige und korrekte Auskunftserteilungen zu treffen.

Anlage 14

Kurzpapier Nr. 7
Marktortprinzip: Regelungen für außereuropäische Unternehmen

Dieses Kurzpapier der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) dient als erste Orientierung insbesondere für den nicht-öffentlichen Bereich, wie nach Auffassung der DSK die Datenschutz-Grundverordnung (DS-GVO) im praktischen Vollzug angewendet werden sollte. Diese Auffassung steht unter dem Vorbehalt einer zukünftigen – möglicherweise abweichenden – Auslegung des Europäischen Datenschutzausschusses.

Regelung des Marktortprinzips in Art. 3 Abs. 2 DS-GVO
Das Marktortprinzip schließt unter bestimmten Bedingungen auch Unternehmen, die nicht in der EU niedergelassen sind, in den Anwendungsbereich der DS-GVO ein.

Seit In-Kraft-Treten der EU-Datenschutzrichtlinie im Jahr 1995 haben sich neue Fragestellungen zum Anwendungsbereich des europäischen Datenschutzrechts entwickelt, beispielsweise mit Blick auf die fortschreitende Verlagerung von Geschäftsaktivitäten ins Internet (eCommerce). Sie erfordern keine physischen Betriebs- und Organisationsstrukturen in Europa, die als direkter Anknüpfungspunkt für die Anwendbarkeit europäischen Datenschutzrechts dienen könnten.

Der europäische Gesetzgeber erstreckt den Anwendungsbereich des europäischen Datenschutzrechts mit Einführung des Marktortprinzips auf datenschutzrechtlich relevante Geschäftsaktivitäten von Unternehmen, die keine Niederlassungen in der EU besitzen und damit an sich außerhalb des territorialen Anwendungsbereichs nach Art. 3 Abs. 1 DS-GVO liegen würden. Unter den von Art. 3 Abs. 2 lit. a und lit. b DS-GVO festgelegten Bedingungen erstreckt sich der Anwendungsbereich der DSGVO auf Verarbeitungen personenbezogener Daten von Betroffenen, die sich in der EU befinden, ohne Rücksicht auf physische Organisations- oder Betriebsstrukturen von Unternehmen in der EU.

1. Anknüpfungspunkt: Angebot von Waren und Dienstleistungen (Art. 3 Abs. 2 lit. a DS-GVO)
Die DS-GVO findet Anwendung, wenn eine Daten-verarbeitung im Zusammenhang damit steht, betroffenen Personen in der EU Waren oder Dienst-leistungen anzubieten. Das Unternehmen muss dies offensichtlich beabsichtigen (vgl. ErwGr. 23). Die Zahlung eines Entgeltes für das Waren- oder Dienstleistungsangebot ist hierbei für die Anwendbarkeit der DS-GVO irrelevant, sondern es sollen explizit auch unentgeltliche Angebote, z. B. Dienstleistungen durch soziale Netzwerke, darunter fallen.

Ein maßgeblicher Anknüpfungspunkt ist die Ausrichtung bestimmter Werbe- bzw. Verkaufsmaßnahmen auf Personen, die sich in der EU befinden. Wann dies der Fall ist, muss anhand von Hilfsfaktoren und Indizien bestimmt werden. Keine ausreichenden Anhaltspunkte hierfür sind etwa allein

- die bloße Abrufbarkeit einer kommerziellen Internetpräsenz, einer E-Mail-Adresse oder sonstiger Kontaktdaten oder
- die Verwendung einer (EU-)Sprache, die in dem Drittstaat, in dem das jeweilige Unter-nehmen niedergelassen ist, allgemein gebräuchlich ist.

Haftungsausschlüsse (so genannte Disclaimer), die beispielsweise die Anwendbarkeit der DS-GVO beschränken oder ausschließen, lassen wiederum nicht zwingend auf die Nichtanwendbarkeit der DS-GVO schließen.
Andere Faktoren wie

- die Verwendung der Sprache oder Währung eines Mitgliedstaates in Verbindung mit der Möglichkeit, Waren und Dienstleistungen in dieser anderen Sprache zu bestellen oder
- die Erwähnung von Kunden oder Nutzern, die sich in der EU befinden,

können darauf hindeuten, dass ein Unternehmen beabsichtigt, den betroffenen Personen in der EU Waren oder Dienstleistungen anzubieten (vgl. ErwGr. 23). Ein Angebot kann auch dann (potenziellee) Kunden und Nutzer in der EU adressieren, wenn das jeweilige Waren- oder Dienstleistungsangebot einen hinreichend konkreten perso-

nalen Bezug zum Marktgeschehen aufweist. Zur Bestimmung dessen können beispielsweise „Flaggen-Icons“, landesspezifische „Top Level Domains“ oder geographische Referenzen zu den mitgliedstaatlichen Märkten herangezogen werden.

2. Anknüpfungspunkt: Überwachung des Verhaltens von Personen (Art. 3 Abs. 2 lit. b DS-GVO)

Die DS-GVO ist auch dann anwendbar, wenn die Datenverarbeitung im Zusammenhang damit steht, das Verhalten von betroffenen Personen zu beobachten, soweit dieses Verhalten in der EU erfolgt. Dies ist zum Beispiel dann der Fall, wenn die Internetaktivitäten der betroffenen Person nachvollzogen werden. Eine solche Nachvollziehbarkeit kann auch im Fall der nachfolgenden Erstellung von (Persönlichkeits-)Profilen angenommen werden, wenn

- diese die Grundlage für eine die jeweilige Person betreffende Entscheidung bilden oder
- anhand derer die Vorlieben, Verhaltensweisen oder Gepflogenheiten einer natürlichen Person analysiert oder vorausgesagt wer-den sollen (vgl. ErwGr. 24).

Dies kann zum Beispiel durch den Einsatz von „Tracking-Cookies“ oder „Browser Fingerprints“ statt-finden. Diese Techniken können auch als Grundlage für die weitere Erstellung persönlicher Profile, etwa zum Zwecke individualisierter bzw. zielgruppenspezifischer Werbung (sog. Behavioural Targeting) dienen.

Weitere Folgen

Außereuropäische Unternehmen, auf deren Verarbeitungstätigkeiten die DS-GVO anwendbar ist, müssen grundsätzlich einen in einem betroffenen Mitgliedstaat niedergelassenen Vertreter benennen. Der Vertreter ist ausdrücklich zu bestellen und schriftlich zu beauftragen, in Bezug auf die sich aus der DS-GVO ergebenden Pflichten an Stelle des Verantwortlichen oder des Auftragsverarbeiters zu handeln. Als Anlaufstelle soll dieser Vertreter einerseits den betroffenen Personen ermöglichen, ihre Betroffenenrechte wirksam geltend zu machen und andererseits die Aufsichtsbehörden in die Lage versetzen, ihre Aufsichtsmaßnahmen effektiv durchzusetzen (Art. 27 DS-GVO, siehe auch ErwGr. 80). Die Pflicht entfällt, wenn die Verarbeitung

- lediglich gelegentlich erfolgt,
- nicht die umfangreiche Verarbeitung sensibler personenbezogener Daten im Sinn von Art. 9 DS-GVO einschließt,
- nicht die umfangreiche Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten (Art. 10 DS-GVO) einschließt und
- nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.

Der Verstoß gegen die Pflicht zur Bestellung ist bußgeldbewehrt (vgl. Art. 83 Abs. 4 lit. a DS-GVO).

Fazit
Auch Unternehmen, die keine Niederlassung in der EU haben, aber auf dem europäischen Markt tätig sind, müssen die DS-GVO voll anwenden. Darüber hinaus sind diese Unternehmen grundsätzlich verpflichtet, einen Vertreter in der EU zu benennen. Der europäische Gesetzgeber stellt die Aufsichtsbehörden mit Einführung des Marktortprinzips vor die nicht zu unterschätzende Herausforderung, den Geltungsanspruch der DS-GVO gegenüber Unternehmen in Drittstaaten durchzusetzen.

Anlage 15

Kurzpapier Nr. 8
Maßnahmenplan „DS-GVO“ für Unternehmen

Dieses Kurzpapier der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) dient als erste Orientierung insbesondere für den nicht-öffentlichen Bereich, wie nach Auffassung der DSK die Datenschutz-Grundverordnung (DS-GVO) im praktischen Vollzug angewendet werden sollte. Diese Auffassung steht unter dem Vorbehalt einer zukünftigen – möglicherweise abweichenden – Auslegung des Europäischen Datenschutzausschusses.

Bedeutung
Die DS-GVO, die im Mai 2016 in Kraft getreten ist, wird weitreichende Auswirkungen auf nahezu alle Unternehmen in Europa haben. Anders als die bisherige EU-Richtlinie wird diese EU-Verordnung ab dem 25. Mai 2018 unmittelbar in den Mitgliedsstaaten der EU anwendbar sein und wird das bis dahin geltende Bundesdatenschutzgesetz (BDSG) ablösen. Gleichzeitig sieht das deutsche Datenschutz-Anpassungs- und Umsetzungsgesetz-EU (DSAnpUG-EU) eine ergänzende Neufassung des nationalen Rechts vor (z. B. BDSG-neu), soweit in der DS-GVO Spielraum für nationale Regelungen besteht. Viele Unternehmen sind aber noch nicht auf die DS-GVO und deren Auswirkungen auf die Unternehmensprozesse vorbereitet. Daher haben die unabhängigen Datenschutzbehörden einige Tipps zur Erstellung eines Maßnahmenplans für Unternehmen zusammengestellt.

Information der Geschäftsleitung
Alle Entscheidungsträger in einem Unternehmen sollten sich der Auswirkungen der DS-GVO bewusst sein und wissen, was dies für den alltäglichen Betrieb in ihrem Unternehmen bedeutet. In einem ersten Schritt ist daher von den betrieblichen Datenschutzbeauftragten und/oder den IT-Verantwortlichen die Geschäftsleitung zu informieren.

Start eines Projekts zur Umsetzung der DS-GVO

Alle Verfahren, mit denen personenbezogene Daten verarbeitet werden, sind dahingehend zu überprüfen, ob es einen Anpassungsbedarf im Hinblick auf die DS-GVO gibt. Dies betrifft insbesondere die rechtlichen, technischen und organisatorischen Bereiche in einem Unternehmen. Da folglich verschiedene Personen bzw. Abteilungen im Unternehmen beteiligt sind, die untereinander koordiniert werden müssen, bietet es sich an, ein Projekt mit dem Ziel zu initiieren, die Datenschutzkonzeption anhand eines Soll-Ist-Abgleichs zu aktualisieren.
Die Kernaufgabe wird dabei sein, herauszufinden, welche Prozesse im Unternehmen anzupassen sind.

1. Bestandsaufnahme
Um ein genaues Verständnis davon zu bekommen, wie in einem Unternehmen mit personenbezogenen Daten umgegangen wird, sollten die aktuell realisierten Rahmenbedingungen aller Datenverarbeitungen analysiert werden (Ist-Zustand). Dies betrifft u. a.

- die derzeitigen Prozesse im Unternehmen, in denen personenbezogene Daten verarbeitet werden (bestehende Dokumentationen, bspw. ein Verfahrensverzeichnis, können hierfür einen Ausgangspunkt bilden),
- die dazugehörigen Rechtsgrundlagen (die Verarbeitung personenbezogener Daten ist nur dann zulässig, wenn entweder ein Gesetz oder eine Rechtsvorschrift dies erlaubt oder der Betroffene eingewilligt hat),
- die Datenschutzorganisation (d. h. alle Vorkehrungen und Maßnahmen, die im Unternehmen zum Schutz personenbezogener Daten getroffen werden),
- die Dienstleistungsbeziehungen (wie etwa Verträge über eine Auftragsdatenverarbeitung),
- die Dokumentation (z. B. Verfahrensverzeichnisse, Vorabkontrollen, Datenschutzkonzepte, IT-Sicherheitskonzepte, Sicherheitsvorfälle) und
- sofern vorhanden Betriebsvereinbarungen, denn diese können auch Regelungen zum Umgang mit den Daten der Beschäftigten enthalten.

2. Handlungsbedarf eruieren

Nunmehr ist der Soll-Zustand zu ermitteln und im Anschluss daran eine Lückenanalyse zwischen dem jetzigen Ist-Zustand und dem künftigen Soll-Zustand durchzuführen. Dabei sind u. a. folgende Punkte vor dem Hintergrund der DS-GVO zu beachten (zu den einzelnen Themen erscheinen weitere Kurzpapiere):

- **Rechtsgrundlagen:**
  Auch unter der DS-GVO ist für die Verarbeitung personenbezogener Daten eine Legitimationsgrundlage erforderlich. Folglich ist zu prüfen, ob das neue Recht für alle Prozesse eine Rechtsgrundlage bereitstellt. Sofern sich die Datenverarbeitung auf eine Einwilligung stützt, ist zu prüfen, ob die Anforderungen des Art. 7 DS-GVO erfüllt sind (bei Einwilligung eines Kindes in Bezug auf Dienste der Informationsgesellschaft ist zudem Art. 8 DS-GVO zu beachten).
- **Betroffenenrechte:**
  Den betroffenen Personen stehen umfangreiche Rechte zu, die der Verantwortliche zu beachten hat (z. B. Informationspflichten des Verantwortlichen gegenüber den betroffenen Personen nach Art. 13 und Art. 14 DS-GVO, Auskunftsrecht nach Art. 15 DS-GVO, Recht auf Berichtigung nach Art. 16 DS-GVO, Recht auf Löschung nach Art. 17 DS-GVO, das neue Recht auf Datenübertragbarkeit nach Art. 20 DS-GVO, Widerspruchsrecht nach Art. 21 DS-GVO).
- **Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen:**
  Die DS-GVO enthält spezifische Rahmen-bedingungen für die Art und Weise, wie die Anforderungen der DS-GVO schon bei der Prozessgestaltung und bei den Voreinstellungen umzusetzen sind (Art. 25 DS-GVO: Data Protection by design und Data Protection by default).
- **Dienstleistungsbeziehungen:**
  Dabei sollten insbesondere die bestehenden Verträge zur Auftragsverarbeitung überprüft werden. Die Art. 28 und 29 DS-GVO enthalten Vorgaben für Vereinbarungen mit Auftragsverarbeitern.
- **Dokumentationspflichten:**
  Die DS-GVO verpflichtet in Art. 5 Abs. 2 DS-GVO den Verantwortlichen zum Nachweis, dass personenbezogene Daten rechtmäßig verarbeitet werden (Rechenschaftspflicht). Zusätz-

lich sieht die DS-GVO an unterschiedlichen Stellen Dokumentationspflichten vor (z. B. für das Verarbeitungsverzeichnis in Art. 30 DS-GVO, für die Dokumentation von Datenschutzvorfällen in Art. 33 Abs. 5 DS-GVO oder für die Dokumentation von Weisungen im Rahmen der Auftragsverarbeitung in Art. 28 Abs. 3 lit. a DS-GVO).

- **Datenschutz-Folgenabschätzung:**
  Die aus dem BDSG bekannte Vorabkontrolle wird durch die Datenschutz-Folgen-abschätzung nach Art. 35 DS-GVO abgelöst und erfordert eine umfangreiche Dokumentation. Die Datenschutz-Folgenabschätzung kann zudem eine Konsultation der Aufsichtsbehörde nach sich ziehen (Art. 36 DS-GVO).
- **Meldepflichten:**
  Nach Art. 37 Abs. 7 DS-GVO muss der Verantwortliche oder der Auftragsverarbeiter die Kontaktdaten des Datenschutzbeauftragten der zuständigen Aufsichtsbehörde melden. Ebenso ist der Aufsichtsbehörde die Verletzung des Schutzes personenbezogener Daten zu melden (Art. 33 Abs. 1 DS-GVO).
- **Datensicherheit:**
  Unternehmen müssen ein angemessenes Schutzniveau in Bezug auf die Sicherheit der Verarbeitung gewährleisten und die dafür implementierten Sicherungsmaßnahmen einer regelmäßigen Überprüfung unterziehen (Art. 24 und 32 DS-GVO).
- **Zertifizierung:**
  Schlussendlich besteht im Rahmen eines Zertifizierungsverfahrens die Möglichkeit, den Nachweis zu erbringen, dass die Datenverarbeitung im Einklang mit der DS-GVO erfolgt.

3. Umsetzung bis zum 25. Mai 2018

Bei der Umsetzung sind dann u. a. folgende Punkte wieder zu beachten:

- Anpassung der betroffenen Prozesse und Strukturen,
- Festlegung der Rechtsgrundlagen und des Zwecks der Datenverarbeitung sowie Dokumentation von Interessenabwägungen (sofern erfolgt),
- Implementierung von Informationspflichten, Betroffenenrechten und Löschkonzepten,
- Anpassung der Datenschutzorganisation,
- ggf. Bestellung eines Datenschutzbeauftragten,

- Reaktionsmechanismen auf Datenpannen,
- Organisation von Meldepflichten,
- Anpassung der Dienstleistungsbeziehungen,
- Aufbau der Dokumentation,
- Anpassung der IT-Sicherheit und
- ggf. Anpassung der Betriebsvereinbarungen.

Anlage 16

Kurzpapier Nr. 9
Zertifizierung nach Art. 42 DS-GVO

Dieses Kurzpapier der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) dient als erste Orientierung insbesondere für den nicht-öffentlichen Bereich, wie nach Auffassung der DSK die Datenschutz-Grundverordnung (DS-GVO) im praktischen Vollzug angewendet werden sollte. Diese Auffassung steht unter dem Vorbehalt einer zukünftigen - möglicherweise abweichenden - Auslegung des Europäischen Datenschutzausschusses.

Sinn und Zweck von Zertifizierungen
Im Datenschutzalltag trifft man häufig auf eine grundlegende Fragestellung: *„Woher weiß man, ob datenschutzrechtliche Vorgaben von einem Unternehmen oder einer Behörde eingehalten werden?“*. Eine auf den ersten Blick einfache und pragmatische Lösung wäre, sich dies durch entsprechende Zertifizierungen nachweisen zu lassen. Mit den Artikeln 42 und 43 der DS-GVO legt der Gesetzgeber einen rechtlichen Grundstein für europäisch einheitliche Akkreditierungs- und Zertifizierungsverfahren, die dazu dienen, die Einhaltung der DS-GVO bei Verarbeitungsvorgängen nachzuweisen.

Bisherige Erfahrungen der Aufsichtsbehörden
Die Aufsichtsbehörden haben in ihren Kontrollen zwar festgestellt, dass Organisationen oft verschiedenste Zertifikate vorweisen konnten – jedoch war häufig unklar, inwieweit die gesetzlichen Anforderungen an den Datenschutz ausreichend berücksichtigt wurden. Manche bestehende Zertifizierungsverfahren, wie beispielsweise das Informationssicherheitsmanagement nach ISO 27001, decken nur einen Teilbereich des Datenschutzes ab und haben mitunter auch die betroffenen Personen mit ihren Rechten und Freiheiten nicht im Mittelpunkt der Betrachtung.

Förderung von Zertifizierungen
Einleitend weist Art. 42 Abs. 1 DS-GVO darauf hin, dass unter anderem auch die Aufsichtsbehörden auf Unionsebene die Einführung von datenschutzspezifischen Zertifizierungsverfahren, Datenschutz-

siegeln und -prüfzeichen fördern sollen. Diese dienen dazu, nachzuweisen, dass die DS-GVO bei Verarbeitungsvorgängen von Verantwortlichen oder Auftragsverarbeitern eingehalten wird. Bis es jedoch so weit ist, dass die Verordnung umgesetzt und angewandt werden kann, müssen die Mitgliedstaaten in einer engen Zusammenarbeit die in der DS-GVO geforderten Mechanismen und Kriterien entwickeln. Dies ist zeitlich, räumlich und kapazitiv eine große Herausforderung für alle Beteiligten.

Vorteile einer Zertifizierung

Die DS-GVO nennt explizit einige Anwendungsbereiche, bei denen eine Zertifizierung für den Nachweis der Einhaltung der Grundverordnung als Faktor mit herangezogen werden kann:

- Erfüllung der Pflichten des Verantwortlichen (Art. 24 Abs. 3)
- Erfüllung der Anforderungen an Technikgestaltung und datenschutz-freundliche Voreinstellungen des Art. 25 Abs. 1 und 2 (vgl. Abs. 3)
- Garantien des Auftragsverarbeiters nach Art. 28 (vgl. Abs. 5 und 6)
- Sicherheit der Verarbeitung (Art. 32 Abs. 3)
- Datenübermittlung an ein Drittland (Art. 46 Abs. 2 lit. f)
- Datenschutz-Folgeabschätzung (ErwGr. 90)

Daneben kann ein Zertifikat auch für Marketingzwecke genutzt werden, um sowohl Geschäftskunden, Verbrauchern als auch Bürgern gegenüber die Beachtung des Datenschutzrechts darzustellen.

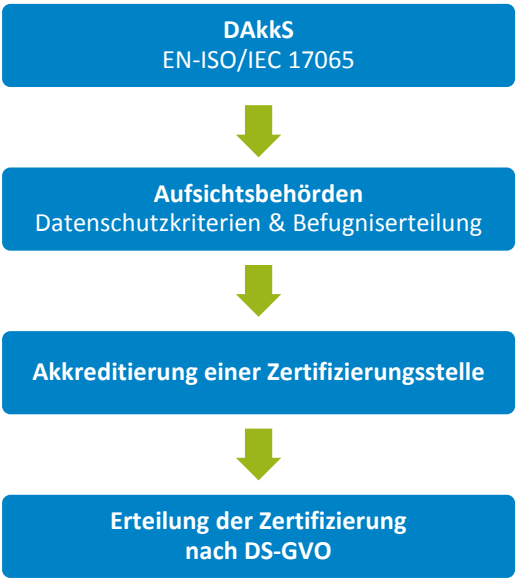
Einhaltung der DS-GVO – auch mit Zertifikat

Art. 42 Abs. 4 hebt hervor, dass eine erfolgreiche Zertifizierung eine Organisation (unabhängig davon, ob Verantwortlicher oder Auftragsverarbeiter) nicht von der Verantwortung für die Einhaltung der DS-GVO befreit. Ebenso verdeutlicht Art. 42 Abs. 4, dass die Aufgaben und Befugnisse der zuständigen Aufsichtsbehörden von einer Zertifizierung unberührt bleiben. Ein nach DS-GVO genehmigtes Zertifizierungsverfahren kann jedoch bei aufsichtlichen Kontrollen von Vorteil sein und die Prüfung erleichtern.

Zertifizierungsstellen

Nach Art. 42 Abs. 5 DS-GVO können sowohl akkreditierte Zertifizierungsstellen als auch die zuständigen Aufsichtsbehörden eine Datenschutz-Zertifizierung nach DS-GVO erteilen. Die Akkreditierung nimmt in Deutschland die Deutsche Akkreditierungsstelle GmbH (DAkkS) zusammen mit den Aufsichtsbehörden gemäß § 39 Akkreditierung DSAnpUG („BDSG-neu“) vor. Die Kriterien für die Akkreditierung werden von den Aufsichtsbehörden entwickelt und beruhen u. a. auf einschlägigen ISO-Normen (siehe Abbildung). Eine einvernehmliche Entscheidung der beiden Parteien in einem eigens dafür eingerichteten Ausschuss ist Voraussetzung für die Akkreditierung einer Zertifizierungsstelle. Erst danach und nach der Erteilung der Befugnis durch die zuständige Aufsichtsbehörde, kann die Zertifizierungsstelle tätig werden. Sie darf im Anschluss, nach entsprechender Prüfung der Einhaltung der DS-GVO, Zertifizierungen erteilen.

Gesamtverfahren im Überblick



Voraussetzung für eine Zertifizierung

Damit eine Zertifizierung durchgeführt werden kann, muss die zu zertifizierenden Stelle alle für die Durchführung des Zertifizierungsverfahrens erforderlichen Informationen zur Verfügung stellen und

Zugang zu den betroffenen Verarbeitungstätigkeiten gewähren (Art. 42 Abs. 6 DS-GVO). Somit wird es künftig umso wichtiger, die eigenen Verarbeitungsvorgänge zu kennen und transparent zu dokumentieren. Unternehmen, die bereits jetzt Informationssicherheit leben, über ein Datenschutz-Managementsystem verfügen und sich mit der Umsetzung der DS-GVO befassen, erfüllen bereits wesentliche Voraussetzungen.

Rahmenbedingungen
Art. 42 Abs. 7 DS-GVO weist darauf hin, dass eine Zertifizierung zeitlich begrenzt zu erteilen ist. So besteht eine Höchstdauer von drei Jahren, die bei Erfüllung der einschlägigen Voraussetzungen verlängert werden kann. Die zuständige Zertifizierungsstelle und die Aufsichtsbehörde können die Zertifizierung widerrufen, wenn die Voraussetzungen für die Zertifizierung

Ausblick zu Datenschutz-Zertifizierungen
Zertifizierungen nach der DS-GVO bieten das Potenzial, künftig bei Verarbeitungsvorgängen (u. a. bei Auftragsverarbeitung) Klarheit darüber zu verschaffen, ob die gesetzlichen Datenschutzanforderungen eingehalten werden. So können etwa Cloud-Dienste entscheidend profitieren, da deren Kunden und vor allem auch betroffene Personen sich selbst leichter ein Bild von einem bestimmten Produkt hinsichtlich der Einhaltung der DS-GVO machen können. Voraussetzung hierfür sind jedoch auf die DS-GVO ausgerichtete, praxistaugliche Zertifizierungsverfahren. Bei bestehenden Zertifizierungsverfahren muss zwangsläufig eine Überarbeitung hinsichtlich der neuen Vorgaben stattfinden.

Die Aufsichtsbehörden des Bundes und der Länder arbeiten derzeit intensiv an der Entwicklung abgestimmter, länderübergreifend geltender Kriterien, damit auch im Vollzug der Aufsichtsbehörden eine einheitliche Bewertung im Sinne der DS-GVO ermöglicht wird. Ein Wildwuchs zahlreicher unter-schiedlicher Zertifizierungsverfahren sollte gerade mit Blick auf ein einheitliches europäisches Datenschutzniveau im Interesse aller Beteiligten vermieden werden.

Anlage 17

Kurzpapier Nr. 10
Informationspflichten bei Dritt- und Direkterhebung

Dieses Kurzpapier der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) dient als erste Orientierung insbesondere für den nicht-öffentlichen Bereich, wie nach Auffassung der DSK die Datenschutz-Grundverordnung (DS-GVO) im praktischen Vollzug angewendet werden sollte. Diese Auffassung steht unter dem Vorbehalt einer zukünftigen – möglicherweise abweichenden – Auslegung des Europäischen Datenschutzausschusses.

Bedeutung der Informationspflichten
Die Informationspflichten bilden die Basis für die Ausübung der Betroffenenrechte (insbesondere der Art. 15 ff. DS-GVO). Nur wenn die betroffene Person weiß, dass personenbezogene Daten über sie verarbeitet werden, kann sie diese Rechte auch ausüben. Die Informationspflichten gemäß der DS-GVO gehen daher weit über die bisherige Rechtslage hinaus und müssen beachtet werden, sofern keine Ausnahmevorschriften greifen.

Die DS-GVO regelt die Informationsverpflichtungen des Verantwortlichen gegenüber der betroffenen Person in Abhängigkeit davon, ob personenbezogene Daten bei der betroffenen Person (**Direkterhebung**, Art. 13 DS-GVO) oder bei Dritten (**Dritterhebung**, Art. 14 DS-GVO) erhoben werden. Zu beachten ist, dass aus dieser Unterscheidung nicht pauschal abzuleiten ist, wer für die Information verantwortlich ist. Auch der Verantwortliche, der die Daten direkt bei der betroffenen Person erhoben hat, kann über Art. 13 DS-GVO hinaus zur Mitteilung nach Art. 14 Abs. 3 lit. c DS-GVO verpflichtet sein, wenn er die Daten gegenüber einem anderen Empfänger offenbaren möchte.

Informationspflichten bei Direkterhebung
Bei der Informationspflicht im Falle der **Direkterhebung** wird zwischen den Informationen unterschieden, die der betroffenen Person mitzuteilen sind (Art. 13 Abs. 1 DGS-GVO) und solchen, die zur Verfügung zu stellen sind, um eine faire und transparente Verarbei-

tung der personenbezogenen Daten zu gewährleisten (Art. 13 Abs. 2 DS-GVO).

- Name (ggf. Firmenname gem. § 17 Abs. 1 HGB oder Vereinsname gem. § 57 BGB) und Kontaktdaten des Verantwortlichen sowie ggf. dessen Vertreter
- Kontaktdaten des ggf. vorhandenen Datenschutzbeauftragten
- Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen und zusätzlich die Rechtsgrundlage, auf der die Verarbeitung fußt
- das berechtigte Interesse, insofern die Datenerhebung auf einem berechtigten Interesse des Verantwortlichen oder eines Dritten beruht (Art. 6 Abs. 1 lit. f DS-GVO)
- Empfänger oder Kategorien von Empfängern der personenbezogenen Daten (vgl. Art. 4 Nr. 9 DS-GVO)
- Absicht des Verantwortlichen, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln und zugleich Information, ob ein Angemessenheitsbeschluss der Kommission vorhanden ist oder nicht (bei Fehlen eines solchen Beschlusses ist auf geeignete oder angemessene Garantien zu verweisen und die Möglichkeit, wie eine Kopie von ihnen zu erhalten ist, oder wo sie verfügbar sind)

Zusätzlich sind nach Abs. 2 Informationen über

- die geplante Speicherdauer oder, falls dies nicht möglich ist, die Kriterien für die Festlegung der Speicherdauer,
- die Betroffenenrechte (Auskunfts-, Löschungs-, Einschränkungs- und Wider Widerspruchsrechte sowie das Recht auf Datenübertragbarkeit),
- das Recht zum jederzeitigen Widerruf einer Einwilligung und die Tatsache, dass die Rechtmäßigkeit der Verarbeitung auf Grundlage der Einwilligung bis zum Widerruf unberührt bleibt,
- das Beschwerderecht bei einer Aufsichtsbehörde,
- ggf. die gesetzliche oder vertragliche Verpflichtung des Verantwortlichen, personenbezogene Daten Dritten bereitzustellen und die möglichen Folgen der Nichtbereitstellung der personenbezogenen Daten und
- im Falle einer automatisierten Entscheidungsfindung (einschließlich Profiling) aussagekräftige Informationen über die

verwendete Logik, die Tragweite und angestrebten Auswirkungen einer derartigen Verarbeitung

zur Verfügung zu stellen.

Informationspflichten bei Dritterhebung

Auch im Falle einer **Dritterhebung** unterscheidet die DS-GVO zwischen mitzuteilenden Informationen (Art. 14 Abs. 1 DS-GVO) und zusätzlichen Informationen, die zur Gewährung einer fairen und transparenten Verarbeitung zur Verfügung zu stellen sind (Art. 14 Abs. 2 DS-GVO).

Art und Inhalt der mitzuteilenden bzw. der zur Verfügung zu stellenden Informationen entsprechen in wesentlichen Teilen denjenigen, die auch im Falle einer Direkterhebung mitgeteilt werden müssen.

Allerdings hat die betroffene Person im Gegensatz zur Direkterhebung nicht an der Datenerhebung mitgewirkt und somit auch keine Kenntnis darüber, welche personenbezogene Daten erhoben wurden. Daher ist der Verantwortliche nach Art. 14 Abs. 1 lit. d DS-GVO verpflichtet, die Kategorien der verarbeiteten personenbezogenen Daten mitzuteilen. Diese Information muss so konkret sein, dass für den Betroffenen erkennbar wird, zu welchen Folgen die Verarbeitung führen kann. Nur dann kann er eine bewusste Entscheidung darüber treffen, ob er ergänzend von seinem Auskunftsrecht nach Art. 15 DS-GVO Gebrauch machen sollte.

Bei der Dritterhebung ist zudem nach Art. 14 Abs. 2 lit. f DS-GVO die Datenquelle anzugeben und, ob es sich dabei um eine öffentlich zugängliche Quelle handelt. Stammen die Daten aus mehreren Quellen und kann die Herkunft nicht mehr eindeutig festgestellt werden, muss dennoch eine allgemeine Information gegeben werden.

Bei der Dritterhebung ist weiterhin zu beachten, dass Angaben über die berechtigten Interessen des Verantwortlichen oder eines Dritten (Art. 6 Abs. 1 lit. f DS-GVO) nicht – wie bei der Direkterhebung – unter Abs. 1 fallen, sondern im Rahmen der zusätzlichen Informationen nach Abs. 2 zur Verfügung gestellt werden müssen (Art. 14 Abs. 2 lit. b DS-GVO).

Zweckänderung und Übermittlung

Die Informationspflichten im Falle einer Zweckänderung gelten sowohl für die Direkterhebung als auch für die Dritterhebung. Neben der Information über die geänderte Zweckbestimmung sind alle Informationspflichten gemäß Art. 13 Abs. 2 DS-GVO (Direkterhe-

bung) oder gemäß Art. 14 Abs. 2 DS-GVO (Dritterhebung) erneut zu erfüllen.
Die Übermittlung an einen Dritten ist häufig eine Zweckänderung, so dass schon aus diesem Grund vor der Übermittlung die betroffene Person entsprechend zu informieren ist. Darüber hinaus stellt Art. 14 Abs. 3 lit. c DS-GVO klar, dass bei der Offenlegung an einen neuen Empfänger (einschließlich Auftragsverarbeitern, vgl. Art. 4 Nr. 9 DS-GVO) informiert werden muss, soweit dieser nicht von der bereits nach Artikel 13 Abs. 1 lit. e DS-GVO erteilten Information über Empfänger oder Empfängerkategorien umfasst ist.

Zeitpunkt der Erfüllung der Informationspflichten
Bei der **Direkterhebung** müssen die Informationen zum Zeitpunkt der Erhebung der Daten mitgeteilt bzw. zur Verfügung gestellt werden.
Im Falle der **Dritterhebung** ist der Verantwortliche verpflichtet, die Informationen nachträglich innerhalb einer angemessenen Frist nach Erlangung der Daten mitzuteilen (Art. 14 Abs. 3 DS-GVO). Diese Frist bestimmt sich nach den spezifischen Umständen, darf aber einen Monat nicht überschreiten. Die Monatsfrist ist eine Maximaldauer und sollte nicht pauschal angesetzt werden. Werden die personenbezogenen Daten zur Kommunikation mit der betroffenen Person verwendet, sind die Informationen spätestens zum Zeitpunkt der ersten Kontaktaufnahme mitzuteilen. Falls die Offenlegung an einen anderen Empfänger beabsichtigt ist, müssen die Informationen spätestens zum Zeitpunkt der ersten Offenlegung erteilt werden.

Ausnahmen
Die Informationspflichten nach den Art. 13 und 14 DS-GVO bestehen nicht, wenn und soweit die betroffene Person bereits über die Informationen verfügt. Im Falle der Dritterhebung bestehen darüber hinaus keine Informationspflichten, wenn die Informationserteilung sich z. B. als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordern würde, die Daten einem Berufsgeheimnis unterliegen oder die Erlangung durch Rechtsvorschrift ausdrücklich geregelt ist.
Außerdem sind in den §§ 32 und 33 des neuen Bundesdatenschutzgesetzes (BDSG-neu) weitere Ausnahmen von den Informationspflichten normiert. Die Informationspflicht nach Art. 13 DS-GVO soll beispielsweise gem. § 32 Abs. 1 Nr. 4 BDSG-neu nicht beste-

hen, wenn die Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche beeinträchtigt würde und die Interessen des Verantwortlichen an der Nichterteilung der Information die Interessen der betroffenen Person überwiegen.
Es bestehen jedoch Zweifel, ob die in den §§ 32 und 33 BDSG-neu vorgesehenen Beschränkungen der Informationspflichten nach Art. 23 DS-GVO zulässig sind. Jedenfalls sind diese Regelungen grundsätzlich eng und im Sinne einer größtmöglichen Transparenz auszulegen. Ob und in welchem Umfang eine in den §§ 32 und 33 BDSG-neu vorgesehene Beschränkung der Informationspflichten aufgrund des Anwendungsvorrangs der DS-GVO tatsächlich angewendet werden kann, bleibt einer Entscheidung im jeweiligen konkreten Einzelfall vorbehalten.

Form der Informationspflicht
Gemäß Art. 12 Abs. 1 DS-GVO sind die Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form sowie in klarer und einfacher Sprache zu übermitteln. Die Informationen sind schriftlich oder in anderer Form (ggf. elektronisch) zur Verfügung zu stellen. Wird aber auf eine elektronisch verfügbare Information Bezug genommen, dann muss diese leicht auffindbar sein. Hierbei können auch Bildsymbole hilfreich sein.
Die leicht zugängliche Form bedeutet auch, dass die Informationen in der konkreten Situation verfügbar sein müssen. Sollen die Daten also von einer anwesenden Person erhoben werden, darf die Person in der Regel nicht auf Informationen im Internet verwiesen werden. Dies gilt gleichermaßen für eine schriftliche Korrespondenz auf dem Papierweg.

Nachweise der Informationspflichten
Der Verantwortliche hat im Hinblick auf das Transparenzgebot stets den Nachweis einer ordnungsgemäßen Erledigung der Informationspflichten zu erbringen (Art. 5 Abs. 1 lit. a und Abs. 2 DS-GVO).

Folgen eines Verstoßes
Der Verstoß gegen die Informationspflichten kann nach Art. 83 Abs. 5 lit b DS-GVO mit einer Geldbuße bestraft werden.

Empfehlung
Es ist für Verantwortliche im eigenen Interesse ratsam, rechtzeitig die nach Art. 25 DS-GVO erforderlichen technischen und organisatorischen Maßnahmen für eine zügige und korrekte Erfüllung der Informationspflichten zu treffen.

Anlage 18

Kurzpapier Nr. 11
Recht auf Löschung / „Recht auf Vergessenwerden“

Dieses Kurzpapier der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) dient als erste Orientierung insbesondere für den nicht-öffentlichen Bereich, wie nach Auffassung der DSK die Datenschutz-Grundverordnung (DS-GVO) im praktischen Vollzug angewendet werden sollte. Diese Auffassung steht unter dem Vorbehalt einer zukünftigen – möglicherweise abweichenden – Auslegung des Europäischen Datenschutzausschusses.

Mit dem Inkrafttreten der DS-GVO erfährt die Löschung personenbezogener Daten gegenüber der bisherigen Rechtslage insofern eine Aufwertung, als die diesbezüglichen Bestimmungen detaillierter ausformuliert worden sind und zum Teil auch darüber hinausgehen. Das mit dem Löschungsanspruch der betroffenen Person verbundene „Recht auf Vergessenwerden“ wird zum ersten Mal ausdrücklich gesetzlich geregelt; es ergänzt die Löschung unmittelbar beim Verantwortlichen und die bereits bislang im BDSG verankerten Nachberichtspflichten.

Löschungspflicht
Wie aktuell in § 35 Abs. 2 BDSG-alt vorgesehen, bestimmt auch Art. 17 Abs. 1 DS-GVO, dass personenbezogene Daten auf Verlangen der betroffenen Person und/oder unter bestimmten Voraussetzungen ohne Verlangen der betroffenen Person eigenständig durch den Verantwortlichen unverzüglich gelöscht werden müssen. Art. 17 Abs. 1 DS-GVO benennt dazu folgende Fälle:

a) Die Notwendigkeit der Verarbeitung zur Zweckerreichung ist entfallen.
b) Die betroffene Person hat ihre Einwilligung widerrufen und es besteht auch keine sonstige Rechtsgrundlage.
c) Die betroffene Person legt gem. Art. 21 Abs. 1 oder 2 DS-GVO Widerspruch gegen die Verarbeitung ein; im Falle des Art. 21 Abs. 1 gilt dies nur, soweit keine vorrangigen berechtigten Gründe für die Verarbeitung vorliegen. Das Widerspruchsrecht

nach Art. 21 Abs. 1 DS-GVO besteht ausschließlich bei Verarbeitungen, die auf Art. 6 Abs. 1 lit. e oder f DS-GVO gründen. Für die Löschungsverpflichtung bedarf es dabei einer Interessenabwägung. Anders bei Widersprüchen in Bezug auf Direktwerbung (Art. 21 Abs. 2 DS-GVO): Hier bedarf es keiner Interessenabwägung.

d) Die personenbezogenen Daten wurden unrechtmäßig verarbeitet.
e) Die Löschung ist zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erforderlich, dem der Verantwortliche unterliegt.
f) Die personenbezogenen Daten wurden in Bezug auf angebotene Dienste der Informationsgesellschaft gemäß Art. 8 Abs. 1 DS-GVO erhoben.

Der Verweis auf Art. 8 Abs. 1 DS-GVO (Einwilligung eines Kindes in Bezug auf Dienste der Informationsgesellschaft) impliziert, dass die Daten rechtmäßig erhoben wurden. Eine Löschungspflicht ergibt sich damit allein aufgrund des Löschungsverlangens der betroffenen Person. Weil Diensten der Informationsgesellschaft (z. B. Soziale Netzwerke, Online-Spiele) in Bezug auf Minderjährige weniger Schutzbedarf als den betroffenen Personen zugestanden wird, bedarf es neben dem Löschungsverlangen keiner weiteren Voraussetzung; auch kann dieser Anspruch noch als Erwachsener geltend gemacht werden.

Recht auf Vergessenwerden

Das „Recht auf Vergessenwerden“ gem. Art. 17 Abs. 2 DS-GVO bezieht sich, obwohl der Begriff im ErwGr. 65 als Synonym für „Löschung“ verwendet wird, auf die Tilgung (von Spuren) personenbezogener Daten, die durch Veröffentlichungen, insbesondere im Internet, einer breiten Öffentlichkeit zugänglich sind.

Der Verantwortliche, der die personenbezogenen Daten öffentlich gemacht hat und der gemäß Art. 17 Abs. 1 DS-GVO zu deren Löschung verpflichtet ist, hat unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten angemessene Maßnahmen, auch technischer Art, zu treffen, um für die Datenverarbeitung Verantwortliche, die die personenbezogenen Daten (gleichfalls) verarbeiten, darüber zu informieren, dass eine betroffene Person von ihnen die Löschung aller Links zu diesen personenbezogenen Daten

oder von Kopien oder Replikationen dieser personenbezogenen Daten verlangt hat.
Danach zieht der berechtigte Löschungsantrag einer betroffenen Person bzw. die bestehende Löschungspflicht eines Verantwortlichen dessen Pflicht nach sich, weitere Verantwortliche, die die zu löschenden Daten (noch) verarbeiten, über ein Verlangen des Betroffenen nach Löschung von Links, Kopien oder Replikationen zu informieren. Das Unterlassen entsprechender Bemühungen wird angesichts des Wortlauts der Norm und der fortlaufenden technischen Entwicklung nicht mit einem einfachen Verweis des Verantwortlichen auf unzumutbaren Aufwand begründet werden können.

Ausnahmen von der Löschungspflicht
Die Pflicht zur Löschung nach Art. 17 Abs. 1 und die Pflicht zur Information weiterer Verantwortlicher nach Art. 17 Abs. 2 DS-GVO entfallen, wenn gemäß Art. 17 Abs. 3 DS-GVO die Verarbeitung erforderlich ist

a) zur Ausübung des Rechts auf freie Meinungsäußerung und Information;
b) zur Erfüllung einer rechtlichen Verpflichtung, zur Wahrnehmung einer Aufgabe im öffentlichen Interesse oder zur Ausübung öffentlicher Gewalt;
c) aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit;
d) für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gem. Art. 89 Abs. 1 DS-GVO, soweit die Löschung die Verwirklichung dieser Ziele ernsthaft beeinträchtigt;
e) zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

Allerdings berechtigen die benannten Ausnahmen nicht zu einer zeitlich unbegrenzten Verarbeitung der jeweiligen personenbezogenen Daten. Auch diese Zwecke werden zu einem bestimmten Zeitpunkt erfüllt und die Verarbeitung der Daten wird zur Zweckerreichung nicht mehr erforderlich sein. Dann sind auch diese Daten zu löschen.

Nachberichtspflichten
Die bislang schon bestehenden Nachberichtspflichten zur Löschung (§ 35 Abs. 7 BDSG-alt) bleiben bestehen. Art. 19 DS-GVO verpflichtet den Verantwortlichen, allen Empfängern, denen personenbezogene Daten offengelegt wurden, jede Löschung der personenbezogenen mitzuteilen, es sei denn, dies erweist sich als unmöglich oder ist mit einem unverhältnismäßigen Aufwand verbunden.

Beschränkung des Löschungsanspruchs
Art. 23 DS-GVO befugt die Union und die Mitgliedstaaten, die Löschung gesetzlich zu beschränken, sofern eine solche Beschränkung den Wesensgehalt der Grundrechte und Grundfreiheiten achtet, eine notwendige und verhältnismäßige Maßnahme darstellt und (zumindest) einem der in Art. 23 Abs. 1 lit. a bis j DS-GVO genannten Zwecke dient. Hiervon hat der Bundesgesetzgeber in § 35 BDSG-neu Gebrauch gemacht: Im Fall nicht automatisierter Datenverarbeitung und unter den weiteren dort genannten Voraussetzungen ist statt des Löschungsanspruchs der betroffenen Person ein Anspruch auf Einschränkung der Verarbeitung gemäß Art. 18 DS-GVO vorgesehen.

Anwendbarkeit der Regelungen des BDSG-neu
Es bestehen jedoch Zweifel, ob die in § 35 BDSG-neu vorgesehenen Beschränkungen des Rechts auf Löschung nach Art. 23 DS-GVO zulässig sind. Jedenfalls sind diese Regelungen grundsätzlich eng und im Sinne einer größtmöglichen Transparenz auszulegen. Ob und in welchem Umfang eine in § 35 BDSG-neu vorgesehene Beschränkung des Rechts auf Löschung aufgrund des Anwendungsvorrangs der DS-GVO tatsächlich angewendet werden kann, bleibt einer Entscheidung im jeweiligen konkreten Einzelfall vorbehalten.

Sanktionen
Bei Verstößen gegen die Löschungs- oder Nachberichtspflichten droht die Einleitung eines Bußgeld-verfahrens (Art. 83 Abs. 5 lit. b DS-GVO).

Abkürzungsverzeichnis

Abs.	Absatz
ADV	Auftragsdatenverarbeitung
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
AGB	Allgemeine Geschäftsbedingungen
AMD	Arbeitsmedizinischer Dienst
AöR	Anstalt des öffentlichen Rechts
ArbMedVV	Verordnung zur arbeitsmedizinischen Vorsorge
Art.	Artikel
ASiG	Arbeitssicherheitsgesetz
Aufl.	Auflage
Az.	Aktenzeichen
BayLfDI	Bayerischer Landesbeauftragter für den Datenschutz und die Informationsfreiheit
BDSG	Bundesdatenschutzgesetz
bDSG	behördlicher Datenschutzbeauftragter/ betrieblicher Datenschutzbeauftragter
BGB	Bürgerliches Gesetzbuch
BI	Bürgerinitiative
BMG	Bundesmeldegesetz
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSI-KritisV	BSI-Kritisverordnung
BVerfG	Bundesverfassungsgericht
bzw.	beziehungsweise
ca.	zirka
ChemVerbotsV	Chemikalien-Verbotsverordnung
d. h.	das heißt
DAkkS	Deutsche Akkreditierungsstelle GmbH
DSFA	Datenschutz-Folgenabschätzung

DS-GVO	Datenschutz-Grundverordnung
e. V.	eingetragener Verein
EU	Europäische Union
EU-DSAnpUG-EU	Datenschutz-Anpassungs- und -Umsetzungsgesetz EU
EU-DS-GVO	Europäische Datenschutzgrundverordnung
EWR	Europäischer Wirtschaftsraum
GastG	Gaststättengesetz
gem.	gemäß
GesDV	Gesundheitsdienstverordnung
ggfs.	gegebenenfalls
GPS	Global-Positioning-System
grds.	grundsätzlich
GwG	Geldwäschegesetz
HGB	Handelsgesetzbuch
HS	Halbsatz
i. d. R.	in der Regel
i. S. d.	im Sinne des
i. V. m.	in Verbindung mit
InsO	Insolvenzordnung
Kfz	Kraftfahrzeug
Kita	Kindertageseinrichtung
KUG	Kunsturhebergesetz
LfD SL	Landesbeauftragter für den Datenschutz Saarland
LG	Landgericht
LPI	Landespolizeiinspektion
LRA	Landratsamt
Mio.	Millionen
Nr.	Nummer

NRW	Nordrhein-Westfalen
NSL	Notrufserviceleitstelle
o. g.	oben genannte/r/s
OVG	Oberverwaltungsgericht
PAuswG	Personalausweisgesetz
PC	Personalcomputer
PI	Polizeiinspektion
Rn.	Randnummer
s. a.	siehe auch
sog.	sogenannte(s,r)
StGB	Strafgesetzbuch
SV	Stadtverwaltung
ThürDSG	Thüringer Datenschutzgesetz
ThürSpiel-hallenG	Thüringer Spielhallengesetz
ThürVwVfG	Thüringer Verwaltungsverfahrensgesetz
ThürWTG	Thüringer Gesetz über betreute Wohnformen und Teilhabe
TKG	Telekommunikationsgesetz
TLfDI	Thüringer Landesbeauftragter für den Datenschutz und die Informationsfreiheit
TOMs	technische und organisatorische Maßnahmen
TPG	Thüringer Pressegesetz
u. a.	unter anderem
u. ä.	und ähnliches
u. U.	unter Umständen
UAbs.	Unterabsatz
usw.	und so weiter
UVV	Unfallverhütungsverordnung
VG	Verwaltungsgericht
vgl.	vergleiche

z. B.	zum Beispiel
ZB	Zwischenbericht
ZPO	Zivilprozessordnung

Stichwortverzeichnis/ Index

(DS-GVO 12.3
§ 201 StGB 6.32
§ 28 BDSG 3.44
§ 42a 5.1
66399 ..... 3.29
Abgabenordnung 3.32, 3.22
Abrufverfahren 4.4
Abschleppdienst 3.6
Abwägung 12.7, 9.1, 7.22, 7.18, 7.1, 6.69, 6.64, 6.62, 6.58, 6.38, 6.37, 6.27, 5.1, 3.45
Adresse 12.11, 12.7, 12.6, 10.19, 10.16, 10.9, 6.36, 6.31, 6.30, 6.20, 6.14, 5.1, 4.3, 3.46, 3.45, 3.44, 3.42, 3.40, 3.26, 3.20, 3.19, 3.18, 3.10, 3.9
Akten.. 10.18, 10.11, 10.2, 7.6, 3.47, 3.42, 3.39, 3.34, 3.29, 3.26, 2.6
Akteneinsicht 10.6, 10.2, 6.30, 3.42
Aktenlager 3.29, 3.1
Aktenvernichtung 10.18, 3.39, 3.34, 2.6
Alarm 6.10
allgemeines Persönlichkeitsrecht 6.62, 6.48, 6.46, 6.27, 6.26, 6.13
Altakten 3.47
Altenhilfe 7.6
Amtsarzt 10.16
Amtshandlung 6.57
Amtshilfe 6.57, 6.43, 6.12, 3.42, 3.1
Anlage 6.50
Anonymisierung 12.12, 7.22
Anordnung 6.46, 6.42, 6.37, 6.30, 6.10, 4.3, 3.32
Anpassungsgesetz zur EU-Datenschutz-Grundverordnung (EU-DSAnpUG-EU) 6.38
Anschrift 8.1, 6.12, 4.3, 4.2, 3.45, 3.44, 3.40, 3.36, 3.32, 3.26, 3.18, 3.14, 3.13, 3.12, 3.11, 3.6, 3.3, 3.2
Ansteckung 10.1
Anwendungssoftware 4.5
Anzeigenerstatter 6.62
Apotheke 10.19, 10.9, 10.4, 10.3, 6.68
Apotheker 10.19, 10.9, 10.3, 6.68
App 12.15, 12.4, 10.22, 10.20, 10.5, 6.10, 6.3, 4.5, 3.33, 3.24
App-Entwicklung 4.5

Approbation 10.22
Arbeitgeber 10.2, 7.22, 7.21, 7.20, 7.19, 7.18, 7.17, 7.16, 7.14, 7.13, 7.11, 7.9, 7.8, 7.5, 7.4, 7.2, 6.71, 6.28, 4.1, 3.25
Arbeitnehmer ..... *Siehe* Beschäftigte
Arbeitnehmerdatenschutz 7.22, 6.9
Arbeitnehmerüberlassung 7.10
Arbeitsleistung 7.22, 7.15
Arbeitsplatzrechner 7.13
Arbeitsplatzüberwachung 6.71
Arbeitssicherheitsgesetz 10.2, 7.9
Arbeitsunfall 7.12
Arbeitsverhältnis 10.2, 7.22, 7.20, 7.19, 7.8, 2.2
Arbeitsvermittlung 7.19, 7.8
Arbeitsvertrag 7.17, 7.9
Arbeitszeit 7.17, 7.15
Armaturenbrett 6.62
Art der Daten 3.30
Arzt 10.22, 10.15, 10.14, 10.11, 10.10, 10.6, 10.1, 7.9, 7.9, 3.26
Arztpraxis 10.14, 10.11, 10.10, 10.9, 10.8, 10.7, 5.1, 3.26
Attest 10.16
Attrappe 6.68, 6.67, 6.56, 6.55, 6.54, 6.51, 6.48, 6.43, 6.35, 6.34, 6.27, 6.22, 6.19, 6.16
Aufbewahrungsfrist 10.18
Aufbewahrungsfriste 7.6
Aufgaben 12.8, 10.16, 10.4, 10.2, 7.6, 7.5, 6.68, 6.57, 6.32, 6.17, 4.2, 3.36, 3.30, 3.18, 2.5, 2.4, 2.3, 2.2
Aufnahmebereich 7.5, 6.71, 6.68, 6.64, 6.56, 6.53, 6.50, 6.43, 6.32, 6.27, 6.23, 6.21, 6.11, 6.8, 6.5
Aufsichtsbehörde 12.9, 12.6, 12.1, 11.1, 10.12, 10.11, 10.5, 10.4, 10.2, 7.5, 7.3, 6.68, 6.42, 6.41, 6.40, 6.39, 6.38, 6.37, 6.32, 6.27, 6.24, 6.21, 6.20, 6.18, 6.14, 6.12, 6.11, 6.9, 6.3, 6.2, 5.1, 4.3, 3.41, 3.35, 3.21, 3.20, 3.18, 3.3, 3.2, 2.6, 2.5
Auftragsdatenverarbeitung 12.6, 10.18, 10.12, 10.5, 3.47, 3.39, 3.34, 3.24, 3.5, 2.1
Aufzeichnung 10.20, 10.2, 7.17, 7.1, 6.74, 6.64, 6.62, 6.58, 6.50, 6.41, 6.40, 6.29, 6.28, 6.23, 6.23, 6.20, 6.13, 6.13, 6.8, 6
Auskunft 10.13, 10.11, 10.6, 10.5, 10.3, 10.2, 9.3, 9.2, 9.1, 8.2, 8.1, 7.18, 7.16, 7.15, 7.11, 7.10, 7.8, 7.7, 6.68, 6.67, 6.44, 6.43, 6.42, 6.30, 6.29, 6.28, 6.27, 6.17, 6.12, 6.10, 4.5, 3.43, 3.42, 3.31, 3.25, 3.23, 3.23, 3.19, 3.15, 3.13, 3.8, 3.7

Auskunftei 9.2, 9.1, 3.19
Auskunfteiabfrage 9.2, 9.1
Auskunftsanspruch 8.1, 3.43, 3.7
Auskunftsbescheid 6.42
Auskunftsersuchen 10.6, 10.3, 9.3, 8.2, 7.20, 7.1, 6.76, 6.75, 6.74, 6.69, 6.68, 6.64, 6.52, 6.45, 6.42, 6.36, 6.30, 6.28, 6.27, 6.9, 6.8, 6.7, 6.4, 3.43, 3.36, 3.27, 3.17, 3.13, 3.7, 3.3
Auskunftserteilung 6.17, 6.14, 3.23
Auskunftspflicht 8.2, 7.10, 6.63, 6.32, 3.43, 3.13
Auskunftsrecht 12.4, 9.3, 7.10, 6.26
Auskunftsverlangen 10.11, 10.7, 9.3, 7.21, 7.10, 7.4, 6.71, 6.63, 6.53, 6.50, 6.48, 6.47, 6.46, 6.44, 6.35, 6.16, 6.6, 6.5, 4.3, 3.45, 3.43, 3.16, 3.7, 3.2
Auskunftsverweigerung 6.17, 3.23
Ausland 3.42, 3.30, 3.20
außereuropäisches Ausland 3.30, 1
Ausweichfläche 6.48
Ausweiskopie 3.14, 3.12, 3.6
Authentifizierung 12.10, 12.8, 10.5, 2.7
Auto 12.4, 6.62, 6.54, 3.6
Autohaus 6.59, 6.31, 3.7, 3.6
automatisierte Verarbeitung 7.18, 7.5, 6.58, 6.39, 6.28, 6.21, 6.9, 6.2, 3.2, 2.6, 2.5, 2.1
Bade- und Ruhebereich 6.40
Bank 9.1, 9.1, 5.1, 3.44, 3.44, 3.35, 3.23, 3.23, 3.22, 3.22
Baumarkt 3.10
Bauordnungsamt 3.42
Baustelle 6.11
Baustellenkamera 6.11
bDSB 3.42, 3.30, 2.6, 2.5, 2.3, 2.2, 2.1
Behandlungsfehler 10.8, 10.7
behinderte Menschen 7.14
Behördenebene 6.57
behördlicher Datenschutzbeauftragter 13.2, 3.42, 3.30, 2.1
Beitragszahlung 3.25
Beobachtung 7.17, 7.1, 6.75, 6.74, 6.72, 6.71, 6.70, 6.69, 6.66, 6.64, 6.62, 6.61, 6.60, 6.58, 6.54, 6.50, 6.48, 6.44, 6.41, 6.40, 6.36, 6.35, 6.29, 6.23, 6.20, 6.15, 6.14, 6.13, 6.11, 6.8, 6.7, 6.6, 6.3, 2.1
Beobachtungsbefugnis 6.66, 6.58, 6.54, 6.53, 6.50, 6.48, 6.44, 6.33, 6.31, 6.24, 6.23, 6.21, 6.16

Beobachtungskamera 6.63
Beratung 10.16, 10.6, 7.17, 7.12, 6.55, 6.51, 6.14, 4.1, 3.41, 2.4
Beratung durch den TLfDI 7.12, 6.41
Beratungsersuchen gem. § 38 Abs. 1 Satz 2 BDSG 2.4
berechtigte Interessen 9.2, 8.1, 7.17, 7.9, 7.5, 7.4, 7.1, 6.76, 6.75, 6.74, 6.72, 6.71, 6.70, 6.69, 6.66, 6.65, 6.64, 6.61, 6.60, 6.59, 6.58, 6.53, 6.48, 6.44, 6.40, 6.38, 6.37, 6.36, 6.35, 6.34, 6.31, 6.29, 6.28, 6.27, 6.26, 6.24, 6.23, 6.21, 6.20, 6.18, 6.16, 6.15, 6.13, 6.11, 6.9, 6.8, 6.7, 6.6, 6.5, 6.4, 6.3, 4.3, 3.45, 3.37, 3.31, 3.28, 3.19, 3.15, 3.14, 3.8, 3.4, 3.3
Berufsgeheimnis 10.6, 5.1, 3.34
Berufsgeheimnisträger 10.6, 10.3, 5.1, 3.34, 3.26
Beschädigungen 6.75, 6.59, 6.55, 6.53, 6.48, 6.44, 6.40, 6.27, 6.20, 6.16
Beschäftigte 14, 10.17, 10.2, 7.22, 7.20, 7.19, 7.18, 7.17, 7.16, 7.15, 7.14, 7.14, 7.13, 7.12, 7.11, 7.10, 7.9, 7.8, 7.5, 7.4, 7.2, 7.1, 6.71, 6.69, 6.28, 6.8, 6.6, 4.1, 3.30, 3.25, 2.3
Beschäftigtendaten 7.20, 7.17, 7.16, 7.5, 4.1
Beschäftigtendatenschutz 7.16, 7.15, 7.4, 6.28, 6.8, 1
Beschäftigungsverhältnis 7.20, 7.18, 7.16, 7.15, 7.8, 6.28, 6.11
Bescheid 6.71, 6.30, 6.17, 3.15
Beschwerde 12.5, 10.21, 10.16, 10.15, 10.10, 10.9, 10.6, 10.4, 9.3, 8.1, 7.21, 7.20, 7.19, 7.18, 7.17, 7.10, 7.8, 7.7, 7.5, 7.3, 7.2, 6.74, 6.71, 6.68, 6.66, 6.64, 6.63, 6.57, 6.56, 6.54, 6.53, 6.52, 6.51, 6.50, 6.48, 6.44, 6.37, 6.36, 6.33, 6.31, 6.30, 6.29, 6.27, 6.26, 6.22, 6.18, 6.17, 6.16, 6.15, 6.14, 6.13, 6.9, 6.8, 6.5, 6.4, 3.46, 3.44, 3.43, 3.36, 3.27, 3.22, 3.21, 3.20, 3.17, 3.16, 3.15, 3.13, 3.12, 3.11, 3.9, 3.8, 3.7, 3.6, 3.5, 3.2
besondere Art personenbezogener Daten 10.18, 10.11, 10.10, 10.9, 10.5, 10.1, 6.37, 5.1, 3.41, 3.39, 3.37, 3.26, 3.4
Bestattung 3.13
Bestattungsunternehmen 3.13
Bestattungswald 3.28
Bestellpflicht 3.30, 2.5, 2.1
Bestellung des DSB 2.5, 2.3, 2.2
Bestimmbarkeit 3.17
Besucher 7.1, 6.75, 6.74, 6.71, 6.69, 6.52, 6.48, 6.37, 6.27, 6.25, 6.23, 6.18, 6.15, 6.8, 6.4, 3.3
Betäubungsmittelgesetz 6.5

Betreiber 12.10, 12.9, 12.7, 12.4, 12.2, 10.20, 10.5, 6.76, 6.75, 6.74, 6.67, 6.66, 6.65, 6.64, 6.63, 6.58, 6.56, 6.52, 6.50, 6.47, 6.44, 6.43, 6.42, 6.38, 6.32, 6.30, 6.29, 6.27, 6.26, 6.24, 6.22, 6.20, 6.19, 6.18, 6.14, 6.13, 6.9, 6.7, 6.6, 6.3, 6.1, 3.35, 3.19, 3.8
Betreuer 7.14
Betreuungseinrichtung 10.1
betrieblicher Datenschutzbeauftragter 13.2, 11.1, 10.2, 9.3, 7.5, 7.5, 7.4, 6.21, 6.9, 6.3, 3.23, 3.7, 3.2, 2.5, 2.4, 2.4, 2.3, 2.2
Betriebsarzt 10.2, 7.10
Betriebsarztdokumentation 10.2
Betriebsstätte 7.21, 7.16, 3.23, 3.20
Betriebsvereinbarung 7.18
Bewegungsmelder 6.62, 6.7
Bewegungsprofil 7.22, 7.18, 7.11, 6.18
Beweiserheblichkeit 6.62
Beweismittel 6.62, 6.57
Beweissicherung 7.5, 6.71, 6.66, 6.62, 6.50, 6.36, 6.4, 6.3
Beweissicherungsinteresse 6.62
Bewerber 7.21, 3.7
Bewerbers 7.20
Bewerbung 7.21, 7.20, 7.19, 7.10, 7.8, 7.7, 3.7
Bewerbungsunterlagen 7.21, 7.20, 7.19, 7.10
Bewerbungsverfahren 7.7, 3.7
Biergarten 6.6
Bildauflösung 6.25
Bilder 7.14, 7.12, 6.75, 6.64, 6.62, 6.57, 6.52, 6.51, 6.50, 6.38, 6.29, 6.28, 6.23, 6.20, 6.19, 6.18, 6.13, 6.11, 6.9, 6.3, 6.2, 3.6
Biometrie 12.10
Black-Box-Verfahren 6.40, 6.38
Black-List 2.6
Blickwinkel 6.62, 6.23, 6.14
Bluetooth 12.15, 12.3
Bombenbau 3.14
Bonitätsabfrage 9.2, 3.19
Bonitätsprüfung 3.19
Botnetz 12.11
BSI 12.13, 12.11, 12.8, 10.5, 7.13, 2.2
BSI-Gesetz 12.9
BSI-Kritisverordnung 12.9, 12.2
Bundesmeldegesetz 3.11

Bundesnetzagentur 12.15, 12.9, 12.8, 8.1
Bundesverfassungsgericht 6.62, 6.48, 6.34, 6.13, 1
Büro 7.3, 6.66, 6.32, 6.28, 6.8
Büroeingang 6.66
Bußgeldtatbestand 6.2
Bußgeldverfahren 11.1, 10.9, 7.19, 7.5, 7.2, 6.69, 6.62, 6.44, 6.32, 6.30, 6.24, 6.19, 6.17, 6.2, 6.1, 2.4, 1
Campingplatz 6.29
Canvas-Blocker 12.12
Cayla 12.15
CDU 3.1
Checkliste 5.1
Cookie-Richtlinie 12.3
Dachverband 4.2, 3.18
Dashboardcams 6.62
Dashcams 6.62, 1
Data protection by default 12.4, 10.20
Datendiebstahl 10.4, 5.1
Datenerhebung 10.9, 9.2, 6.75, 6.71, 6.61, 6.7, 6.6, 6.4, 6.2, 6.1, 4.5, 4.1, 3.44, 3.40, 3.31, 3.28, 3.11, 3.10, 3.8, 3.6, 3.3, 3.2
Datenermittlung 6.61
Datenpanne 5.1
Datenschutzbeauftragter 13.2, 12.13, 12.10, 12.7, 12.5, 12.3, 12.1, 10.18, 10.14, 10.13, 10.12, 10.6, 10.2, 9.3, 7.15, 7.12, 7.5, 7.3, 6.32, 6.28, 6.24, 6.9, 6.3, 3.37, 3.30, 3.23, 3.22, 3.20, 3.18, 2.6, 2.5, 2.4, 2.4, 2.3, 2.2, 2.1
Datenschutz-Folgenabschätzung 10.12, 2.6, 2.1
Datenschutz-Grundverordnung 13.2, 12.3, 11.1, 10.12, 6.72, 6.60, 6.41, 6.40, 6.38, 6.1, 2.6, 2.1, 1
datenschutzrechtliche Einwilligungserklärung 3.40, 3.11
Datenträgervernichtung 10.13, 2.6
Datenübermittlung 10.16, 10.14, 10.6, 7.9, 4.4, 4.2, 3.45, 3.40, 3.37, 3.30, 3.28, 3.26, 3.18, 3.8, 3.4, 1
Datenübertragung 10.5
Datenverarbeitung im Auftrag 10.18, 7.8, 6.27, 3.5
Datenweitergabe 4.2, 3.28, 3.26, 3.18
Deutsche Post AG 3.48
Deutscher Presserat 3.21
Diebstahl 7.4, 7.1, 6.59, 6.53, 6.50, 6.29, 6.8, 6.6, 6.5, 5.1, 2.7
Dienstkräfte 6.57

Dienstpläne 7.6, 2.7
digitale Unterschrift 3.38
digitaler Türspion 6.13
DIN 32757-1 ..... 3.34
DIN 66399 ..... 10.21, 10.18, 10.13
DIN 66399-1 ..... 3.39
DIN 66399-2 ..... 3.47
Diözesandatenschutzbeauftragter 3.48
Diskothek 6.76
Double-Opt-In 3.9
Drehkreuze 6.40, 6.37
DS-GVO 12.4, 12.1, 11.1, 10.20, 10.12, 6.72, 6.60, 6.41, 6.40, 6.38, 3.30, 2.6, 2.1, 1
Durchsuchungsbeschluss 6.30
dynamische IP-Adresse 12.7
e-Datenschutz-Richtlinie 12.3
eID 12.13
eIDAS-Durchführungsgesetz 12.8
eIDAS-Verordnung 12.8
eigene Grundstück 6.54
eigenes Grundstück 6.75, 6.67, 6.66, 6.64, 6.58, 6.52, 6.43, 6.37, 6.33, 6.24, 6.23, 6.21, 6.18
Eigentümer 12.11, 12.4, 6.75, 6.74, 6.55, 6.53, 6.47, 6.46, 6.45, 6.36, 6.35, 6.34, 6.33, 6.31, 6.29, 6.27, 6.20, 6.12, 6.7, 6.4, 3.47, 3.42, 3.8
Eigentumsrecht 6.51
Einbrüche 7.5, 7.3, 6.67, 6.66, 6.59, 6.53, 6.50, 6.32, 6.29, 6.28, 6.27, 6.20, 6.16, 6.13, 6.10, 6.8, 6.7, 6.5, 5.1, 2.7
Eingangs- und Kassenbereich 6.40
Eingangsbereich 7.3, 7.1, 6.76, 6.75, 6.74, 6.71, 6.67, 6.66, 6.45, 6.36, 6.27, 6.22, 6.18, 6.15, 6.13, 6.6, 6.4, 6.3
Eingriff 12.9, 12.7, 7.21, 6.75, 6.74, 6.72, 6.72, 6.69, 6.68, 6.67, 6.65, 6.64, 6.62, 6.58, 6.56, 6.55, 6.48, 6.46, 6.41, 6.40, 6.34, 6.27, 6.26, 6.23, 6.13, 3.6, 3.4
Einkaufen 6.3, 3.19
Einkaufszentrum 3.33
Einlasskontrolle 6.18, 6.13
Einrichtung 12.7, 12.4, 10.17, 10.1, 7.17, 7.14, 7.6, 6.76, 6.75, 6.72, 6.71, 6.70, 6.69, 6.64, 6.61, 6.60, 6.57, 6.44, 6.38, 6.35, 6.29, 6.21, 6.16, 6.13, 6.7, 6.3, 3.39, 2.7, 1

Einsichtsrecht 10.6
Eintrittskarten 3.3
Einverständnis 10.7, 7.5, 6.71, 6.69, 6.64, 6.14, 3, 3.20, 3.16
Einwilligung 12.7, 12.4, 12.3, 10.16, 10.14, 10.9, 10.8, 10.7, 10.6, 10.3, 10.2, 10.1, 9.2, 7.22, 7.21, 7.20, 7.19, 7.14, 7.10, 7.9, 7.5, 7.3, 7.2, 6.75, 6.72, 6.71, 6.52, 6.44, 6.39, 6.34, 6.27, 6.23, 6.21, 6.20, 6.18, 6.15, 6.13, 6.12, 6.11, 6.8, 6.7, 6.6, 6.4, 6.2, 4.3, 4.2, 3.45, 3.44, 3.40, 3.38, 3.37, 3.33, 3.30, 3.28, 3.26, 3.25, 3.18, 3.17, 3.16, 3.15, 3.12, 3.11, 3.10, 3.9, 3.8, 3.3, 1
Einwilligungserklärung 10.20, 10.14, 10.9, 7.21, 7.19, 7.14, 6.75, 6.69, 3.41, 3.40, 3.36, 3.26, 3.18, 3.11
E-Learning-Plattform 12.10
Eltern 10.16, 7.14, 6.53
Entsorgung 10.21, 3.47, 3.34
e-Privacy-Richtlinie 12.3
e-Privacy-Verordnung 12.3
ERFA-Kreis 13.2
Erfassungsbereich 6.76, 6.71, 6.67, 6.58, 6.55, 6.52, 6.51, 6.49, 6.44, 6.43, 6.36, 6.34, 6.33, 6.27, 6.24, 6.23, 6.21, 6.16, 6.11, 6.3
Erfassungsblatt Kameras 6.41
Erforderlichkeit 9.2, 7.22, 6.76, 6.75, 6.66, 6.64, 6.60, 6.58, 6.41, 6.40, 6.37, 6.23, 6.6, 6.4, 6.3, 4.3, 3.45, 3.14, 3.10, 3.3
Erlaubnisnorm 12.4, 6.41, 6.23, 6.21, 6.18, 6.8, 6.7, 6.6, 3.44, 3.32, 3.31, 3.15, 3.11, 3.8, 3.3
Etage 6.16, 3.45
EuGH C-212/13 (Rynes-Urteil) 6.37
Europäische Datenschutz-Grundverordnung 12.4, 6.38
externer Datenschutzbeauftragter 10.14, 7.4, 6.69, 3.7, 2.5, 2.4, 2.1
Facebook 12.5, 7.2, 5.1
Fachkunde 13.2, 7.5, 2.5, 2.4, 2.3, 2.2
Fahrgastbereich bzw. -raum 6.72
Fahrzeug 12.4, 7.11, 7.4, 6.75, 6.72, 6.62, 6.61, 6.54, 6.53, 6.38, 6.5, 3.6, 1
familiäre und persönliche Tätigkeit 6.66, 6.52, 6.37, 6.23, 6.16
Familienversicherung 10.15
Fassade 6.55, 6.54, 6.50, 6.48, 6.17, 6.4
Fassadenteile 6.5
Fenster 6.66, 6.64, 6.50, 6.48, 6.16, 6.14, 2.7
Festlegung 10.18, 10.16, 10.2, 7.18, 7.17, 7.15, 7.11, 7.7, 7.4, 7.2, 6.41, 6.28, 6.5, 6.4, 6.3, 3.38, 2.7

Filiale 7.16, 3.23, 3.22
Fingerprinting 12.12
Firmengelände 6.64, 6.60, 6.39, 6.28, 6.8
Firmensitz 6.8, 3.42
Firmenwagen 7.18, 7.11, 7.4
Fitnessstudio 7.3
Fitness-Tracker 10.20
Foto 12.5, 10.19, 10.8, 10.7, 7.21, 6.66, 6.61, 6.54, 6.50, 6.47, 6.30, 6.19, 6.16, 6.11, 3.42, 3.40, 3.29, 2.7
Fotoaufnahme 10.8, 10.7, 6.12
Fotodokumentation 10.7, 6.57, 3.6
Fragenkatalog 6.68, 6.63, 6.53, 6.50, 6.48, 6.42, 6.22, 6.16, 6.5, 3.38
Freiwilligkeit 12.4, 7.2, 6.71, 6.69, 6.11, 6.8, 6.6, 3.25
Freizeitpark 7.1
Friedhof 6.63
Fristsetzung 9.3, 6.17, 3.7
Garage 6.44, 6.24, 6.5
Garagenzufahrt 6.66
Garten 6.75, 6.67, 6.51, 6.23, 6.22, 6.4
Gartenanlage 6.49
Gäste . 7.1, 6.74, 6.72, 6.40, 6.37, 6.32, 6.29, 6.23, 6.6, 3.11, 3.8, 3.3
Gastraum 6.74, 6.72, 6.6
Gaststätte 6.74, 6.29, 6.6
Gaststättengesetz 6.74
Gebäude 6.75, 6.69, 6.67, 6.66, 6.64, 6.55, 6.54, 6.53, 6.50, 6.48, 6.47, 6.46, 6.45, 6.44, 6.36, 6.34, 6.33, 6.30, 6.29, 6.28, 6.27, 6.22, 6.19, 6.17, 6.16, 6.15, 6.14, 6.13, 6.12, 6.8, 6.7, 6.6, 6.4, 3.47, 3.42, 3.29, 3.14, 2.7
Gebäudeservice 3.12
Geeignetheit 6.76, 6.28, 6.4
Gefahr für Leib und Leben 10.1
Gefährdung 12.2, 6.71, 6.53, 6.38, 6.27, 6.20, 6.5
Gefahrenlage 6.76, 6.75, 6.72, 6.71, 6.69, 6.53, 6.48, 6.38, 6.27, 6.20, 6.16, 6.13, 6.7, 6.5, 6.4
Geheimnis 10.11, 10.10, 10.3, 10.1, 3.47, 3.39, 3.34, 3.26
Gehweg 6.76, 6.75, 6.67, 6.50, 6.48, 6.45, 6.44, 6.37, 6.24, 6.21, 6.20, 6.18, 6.16, 6.8, 6.4
Geldbuße 11.1, 6.68, 6.63, 6.60, 3.7
Geldspielgeräte 6.71
Geldwäsche 3.22

Geldwäschegesetz 3.22, 3.12
Gemeindekindergarten 6.53
Geschäft des täglichen Lebens 4.1
Geschäftsbedingungen 9.2, 6.3, 3.5
gespeicherte Daten 10.13, 9.1, 8.2, 7.10, 7.8, 7.7, 6.32, 3.43, 3.23, 3.13, 3.7
Gesundheit . 12.4, 12.2, 10.20, 10.19, 10.15, 10.14, 10.2, 10.1, 5.1, 1
Gesundheit oder Freiheit von Personen 6.72, 6.61, 6.38
Gesundheitsdaten 10.20, 10.18, 10.13, 10.11, 10.10, 10.9, 10.6, 10.5, 10.1, 5.1, 3.39, 3.37, 3.26
Gesundheitsverordnung 10.16
Gesundheitsvorsorge 10.2, 10.1
Gewerbeamt 6.7, 3.42
Gewerbetreibende 6.31, 6.5
Google Analytics 12.6
GPS 7.18, 7.11, 7.11, 7.4, 1
Graffiti 6.75, 6.55, 6.50, 6.44, 6.19, 6.5
Grenze 12.4, 6.69, 6.65, 6.62, 6.59, 6.58, 6.57, 6.53, 6.50, 6.44, 6.8, 3.31
großflächige Anlagen des Personennahverkehrs 6.38
Grundbuchamt 6.47, 6.12
Grundrecht 12.11, 12.7, 12.4, 7.2, 6.67, 6.62, 6.55, 6.48, 6.34, 6.18, 6.16, 6.13, 6.3, 4.3, 1
Grundstück 10.4, 6.67, 6.66, 6.64, 6.63, 6.58, 6.57, 6.56, 6.54, 6.53, 6.52, 6.51, 6.50, 6.49, 6.48, 6.46, 6.44, 6.43, 6.36, 6.34, 6.33, 6.32, 6.30, 6.24, 6.23, 6.22, 6.21, 6.20, 6.18, 6.17, 6.16, 6.14, 6.12, 6.8
Grundstücksgrenze 6.64, 6.58, 6.54, 6.53, 6.51, 6.50, 6.48, 6.33, 6.31, 6.24, 6.23, 6.21, 6.16
Grundstücksnutzer 6.53
Hacker-Angriff 12.14, 12.13, 12.11, 12.2, 5.1, 3.35
Handelsregisterauszug 6.31
Haus 12.11, 6.75, 6.67, 6.64, 6.55, 6.48, 6.43, 6.33, 6.30, 6.28, 6.27, 6.26, 6.20, 6.19, 6.18, 6.14, 6.4, 3.35, 3.27, 2.7
Hauseingang 6.75, 6.52, 6.48, 6.43, 6.35, 6.27, 6.23, 6.22, 6.13
Hausgrundstück 6.51
Hausleitung 3.1
Hausrecht 7.17, 7.1, 6.76, 6.75, 6.74, 6.72, 6.71, 6.69, 6.67, 6.66, 6.65, 6.64, 6.61, 6.60, 6.58, 6.54, 6.53, 6.52, 6.50, 6.48, 6.44,

6.40, 6.38, 6.37, 6.36, 6.35, 6.34, 6.32, 6.31, 6.29, 6.24, 6.23, 6.21, 6.20, 6.18, 6.16, 6.11, 6.9, 6.8, 6.7, 6.4, 6.3
Hausrechtsinhaber 6.54, 6.53, 6.50, 6.48, 6.44, 6.33, 6.24, 6.23, 6.21, 6.16
Hausverwaltung 6.27, 3.45, 3.27
Hecke 6.49
Heimaufsicht 10.17
Hilfe 8.1, 7.12, 7.1, 6.57, 6.37, 6.1, 3.11, 2.5
Hinterbliebene 3.13
Hinweispflicht 6.62, 6.60, 6.36
Hinweisschild 7.3, 7.1, 6.60, 6.55, 6.52, 6.50, 6.46, 6.44, 6.36, 6.36, 6.23, 6.18, 6.13, 6.11, 6.8, 6.5
Hotel 6.32, 3.11, 3.8
Identitätsbetrug 3.46
Imbisslokal 6.74
Immelborn 3.1
Inbetriebnahme .. 10.17, 7.5, 6.66, 6.51, 6.39, 6.33, 6.28, 6.9, 6.2, 3.2
informationelle Selbstbestimmung 12.4, 7.22, 7.14, 6.72, 6.62, 6.55, 6.48, 6.34, 6.23, 6.23, 6.18, 6.11, 6.3, 3.17, 3.6, 3.6, 3.4, 1
informationelles Selbstbestimmungsrecht 12.7, 10.10, 6.75, 6.74, 6.69, 6.67, 6.64, 6.58, 6.40, 6.38, 6.13, 3.26
Infotainmentsysteme 12.4
Innenhof 6.66, 6.36, 6.31
Insolvenz 6.45, 6.12, 3.37, 3.26, 3.8
Insolvenzmasse 6.45, 6.12, 3.8
Insolvenzverwalter 6.45, 6.12, 3.26, 3.8
Interessen 10.1, 9.1, 7.22, 7.18, 7.17, 7.6, 7.5, 7.1, 6.75, 6.74, 6.72, 6.71, 6.70, 6.69, 6.67, 6.66, 6.65, 6.64, 6.62, 6.61, 6.60, 6.58, 6.58, 6.54, 6.53, 6.52, 6.50, 6.48, 6.44, 6.41, 6.40, 6.38, 6.37, 6.36, 6.35, 6.29, 6.28, 6.27, 6.24, 6.23, 6.21, 6.20, 6.18, 6.16, 6.15, 6.13, 6.11, 6.9, 6.8, 6.7, 6.6, 6.5, 6.4, 6.3, 5.1, 4.3, 3.45, 3.37, 3.31, 3.28, 3.4, 3.3, 2.5, 2.2
Interessenabwägung 12.7, 6.72, 6.58, 3.45, 3.37, 3.4
Interessenkollision 2.5, 2.3, 2.2
Interessenkonflikt 10.6, 7.5, 2.5, 2.3, 2.2
Internethandel 3.35
Intimsphäre 6.69, 6.40
IT-Mitarbeiter 2.2
IT-Sicherheitsbeauftragter 2.3, 2.2
IT-Sicherheitsgesetz 12.2

Jäger 6.70, 6.58, 6.2
Jobcenter 7.10, 3.20
journalistisch-redaktionelle Zwecke 4.3, 3.21
juristische Person 6.18, 6.2, 4.4, 4.1, 3.46, 3.13, 2.5, 2.4, 2.1
Justiz 3.1
Kamera 7.17, 7.5, 7.3, 7.1, 6.76, 6.75, 6.74, 6.72, 6.71, 6.70, 6.69, 6.68, 6.67, 6.66, 6.65, 6.64, 6.63, 6.62, 6.61, 6.60, 6.58, 6.57, 6.56, 6.55, 6.54, 6.53, 6.52, 6.51, 6.49, 6.48, 6.47, 6.46, 6.45, 6.44, 6.43, 6.42, 6.41, 6.40, 6.38, 6.36, 6.35, 6.34, 6.33, 6.32, 6.31, 6.30, 6.29, 6.28, 6.27, 6.26, 6.25, 6.24, 6.24, 6.23, 6.22, 6.21, 6.20, 6.19, 6.18, 6.17, 6.16, 6.15, 6.14, 6.13, 6.12, 6.11, 6.10, 6.9, 6.8, 6.7, 6.6, 6.5, 6.4, 6.3, 6.2
Kameraattrappe 6.67, 6.57, 6.56, 6.55, 6.54, 6.51, 6.48, 6.43, 6.42, 6.35, 6.34, 6.27, 6.22, 6.16
Kamerasystem 6.5
Kasse 7.16, 6.74, 6.9, 3.44, 3.3
Kinder 12.15, 10.16, 10.11, 7.14, 6.53, 6.21
Kindergarten 6.53
Kindertageseinrichtung 2.7
kirchliche Stellen 3.20
Klageschrift 3.4
Klageverfahren 3.4
Klausel 10.12, 7.9, 2.2
Kleider- und Wertspindschließfächer 6.40
Klingel 6.52, 6.36, 6.23, 6.15, 6.13
Klingelkamera 6.15
kommunales Wettbewerbsunternehmen 4.1
Konkurrenzunternehmen 7.8
Kontaktdaten ... 10.19, 7.10, 7.1, 6.60, 6.55, 6.36, 6.23, 6.18, 4.3, 3.9
Kontrolle 12.4, 10.18, 10.11, 10.4, 9.2, 7.22, 7.7, 7.5, 7.4, 6.72, 6.69, 6.68, 6.65, 6.64, 6.60, 6.59, 6.47, 6.36, 6.32, 6.27, 6.18, 6.8, 6.7, 3.44, 3.29, 3.20, 3.2, 2.5, 2.3
Kopie 3.22, 3.14, 3.14, 3.12, 3.12, 3.7
Korruptionsbekämpfung 4.1
Kosten 12.11, 12.4, 6.38, 6.25, 6.19, 3.13, 3.6
Krankenhaus 12.2, 10.13, 10.12, 10.9, 3.6
Krankenkasse 10.15, 3.20
Krankenversicherung 10.15
Kredit 9.1
Kreditkartendaten 3.35, 3.8

Kundendaten 10.9, 10.9, 10.3, 3.37, 3.36, 3.26, 3.16, 3.15, 3.10, 3.8, 3.8, 3.4
Kündigung 7.20, 7.19, 7.8
Ladeneingang 6.50
Lageplan 6.68, 6.54, 6.42, 6.27, 6.18, 6.8
Landesärztekammer Thüringen 10.22, 10.2
Lastschriftverfahren 9.2, 3.44, 3.40
Lehrernamen 3.24
Leistungs- und Verhaltenskontrolle 7.18, 7.16, 7.15, 7.12, 7.11, 7.4, 7.1
Leistungskontrolle 7.22, 1
Leserservice 3.9
Lichtbild 12.13, 6.51
Linse 6.49, 6.6
Liquidation 3.42
Liquidator 3.42
Listendaten 3.26
Live-Beobachtung 6.38
Logistikunternehmen 7.22
Löschen 12.7, 10.21, 10.18, 10.13, 10.13, 9.3, 7.7, 3.40, 3.9, 3.7
Löschung 12.6, 12.5, 10.21, 10.18, 10.5, 9.1, 9.1, 8.2, 7.21, 7.21, 7.10, 7.7, 7.6, 7.5, 7.3, 6.71, 6.50, 6.41, 3.42, 3.41, 3.39, 3.7, 3.3
Löschungsfrist 10.2, 6.50
Makler 3.37
Markt- und Meinungsforschung 3.2
Mediengruppe 3.9
Medienprivileg 4.3
Mehrfamilienhaus 6.75, 6.31, 6.27, 6.26, 6.13, 3.45, 3.27
Meinungsfreiheit 12.5, 7.2
Meldeadresse 3.42
Meldeformular 6.37, 6.9
Meldepflicht 12.9, 6.70, 6.39, 6.33, 6.28, 6.21, 6.2, 6.1, 5.1, 4.1, 3.2, 1
Melderegister 6.39
Melderegisterpflicht 3.2
Meldeunterlagen 6.39
Meldung nach § 4d Abs. 1 BDSG 7.5, 6.9
Messdaten 3.31
Microsoft 12.14, 12.1
Mieter ... 6.75, 6.48, 6.47, 6.35, 6.31, 6.27, 6.26, 6.13, 6.5, 3.45, 3.27

Mieterselbstauskunft 3.12
Mietvermittlung 3.12
milderes Mittel 6.76, 6.71, 6.69, 6.59, 6.40, 6.4
Mitarbeiter 14, 12.5, 10.21, 10.17, 10.15, 10.11, 10.7, 10.5, 10, 10.2, 10.1, 7.21, 7.20, 7.19, 7.18, 7.17, 7.16, 7.15, 7.13, 7.11, 7.8, 7.6, 7.5, 7.4, 7.3, 7.2, 7.1, 6.74, 6.71, 6.69, 6.65, 6.59, 6.44, 6.39, 6.32, 6.28, 6.10, 6.9, 6.8, 6.6, 5.1, 4.2, 4.1, 3.34, 3.25, 3.18, 3.10, 3.9, 3.8, 3.7, 3.6, 2.7, 2.3, 2.1, 1
Mitarbeiterschutz 6.9
Mitarbeiterüberwachung 7.11, 6.8
Mitgliederdaten 4.2, 3.25, 3.18, 3.18
Mitgliederzeitschrift 4.3
Mitgliedsantrag 4.2, 3.18
Mitgliedsbeitrag 3.25, 3.18
Mithören 10.11, 10.10
Mitteilungsblatt 4.3
Monitor 7.3, 7.1, 6.74, 6.64, 6.60, 6.23, 6.18, 6.17, 6.13
Monitoring 7.12, 6.74, 6.65, 6.59, 6.58, 6.41, 6.40, 6.38, 6.18, 6.3
Mülltonne 6.5
multiresistente Keime 10.1
Nachbargrundstück 6.58, 6.52, 6.49, 6.44, 6.43, 6.37, 6.31, 6.21
Nachbarn 6.64, 6.52, 6.49, 6.48, 6.44, 6.34, 6.33, 6.24, 6.23, 6.22, 6.21, 6.18, 6.16, 6.13
Nachbarparzelle 6.49
Nachbarschaft 6.21, 6.18, 6.14, 6.8, 6.7, 6.5
Nachweis 10.21, 10.4, 7.21, 6.69, 6.68, 6.62, 6.59, 6.53, 6.27, 6.20, 6.19, 6.18, 6.16, 6.7, 6.5, 3.14, 2.6
Namen 10.21, 10.17, 10.16, 10.9, 10.3, 8.1, 6.31, 6.30, 6.29, 6.14, 6.12, 4.3, 3.46, 3.45, 3.43, 3.42, 3.40, 3.32, 3.27, 3.25, 3.24, 3.23, 3.21, 3.17, 3.14, 3.12, 3.10, 3.8, 3.6, 3.3, 3.2
Namensnennung 3.10
nationales Recht 12.9, 2.1
Navigieren 3.33
Negativauskunft 9.3, 3.43
Netzwerkdurchsetzungsgesetz 12.5
Newsletter 3.40, 3.9
nicht-öffentlich zugänglicher Bereich 6.75, 6.64, 6.43, 6.41, 6.26
nicht-öffentlich zugänglicher Raum 7.17, 6.36, 6.28, 6.27, 6.18, 6.13
nicht-öffentliche Stellen 10.22, 10.10, 10.6, 10.5, 7.17, 7.12, 7.5, 6.70, 6.69, 6.65, 6.64, 6.59, 6.58, 6.39, 6.35, 6.26, 6.23, 6.21,

6.18, 6.11, 6.9, 6.4, 6.3, 5.1, 3.35, 3.34, 3.29, 3.23, 3.18, 3.13, 3.12, 2.7, 2.4, 2.1
NIS-Richtlinie 12.9
Notstand 10.1
Nutzungsrecht 6.53
Obergeschoss 6.50
Objekt..... 6.66, 6.54, 6.50, 6.47, 6.44, 6.36, 6.19, 6.8, 6.5, 2.7
Objektüberwachung 6.5
öffentlich zugängliche großflächigen Anlagen 6.61, 6.38
öffentlich zugänglicher Bereich 6.71, 6.69, 6.67, 6.65, 6.64, 6.59, 6.54, 6.51, 6.50, 6.48, 6.43, 6.41, 6.33, 6.21, 6.20, 6.17, 6.16, 6.15, 6.13, 6.11, 6.3, 2.6
öffentlich zugänglicher Raum 7.17, 7.1, 6.76, 6.75, 6.74, 6.72, 6.71, 6.70, 6.69, 6.64, 6.61, 6.60, 6.59, 6.58, 6.55, 6.54, 6.53, 6.52, 6.50, 6.48, 6.43, 6.37, 6.36, 6.35, 6.34, 6.33, 6.31, 6.29, 6.27, 6.26, 6.24, 6.23, 6.22, 6.21, 6.20, 6, 6.16, 6.13, 6.11, 6.8, 6.7, 6.6, 6.5, 6.4, 6.3
öffentlich zugängliches Waldgebiet 6.70
öffentliche Stellen 10.5, 6.61, 6.57, 4.4, 4.1, 2.1
öffentliche Verkehrsmittel 6.72
öffentlicher Platz 6.6
öffentlicher Raum 6.61, 6.48, 6, 6.7, 3.34
öffentlicher Verkehrsraum 6.64, 6.44, 6.21, 6.17
Öffnungsklauseln 2.1
Onboard-Kamera 6.62
Onlinekauf 9.2
Onlineshop 3.35
Onlineunternehmen 9.2
Ordnungswidrigkeit 11.1, 6.63, 6.62, 6.32, 6.30, 5.1, 3.42, 3.31, 3.7, 1
Ordnungswidrigkeitenverfahren 11.1, 6.62, 6.30, 2.2
Orientierungshilfe 10.13, 7.17, 7.12, 6.72, 6.65, 6.59, 6.41, 6.40, 6.37, 6.35, 6.26, 6.21, 6.9, 6.4, 6.3, 3.11
Orientierungshilfe Videoüberwachung 6.27
Pächter 6.49, 6.29, 3.8
Parkkralle 3.6
Parzelle 6.49
Passwort 12.13, 12.11, 10.5, 7.13, 2.7
passwortgeschützter Bereich 3.24

Patient 10.22, 10.15, 10.14, 10.11, 10.10, 10.9, 10.8, 10.7, 10.6, 10.4, 10.3, 10.2, 10.1, 3.26, 1
Patientenakte 351, 10.18, 10.11, 10.10, 10.7, 10.6, 3.26
Patientendaten 10.14, 10.11, 10.9, 10.6, 10.5, 10.4, 3.26
Patientenfoto 10.8
Personal 10.1, 7.1, 6.74, 6.71, 6.59, 6.38, 6.3, 3.10, 2.2
Personalausweis 12.13, 3.32, 3.22, 3.14, 3.12, 3.6
Personalausweisgesetz 12.13, 3.14, 3.12
Personalausweisregister 12.13
Personalausweisvorlage 3.22
Personaldienstleister 7.19, 7.8
personalisierte Werbung 12.12
personenbezogene Date 10.16
personenbezogene Daten 14, 12.10, 12.9, 12.7, 12.4, 12.3, 11.1, 10.22, 10.21, 10.20, 10.19, 10.18, 10.17, 10.15, 10.13, 10.12, 10.11, 10.10, 10.9, 10.8, 10.7, 10.5, 10.3, 10.1, 9.1, 8.2, 7.22, 7.21, 7.20, 7.18, 7.16, 7.15, 7.13, 7.10, 7.10, 7.8, 7.7, 7.6, 7.5, 7.4, 7.2, 7.1, 6.75, 6.72, 6.71, 6.69, 6.64, 6.59, 6.58, 6.56, 6.53, 6.52, 6.46, 6.45, 6.44, 6.43, 6.41, 6.39, 6.38, 6.37, 6.36, 6.34, 6.33, 6.32, 6.27, 6.26, 6.25, 6.23, 6.21, 6.20, 6.18, 6.16, 6.15, 6.14, 6.13, 6.12, 6.11, 6.8, 6.7, 6.6, 6.4, 6.2, 5.1, 4.5, 4.4, 4.3, 4.2, 4.1, 3.47, 3.46, 3.45, 3.44, 3.41, 3.39, 3.38, 3.37, 3.36, 3, 3.32, 3.31, 3.30, 3.29, 3.28, 3.27, 3.26, 3.21, 3.20, 3.19, 3.18, 3.17, 3.16, 3.15, 3.14, 3.13, 3.11, 3.10, 3.9, 3.8, 3.7, 3.6, 3.5, 3.4, 3.3, 3.2, 2.7, 2.6, 2.5, 2.3, 2.2, 2.1, 1
Personengesellschaft 3.28, 2.5, 2.4
persönliche Daten 12.4, 10.16, 10.12, 6.48, 6.13, 3.45, 3.19, 3.6, 3.5, 2.2
Persönlichkeitsrecht 7.7, 7.1, 6.74, 6.71, 6.68, 6.66, 6.62, 6.56, 6.51, 6.48, 6.46, 6.34, 6.31, 6.23, 6.22, 6.20, 6.19, 6.18, 6.14, 6.13, 6.12, 3.46, 3.27, 2.6
Pflegedienst 10.5
Piktogramm 7.1, 6.60, 6.36, 6.8
Pkw 6.75, 6.72, 6.62, 6.36, 6.4, 3.12
Polizei 12.14, 12.13, 10.3, 6.62, 6.59, 6.46, 6.44, 6.30, 6.19, 6.5, 3.34, 3.2, 3.1
Positionsbestimmung 3.33
Postdienstunternehmen 3.20
Postgesetz 3.48
Postzustellung 4.4

Pranger 7.2
Presse 4.3, 3.34, 3.33, 3.21
Pressefreiheit 4.3, 3.21
Privacy Shield 12.6, 10.12
privater Hauseigentümer 6.37
Privatgrundstück 6.64, 6.33, 6.18, 6.17
Privatinsolvenz 9.1
Privatsphäre 12.4, 12.3, 10.1, 6.65, 6.23, 6.14, 6.13, 3.45
Privatweg 6.53
Probeabonnement 3.9
Produkte zur Pooldesinfektion 3.14
Pseudonym 3.27
Psychotherapeut 10.6
qualifizierte elektronische Signatur 3.38
Rabattcoupons 7.16
rechtliche Grundlage 3.45, 3.30, 3.9
Rechtsanwalt 10.6, 6.36, 6.30, 6.12, 3.23, 3.4, 2.4
Rechtsanwalts-Partnerschaft 2.4
Rechtsprechung 6.62, 6.58, 6.50, 6.48, 6.44, 6.21, 3.32, 1
Rechtsverstöße 6.54, 6.50, 6.44, 3.31
Register 6.32, 6.28
Registermeldung 6.32
Reihenhaussiedlung 6.14
rein redaktionelle oder journalistische Tätigkeit 3.21
Religionsausübung 3.48
Religionsgesellschaft 3.48
Reparaturen 6.5
Restaurant 7.1, 6.41, 6.6
Restschuldbefreiung 9.1
Rezept 10.19, 10.9, 10, 10.3
Router 12.11
Rückabwicklung 3.16
Rundfunk 3.20
Sachbeschädigung 6.75, 6.72, 6.59, 6.54, 6.50, 6.44, 6.27, 6.5, 6.3
Sachbeschädigungsdelikt 6.5
Sauna 6.69, 6.40, 6.37, 3.14
Schadenersatz 6.4, 3.4
Schaufenster 6.50, 6.23, 6.5, 3.33
Schornsteinfeger 3.36
Schredder 10.21, 10.13, 3.39, 3.29

Schriftform 10.7, 7.21, 7.19, 6.71, 6.2, 3.38, 3.37, 3.28, 2.5
Schufa 9.1, 3.20
Schule 12.1, 3.24
Schulhomepage 3.24
Schutz 12.9, 12.7, 12.3, 10.18, 10.12, 10.11, 10.8, 10.1, 7.17, 7.4, 6.74, 6.71, 6.66, 6.54, 6.54, 6.53, 6.50, 6.48, 6.44, 6.35, 6.34, 6.32, 6.21, 6.13, 6.10, 6.6, 4.1, 3.27, 2.6, 1
Schutz der Patienten 10.8, 10.7
Schutz von Leben 6.72, 6.61, 6.38
Schutzmaßnahme 10.1, 7.3
schutzwürdige Interesse 6.65
schutzwürdige Interessen 10.3, 7.16, 7.5, 7.1, 6.75, 6.74, 6.74, 6.72, 6.71, 6.70, 6.69, 6.66, 6.64, 6.62, 6.60, 6.58, 6.53, 6.50, 6.44, 6.41, 6.40, 6.38, 6.37, 6.36, 6.35, 6.29, 6.28, 6, 6.26, 6.23, 6.20, 6.18, 6.13, 6.11, 6.9, 6.8, 6.6, 6.4, 6.3, 4.3, 4.1, 3.45, 3.37, 3.31, 3.28, 3.26, 3.19, 3.15, 3.14, 3.8, 3.4, 3.3
Schwärzen 6.71, 6.53
schwarzes Brett 3.25
Schweigepflicht 10.16, 10.14, 10.7, 10.6, 10.2, 7.9
Schweigepflichtentbindung 10.14, 10.1, 7.9
Schwimmbäder 6.40, 6.37, 6.32, 3.14
Screenshot 6.72, 6.68, 6.50, 6.8, 3.6
Selbstbedienungsladen 6.3
Seminararbeit 3.17
Seniorenheim 10.17
Server 12.15, 12.11, 10.19, 10.5, 6.50, 6.1
Sicherheitsstufe 10.21, 10.18, 10.13, 3.47, 3.39, 3.34, 3.29
Sicherheitstechnik 6.10
Sicherheits-Updates 12.14
Sichtbereich 6.49
Signaturgesetz 12.8, 3.38
Signaturverordnung 12.8
Skimming 3.35
smarte Lautsprecher 12.15
Smart-Home 6.10
Smartphone 12.15, 12.11, 12.4, 10.22, 10.5, 3.33, 3.24
Software 12.14, 12.12, 12.11, 12.10, 10.5, 6.51, 4.5, 3.35, 3.5, 2.7
Sorgerecht 10.16
soziale Netzwerke 14, 13.1, 12.5, 12.5, 12.4, 7.2
Spaziergänger 6.70, 6.25, 6.23, 6.11

Speicherdauer 7.5, 7.4, 6.36, 6.32, 6.8, 6.3
Speicherfrist 9.1, 6.71, 6.41, 6.36
Speicherkarte 6.66
Speicherung 12.13, 12.7, 10.21, 10.18, 10.13, 10.9, 10.7, 10.3, 9.3, 9.1, 8.2, 7.10, 7.6, 7.5, 6.72, 6.71, 6.64, 6.52, 6.50, 6.48, 6.41, 6.40, 6.34, 6.23, 6.18, 6.15, 6.13, 6.13, 6.8, 6.5, 6.4, 6.3, 4.2, 3.47, 3.44, 3.43, 3.34, 3.32, 3.14, 3.13, 3.12, 3.10, 3.9, 3.7, 3.2, 2.7
Sperrung 12.5, 10.18, 7.10, 7.6
Spielhalle 6.71
Spielplatz 6.53
Spielzeug 12.15
Spindbereich 6.69, 6.40
Sportplatz 6.11
Sportverein 6.11, 4.2
Standardvertragsklauseln 10.12, 3.30
Stellplatz 6.4, 3.12
Steuerkanzlei 3.47
Steuerrecht 7.6, 3.32
Strafanzeige 10.6, 7.2, 6.75
Straftat 11.1, 10.3, 7.22, 7.16, 6.71, 6.69, 6.66, 6.40, 6.29, 6.27, 6.5, 6.4, 4.1, 3.34, 3.31, 3.22, 2.6
Strafverfolgung 12.5, 10.6, 10.3, 6.72, 6.71, 6.66, 6.38, 5.1
Straße 6.76, 6.75, 6.67, 6.62, 6.61, 6.53, 6.50, 6.48, 6.37, 6.34, 6.33, 6.30, 6.24, 6.23, 6.21, 6.20, 6.18, 6.16, 6.15, 6.8, 6.5, 6.4, 3.45, 3.32
Stundenabrechnungen 7.6
Tankstelle 6.9
Täter 11.1, 6.67, 6.62, 6.48, 6.20, 2.7
Tätigkeit 10.17, 10.4, 10.2, 7.22, 7.14, 7.3, 6.69, 6.66, 6.58, 6.57, 6.56, 6.54, 6.53, 6.52, 6.41, 6.37, 6.36, 6.30, 6.18, 6.16, 6.7, 5.1, 4.3, 3.48, 3.36, 3.34, 3.30, 3.21, 3.17, 3.16, 3.15, 2.7, 2.5, 2.3, 2.2, 2.1
tatsächliche Anhaltspunkte 7.16, 5.1, 4.1
technisch-organisatorische Maßnahmen 12.14, 10.19, 10.18, 10.13, 10.10, 10.5, 9.3, 7.13, 6.41, 6.7, 4.5, 4.2, 3.41, 3.39, 3.38, 3.34, 3.29, 2.7
technisch-organistorische Maßnahmen 3.21
Telefonwerbung 8.1, 3.9
Telekommunikation 12.10, 12.2, 6.10, 3.20

Telekommunikationsgesetz 12.15, 12.9, 8.1
Telemediengesetz 12.9, 12.7
Theater 3.3
Therme 6.69
Thüringer Gesetz über betreute Wohnformen und Teilhabe 10.17
Thüringer Innenministerium 3.1
Thüringer Landesverwaltungsamt 10.22
Tonaufnahmen 6.32, 6.9
Tourenpläne 7.6
Tracking 12.12, 12.3
Türklingel 6.13
Türspion 6.13
Übermittlung 10.22, 10.19, 10.14, 10.11, 10.10, 10.3, 10.1, 6.5, 4.4, 4.3, 3.45, 3.41, 3.37, 3.35, 3.31, 3.30, 3.28, 3.26, 3.25, 3.18, 3.17, 3.4, 2.7, 2.1
Überwachung 7.11, 7.5, 7.3, 7.2, 7.1, 6.75, 6.74, 6.72, 6.71, 6.69, 6.66, 6.64, 6.62, 6.61, 6.60, 6.59, 6.58, 6.55, 6.54, 6.52, 6.50, 6.48, 6.44, 6.40, 6.37, 6.36, 6.29, 6.28, 6.27, 6.26, 6.23, 6.21, 6.18, 6.15, 6.13, 6.10, 6.9, 6.8, 6.5, 6.1, 3.22, 2.6
Überwachungsdruck 6.67, 6.56, 6.55, 6.48, 6.46, 6.34, 6.28, 6.20, 6.16, 6.13
Umfrage 10.20, 6.40, 3.30, 3.28, 3.2
Umgang mit personenbezogenen Daten 3.41
Umkleidekabine 6.69, 6.40
Umtausch 3.10
unbefugtes Mitlesen 10.11
Unfallbeteiligte 6.62
Unfalldatenspeicher 6.62
Unternehmen 14, 13.2, 12.14, 12.13, 12.11, 12.9, 12.3, 10.21, 10.18, 10.12, 10.5, 10.3, 10.2, 9.3, 9.2, 8.2, 7.22, 7.21, 7.20, 7.19, 7.18, 7.17, 7.16, 7.15, 7.14, 7.12, 7.10, 7.9, 7.8, 7.7, 7.4, 7.2, 7.1, 6.72, 6.69, 6.65, 6.59, 6.47, 6.39, 6.38, 6.32, 6.28, 6.8, 6.3, 5.1, 4.5, 4.4, 4.3, 4.1, 3.47, 3.46, 3.44, 3.43, 3.42, 3.41, 3.37, 3.36, 3.35, 3.34, 3.32, 3.30, 3.26, 3.23, 3.21, 3.20, 3.19, 3.17, 3.15, 3.14, 3.13, 3.12, 3.11, 3.10, 3.8, 3.7, 3.6, 3.5, 3.4, 3.2, 2.6, 2.5, 2.3, 2.2, 2.1, 1
Unternehmensdaten 3.46
Unternehmenskauf 3.26
Unternehmensverkauf 3.26
Unterschriften-Pad 3.38

Unterschriftensammlung 3.28
Untersuchung 12.9, 10.16, 10.14, 10.2, 7.9
Untersuchungsausschuss 3.1
unzulässige Datenerhebung 3.15
Unzuständigkeit 3.21, 3.20
Urkunde 10.22, 6.57, 2.5
Urkundenverifikation 10.22
USA 12.11, 10.19, 3.30
Vandalismus 7.17, 6.69, 6.67, 6.54, 6.53, 6.50, 6.48, 6.44, 6.27, 6.21, 6.20, 6.16, 6.13, 6.8, 6.7, 6.6, 6.5
Veranstalter 3.3
verantwortliche Stelle 12.14, 11.1, 10.13, 10.11, 10.10, 10.5, 10.4, 9.3, 8.2, 7.13, 7.10, 7.8, 7.7, 7.6, 7.1, 6.76, 6.75, 6.72, 6.71, 6.70, 6.69, 6.65, 6.60, 6.57, 6.55, 6.47, 6.46, 6.45, 6.41, 6.39, 6.36, 6.27, 6.26, 6.23, 6.20, 6.18, 6.17, 6.11, 6.9, 6.8, 6.7, 6.4, 6.3, 6.2, 5.1, 4.3, 4.2, 3.45, 3.43, 3.42, 3.41, 3.40, 3.39, 3.38, 3.37, 3.34, 3.29, 3.28, 3.20, 3.19, 3.18, 3.15, 3.14, 3.13, 3.11, 3.8, 3.7, 3.4, 2.5, 2.4, 2.3, 2.2
Verarbeitung 13.2, 12.7, 12.4, 12.3, 10.21, 10.18, 10.17, 10.14, 10.11, 10.10, 10.9, 10.8, 10.7, 10.3, 10.1, 9.2, 9.1, 7.22, 7.18, 7.17, 7.16, 7.5, 7.4, 6.75, 6.72, 6.71, 6.69, 6.64, 6.52, 6.46, 6.41, 6.39, 6.36, 6.28, 6.27, 6.26, 6.23, 6.20, 6.18, 6.16, 6.12, 6.8, 6.7, 6.6, 6.4, 4.3, 4.2, 4.1, 3.47, 3.45, 3.44, 3.41, 3.40, 3.39, 3.38, 3.36, 3.34, 3.32, 3.31, 3.30, 3.28, 3.26, 3.25, 3.22, 3.20, 3.19, 3.18, 3.17, 3.16, 3.15, 3.14, 3.10, 3.8, 3.5, 3.4, 3.2, 2.7, 2.6, 2.5, 2.4, 2.3, 2.2, 2.1
Verband 4.3, 3.18
Verbreiten 7.14, 6.62
Verein 6.11, 4.3, 4.2, 3.41, 3.40, 3.40, 3.39, 3.28, 3.25, 3.25, 3.18, 3.18
Verfahrensregister 6.2
Verfassungsschutz 12.13
Verfolgung 11.1, 10.3, 6.62, 6.30, 6.6, 3.44, 3.31, 3.21, 3.18, 3.4
Verfolgungsbehörde 6.62
Verkehrsgeschehen 6.62
Verkehrsraum 6.64, 6.62, 6.48, 6.18, 6.17, 6.15, 6.13
Verkehrsunfall 10.3, 6.62
Verletzung 10.16, 10.6, 6.51, 6.46, 6.16, 6.6, 3.34, 3.21
Verletzungsgefahr 7.12
Vermieter 10.10, 6.47, 6.35, 6.31, 6.27, 6.26, 6.13, 3.45, 3.12

vernetztes Fahren 12.4
Veröffentlichung 10.12, 9.1, 7.21, 7.14, 7.2, 5.1, 4.3, 3.40, 3.25, 3.24, 3.21, 3.17
Verschlüsselung 10.22, 10.19, 10.5, 2.7
Versichertendaten 10.15
Versicherung 10.6, 7.16, 7.3, 6.5, 3.37, 3.15
Versicherungsmakler 3.37, 3.37, 3.16
Verstorbene 10.4, 3.13
Vertrag 12.6, 10.18, 10.5, 7.22, 7.9, 7.8, 6.27, 3.47, 3.40, 3.39, 3.38, 3.37, 3.34, 3.16, 3.5
Vertrauensdienstegesetz 12.8
Vertretungsplan 3.24
Verwertbarkeit 6.62
Verwertung 6.72, 6.62
Video 12.5, 12.4, 6.68, 6.62, 6.52, 6.50, 6.32
Videobeobachtung 7.1, 6.64, 6.23, 6.13, 6.7
Videokamera 7.5, 7.3, 7.1, 6.76, 6.75, 6.74, 6.72, 6.71, 6.67, 6.64, 6.62, 6.60, 6.58, 6.57, 6.55, 6.53, 6.52, 6.50, 6.48, 6.46, 6.45, 6.44, 6.41, 6.40, 6.36, 6.31, 6.30, 6.28, 6.24, 6.23, 6.22, 6.21, 6.20, 6.19, 6.16, 6.15, 6.14, 6.11, 6.10, 6.7, 6.6, 6.4, 1
Videoüberwachung 14, 7.17, 7.12, 7.5, 7.3, 7.1, 6.76, 6.75, 6.74, 6.72, 6.71, 6.69, 6.66, 6.65, 6.64, 6.62, 6.61, 6.60, 6.59, 6.58, 6.57, 6.56, 6.55, 6.54, 6.53, 6.52, 6.50, 6.48, 6.47, 6.46, 6.45, 6.44, 6.42, 6.41, 6.39, 6.38, 6.37, 6.36, 6.35, 6.34, 6.33, 6.32, 6.31, 6.30, 6.29, 6.28, 6.28, 6.27, 6.26, 6.24, 6.23, 6.22, 6.21, 6.20, 6.18, 6.17, 6.16, 6.15, 6.14, 6.13, 6.12, 6.11, 6.10, 6.10, 6.9, 6.8, 6.7, 6.6, 6.5, 6.4, 6.3, 6.2, 6.1
Videoüberwachung im Schwimmbad/Erlebnisbad 6.40
Videoüberwachungsanlage 7.3, 6.76, 6.71, 6.69, 6.68, 6.67, 6.65, 6.63, 6.60, 6.59, 6.53, 6.52, 6.51, 6.50, 6.49, 6.48, 6.45, 6.44, 6.43, 6.42, 6.41, 6.40, 6.38, 6.37, 6.36, 6.33, 6.31, 6.30, 6.29, 6.28, 6.27, 6.24, 6.23, 6.21, 6.20, 6.16, 6.13, 6.7, 6.6, 6.5, 6.4, 6.3, 6.2, 6.1
Videoüberwachungsverbesserungsgesetz 6.72, 6.38
Vogelhaus 6.23
VoIP 12.10, 12.3
Volkszählungsgesetz 6.48
Vorabkontrolle 7.12, 7.5, 6.9, 6.3
Vorgesetzter 7.18, 7.15, 7.13, 7.8, 6.28, 4.1, 3.6

Vorkommnis 6.76, 6.75, 6.72, 6.65, 6.59, 6.53, 6.50, 6.48, 6.33, 6.32, 6.27, 6.20, 6.16, 6.4, 6.3
Vor-Ort-Kontrolle 10.11, 10.4, 7.3, 6.43, 6.32, 6.12, 6.6, 3.47, 3.44, 3.2
Wahrnehmung 7.17, 7.1, 6.76, 6.75, 6.74, 6.72, 6.71, 6.70, 6.69, 6.67, 6.66, 6.65, 6.64, 6.61, 6.60, 6.58, 6.57, 6.54, 6.53, 6.50, 6.48, 6.44, 6.40, 6.37, 6.36, 6.35, 6.34, 6.31, 6.29, 6.24, 6.23, 6.20, 6.18, 6.13, 6.11, 6.9, 6.8, 6.7, 6.6, 6.5, 6.4, 6.3, 3.4, 2.5, 2.3
Wahrung berechtigter Interessen 7.5, 7.4, 6.75, 6.64, 6.44, 6.36, 6.28, 6.26, 6.11, 6.4, 4.3, 3.45, 3.31, 3.28, 3.19, 3.15, 3.14, 3.4
Waldrand 6.63
Wanderweg 6.25
WannaCry 12.14
Wanzen 3.35
Warnschild 6.62
Wartebereich 10.11, 10.10, 6.8, 6.4
Wearables 10.20
Weg 12.12, 10.3, 7.22, 6.63, 6.63, 6.53, 6.53, 6.19, 6.11, 6.8, 6.8, 3.37, 3.18, 1
Wegerecht 6.53
Weihnachtsmann 3.48
Weihnachtspostamt 3.48
Weitergabe 12.4, 10.17, 10.16, 10.1, 7.19, 7.10, 6.48, 6.13, 3.45, 3.37, 3.31, 3.26, 3.8
Werbeemails 8.2
Werbung 12.12, 8.2, 3.40, 3.36, 3.26, 3.15, 3.9
Werkstätte 12.4, 7.14
WhatsApp 10.19
Widerruf 10.9, 3.16, 2.5
Widerspruch 12.6, 10.2, 3.37, 3.9, 3.8, 2.3, 2.2
Wildkamera 6.70, 6.58, 6.27, 6.2
Wildtierkamera 6.70, 6.2
Windows 10 ..... 12.1
Windows 8 ..... 12.14
Windows Server 2003 ..... 12.14
Windows XP 12.14
Windschutzscheibe 6.62
Wohnungstür 6.13
Zahlartensteuerung 3.19
Zahlmethode 3.19

Zahnarzt 10.15, 10.11
Zahnarztpraxis 10.15, 10.10
Zaun 6.49, 6.21, 2.7
Zeitung 4.3, 3.21, 3.9
Zentrale 7.16, 2.6
Zeugnisverweigerungsrecht 10.3, 6.30
zivilrechtliche Ansprüche 6.46
Zoomfunktion 6.50, 6.28, 6.23
Zugangskontrolle 7.13, 6.41, 2.7
Zugriffskontrolle 7.13, 3.34, 2.7
Zulassungskopie 3.6
zuständige Aufsichtsbehörde 12.6, 7.3, 6.68, 6.42, 6.37, 6.27, 6.20, 6.18, 6.14, 6.12, 6.2, 5.1, 4.3, 3.35, 3.21, 3.18
Zuständigkeit 12.4, 11.1, 10.16, 10.15, 9.1, 7.16, 7.10, 6.68, 6.47, 6.23, 6.3, 3.48, 3.33, 3.23, 3.21, 3.20
Zuverlässigkeit 13.2, 7.5, 2.5, 2.4, 2.3, 2.2
Zuwegung 6.53
Zwangsgeld 6.42, 6.17
Zweckbestimmung 6.62, 4.3, 3.40, 3.18
Zwecke 13.1, 12.7, 12.4, 10.21, 10.20, 10.18, 10.17, 10.16, 10.14, 10.13, 10.9, 10.8, 10.6, 10.3, 10.2, 9.3, 8.2, 7.22, 7.21, 7.20, 7.18, 7.17, 7.15, 7.11, 7.10, 7.8, 7.7, 7.6, 7.5, 7.4, 7.1, 6.76, 6.75, 6.74, 6.72, 6.71, 6.70, 6.69, 6.67, 6.66, 6.65, 6.64, 6.61, 6.60, 6.58, 6.56, 6.54, 6.53, 6.50, 6.48, 6.44, 6.43, 6.41, 6.40, 6.39, 6.38, 6.37, 6.36, 6.36, 6.35, 6.34, 6.33, 6.32, 6.32, 6.31, 6.30, 6.29, 6.28, 6.27, 6.25, 6.24, 6.23, 6.20, 6.18, 6.17, 6.16, 6.13, 6.11, 6.9, 6.8, 6.7, 6.6, 6.5, 6.4, 6.3, 4.3, 4.1, 3.47, 3.46, 3.45, 3.43, 3.40, 3.38, 3.37, 3.31, 3.28, 3.26, 3.22, 3.21, 3.18, 3.15, 3.14, 3.13, 3.7, 3.6, 3.4, 3.3, 3.2, 2.6, 2.1, 1
zweckfremde Übermittlung 3.31

Vorbemerkungen zum Sprachgebrauch

Die verallgemeinernden Personenbezeichnungen in diesem Bericht gelten aus Gründen der Lesefreundlichkeit der Texte jeweils in der männlichen und weiblichen Form.

Impressum

Herausgeber: Thüringer Landesbeauftragter für den Datenschutz und die Informationsfreiheit (TLfDI)
Häßlerstraße 8, 99096 Erfurt
Postfach 900455, 99107 Erfurt
Telefon: 0361/57 3112900, Telefax: 0361/57 3112904
E-Mail: poststelle@datenschutz.thueringen.de
Internet: www.tlfdi.de

Druck: ReproPartner GbR
Liebknechtstr. 18
99085 Erfurt
Telefon: 0361/7891270
E-Mail: info@repropartner.de

Cover und Layout: Druckhaus Gera GmbH
Jacob-A-Morand-Straße 16, 07552 Gera
Telefon: 0365/737520
E-Mail: info@druckhaus-gera.de

Redaktionsschluss: 31. Januar 2018

Bildnachweis: TLfDI