Thüringer Landesbeauftragter
für den **Datenschutz** und die **Informationsfreiheit**



2021

4. Tätigkeitsbericht zum Datenschutz nach der DS-GVO

4. Tätigkeitsbericht zum Datenschutz nach der DS-GVO | 2021

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) Postfach 90 04 55, 99107 Erfurt Telefon: +49 (361) 57-3112900 E-Mail: poststelle@datenschutz.thueringen.de Internet: https://www.tlfdi.de
Druck:	THÜRINGER LANDESAMT FÜR BODENMANAGEMENT UND GEOINFORMATION (TLBG)
Layout Umschlag:	Druckerei Wittnebert, Erfurt Inh. Ulrich Janzen e. K. Internet: www.wittnebert.de
Endverarbeitung:	TLBG
Bildernachweis:	TLfDI. Siehe bitte auch Bilduntertitel im Text.
Redaktionsschluss:	Oktober 2022

4. Tätigkeitsbericht zum Datenschutz nach der DS-GVO

des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit

Berichtszeitraum: 1. Januar 2021 bis 31. Dezember 2021
Zitiervorschlag: 4. TB DS-GVO LfDI Thüringen

Der 4. Tätigkeitsbericht DS-GVO steht im Internet unter der Adresse www.tlfdi.de zum Abruf bereit.

Erfurt, im Oktober 2022

Dr. Lutz Hasse

Thüringer Landesbeauftragter für den Datenschutz
und die Informationsfreiheit

Inhaltsverzeichnis

Inhaltsverzeichnis **2**

Vorwort 8

1. Themengebiete 10

1.1 Schwerpunkte im Berichtszeitraum einschließlich Statistik 10

1.2 Meldungen über Verletzungen des Schutzes personenbezogener Daten nach Art. 33 DS-GVO 12

1.3 JI-Richtlinie reloaded? – Die Evaluation der Richtlinie (EU) 2016/680 und ihre Bedeutung 14

1.4 Sormas oder wie ein staatlich bundesweit gefördertes Projekt seinen wahren Auftrag sucht… 16

1.5 Rundschreiben des TLfDI an die Schulen und ViKos mit Schulleitungen 20

1.6 Mund-Nasen-Bedeckung in der Schule 22

1.7 AG KMK und Datenschützer zu Microsoft 365 26

1.8 Homeoffice in Pandemiezeiten 28

1.9 Maklertätigkeit und Auftragsverarbeitung – geht das zusammen? 30

1.10 Auswirkungen der Corona-Pandemie auf die Verarbeitung von Beschäftigtendaten 32

1.11 Bußgeldverfahren beim TLfDI 36

1.12 Kein Spaß mit der versteckten Kamera: Videoüberwachung im öffentlichen Bereich 49

1.13 Stand zu Office 365/ Microsoft 365 (neuer Name für das gleiche Produkt) 58

1.14 Sicherheit bei Funkanlagen 60

1.15 Das besondere elektronische Bürger- und Organisationenpostfach (eBO) 62

1.16 Automatisierte Abrufe des Lichtbilds und der Unterschrift aus den Pass- oder Personalausweisregistern 63
1.17 Notruf-App „nora“ 65
1.18 Orientierungshilfe zu Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail 67
1.19 SDM-Baustein „Nr. 41: Planen und Spezifizieren“ 69
1.20 SDM-Baustein „Nr. 51: Zugriff auf Daten, Systeme und Prozesse regeln“ 71
1.21 Künstliche Intelligenz muss dem Menschen dienen 72
1.22 Sicherheitslücke bei Microsoft-Exchange-Server 74
1.23 Roboter für Gangtraining 77

2. Fälle öffentlicher Bereich 80
2.1 Der Angemessenheitsbeschluss vom 28.06.2021 für GB als Folge des Brexit 80
2.2 „The Never Ending Story“ – Der „Jungbrunnen“ für Prüffristen bei der Thüringer Polizei 84
2.3 Auskunftsverlangen der Thüringer Polizei – am Ende unrechtmäßig 86
2.4 Ihr Auskunftsrecht beim Amt für Verfassungsschutz – ABER richtig! 89
2.5 Darf der Rechnungshof denn alles wissen? 91
2.6 Einmal Gerichtspost für ALLE? 93
2.7 Ein Jäger bläst zu laut zum Halali 95
2.8 Die neuen Fangbücher beim Fischen – am Ende datenschutzkonform 98
2.9 Vom Fischer und seiner Ausführungsverordnung: Angaben in Fangkarten datenschutzrechtlich zulässig 101
2.10 Formulare bei der Erlegung von Schwarzwild – Ein Fall für den TLfDI 103

2.11 Ein unbeugsames Dorf – unterfällt auch dem ThürDSG...106
2.12 Feuerwehrleute im Interesse eines Zweckverbandes 109
2.13 Unterschriftenlisten aus Einwohneranträgen – was dürfen Gemeinderäte sehen? 112
2.14 Videoüberwachung im Kindergarten 115
2.15 Thüringer Gesetz zur Förderung der Teilnahme an durchzuführenden Früherkennungsuntersuchungen für Kinder 117
2.16 Datenschutz bei der Vorlage von Kontoauszügen beim Jobcenter 118
2.17 Umgang mit Sozialhilfeakten – Verantwortlich aufbewahren – gilt auch für „geerbte“ Altakten 120
2.18 Ärger ums „Azubi-Ticket Thüringen“ 122
2.19 Abfrage des 3G-Status zum Elternabend 124
2.20 Beschwerde über Corona-Testpflicht in der Schule.....126
2.21 Abfrage nach Corona-Test-Ergebnis bei Mitschülern und Eltern.....128
2.22 Beschwerde über einen Schulleiter wegen Weiterleitung einer Mail.....130
2.23 Maske vergessen? Schulsekretariat darf Schüler bei der Ausgabe von Ersatzmasken nicht erfassen.....132
2.24 „Setzen, Sechs!“ hat ausgedient – Schulnoten dürfen vor der Klasse nicht verkündet werden. 134
2.25 Elternvertreter: Finger weg von WhatsApp!.....136
2.26 Abfrage bei Präsenzveranstaltung an Hochschulen – was darf der Sicherheitsdienst? 139
2.27 Einem Datenschutzverstoß kann nur bei einem Nachweis nachgegangen werden.....141
2.28 Anzeige eines Datenschutzverstoßes führt nicht immer zum Betriebsfrieden.....143
2.29 Wo der Datenschutz endet: Zulässigkeit eines digitalen Suchsystems für Grabstätten.....145

2.30 Was darf der Fragebogen zum Kauf von Wohnungseigentum erheben? 147

3. Fälle nicht-öffentlicher Bereich 152

3.1 Steckbriefe der Ungeimpften im Unternehmen im Internet 152

3.2 Können Datenschutzgründe der Annahme einer Initiativbewerbung entgegenstehen? 157

3.3 Beschwerde über Arbeitgeber wegen Veröffentlichungen zum Beschäftigungsende 158

3.4 Franchisenehmer unter Druck 161

3.5 Überwachung der Exfrau durch GPS-Sender im Fahrzeug 162

3.6 Versand einer Bewerbungsmappe für Mietwohnung per E-Mail durch einen Immobilienmakler 165

3.7 Versicherungswerbung per E-Mail 167

3.8 Missbrauch von Gesundheitsdaten bei Wahl der Schwerbehindertenvertretung 170

3.9 Unberechtigte Abrufe von Patientendaten der Ex-Freundin 177

3.10 Unrechtmäßige Beschaffung einer Geburtsurkunde beim Meldeamt 179

3.11 Videoüberwachung im Einkaufszentrum 183

3.12 Bespitzelung durch TLfDI bei Verlangen einer Auskunft? 186

3.13 Videoüberwachung in einem Autohaus 189

3.14 Videoüberwachung einer gemeinschaftlich genutzten Grundstückszufahrt 192

3.15 Allgemeines zu Mieterselbstauskünften – Freiwilligkeit, Zeitpunkt der Übermittlung der Mieterselbstauskunft und weitere Unterlagen? 195

3.16 Daten hin, Daten her, rundherum ist gar nicht schwer – oder? 200

3.17 Prüfen heißt nicht Kopieren! Irrungen beim Nachweis der Befreiung von der Maskenpflicht 202

3.18 Gästedatenerfassung mit DARFICHREIN datenschutzgerecht?! 204

3.19 Darf jeder medizinische Mitarbeiter eines Klinikums auf alle Patientendaten zugreifen? 207

3.20 Corona macht's möglich: Gläserne Gesundheitsdaten auf Grundlage der 3G-Regel – oder doch nicht? 209

3.21 Wechsel vom ärztlichen Angestelltenverhältnis in die ärztliche Selbstständigkeit – wechseln die Patientenakten in Kopie mit? 211

3.22 Personalausweis und Krankenversicherungskarte im postalischen Bermudadreieck 212

3.23 Lieber eine Einwilligung zu viel als eine zu wenig 215

3.24 Bei Überwachungsverdacht ist der TLfDI zur Stelle 217

4. Entschließungen und Beschlüsse 219

4.1 Coronavirus: Impfnachweis, Nachweis negativen Testergebnisses und Genesungsnachweis in der Privatwirtschaft und im Beschäftigungsverhältnis gehören gesetzlich geregelt! 219

4.2 Chancen der Corona-Warn-App 2.0 nutzen 222

4.3 „Energieversorgerpool" darf nicht zu gläsernen Verbraucher*innen führen 224

4.4 Verarbeitung von Positivdaten von Privatpersonen aus Verträgen über Mobilfunkdienste und Dauerhandelskonten durch Auskunfteien 226

4.5 Verarbeitungen des Datums „Impfstatus" von Beschäftigten durch die Arbeitgeberin oder den Arbeitgeber 229

4.6 Zur Möglichkeit der Nichtanwendung technischer und organisatorischer Maßnahmen nach Art. 32 DSGVO auf ausdrücklichen Wunsch betroffener Personen 231

5. Vorträge und Veranstaltungen 232

5.1 Vorträge und Veranstaltungen 2021 232

Stichwortverzeichnis 238

Vorwort



Liebe Leserinnen und Leser,

schon wieder ist ein Jahr vergangen. Beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) war das Jahr 2021 keines zum Durchatmen. Die Pandemie bestimmte die Arbeit der Aufsichtsbehörde nach wie vor. Ständig änderten sich die gesetzlichen Grundlagen auch für die Datenverarbeitungen im Zusammenhang mit der Pandemie.
Daher gab es zahlreiche Beratungsanfragen, sowohl von Verantwortlichen als auch von Bürgern, die ihr Recht auf informationelle Selbstbestimmung gefährdet sahen. Auch die telefonische Beratung, die statistisch nicht erfasst wird, nahm großen Raum ein.
Vor allem auf dem Gebiet des Beschäftigten-Datenschutzes gab es große Irritation. Plötzlich erhob der Arbeitgeber den Impfstatus und womöglich weitere Gesundheitsdaten. Unklar waren den Verantwortlichen oft die notwendigen technischen und organisatorischen Maßnahmen zur Durchführung von Online-Formaten. Besonders an den Thüringer Schulen war die Verunsicherung groß, welche onlinebasierte Software datenschutzkonform zum Einsatz kommen kann. Obwohl eigentlich der Dienstherr hierzu Vorgaben treffen müsste, war der TLfDI erster Ansprechpartner und hat die Schulen in einer Serie von Rundschreiben beraten und zahlreiche Online-Veranstaltungen mit Thüringer Schulleitern abgehalten.
In dieser turbulenten Zeit legte der TLfDI den Fokus auf die Beratung und sah eine wichtige Rolle darin, den Verantwortlichen einen Weg zu weisen, Datenverarbeitung auch in der Pandemie rechtskonform zu gestalten.
Aufgrund der Corona-Regeln waren nur in den dringendsten Fällen Vor-Ort-Kontrollen möglich. Am Tätigkeitsbericht lässt sich erkennen, dass die Behörde des TLfDI auch unter diesen erschwerten Bedingungen ihren Aufgaben gebührend nachgekommen ist. Neben den hier dargestellten exemplarischen Fällen gab es zahlreiche weitere, deren Schilderung den Rahmen dieses Berichtes sprengen würde.

Ich möchte meinen Mitarbeiterinnen und Mitarbeitern meinen großen Dank aussprechen. Sie haben es durch ihren Einsatz, größtenteils aus dem Homeoffice, ermöglicht, dass „der Laden gelaufen“ ist und Verantwortliche und Betroffene aus Thüringen in einer schwierigen Lage Antworten auf ihre zahlreichen Fragen erhalten haben.

Ich wünsche Ihnen bei der Lektüre nützliche Einblicke in unsere Arbeit und weiterführende datenschutzrechtliche Erkenntnisse.

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

1. Themengebiete



© Cevahir - Datenaustausch - fotolia.com

1.1 Schwerpunkte im Berichtszeitraum einschließlich Statistik

Auch im Jahr 2021 spielte die Corona-Pandemie die Hauptrolle in der Tätigkeit der Datenschutz-Aufsichtsbehörde. Es gab zahlreiche Beratungsanfragen von Verantwortlichen zu digitalen Anwendungen und auch zur datenschutzgerechten Gestaltung der 3 G-Nachweise. Gleichzeitig stieg die Zahl der Meldungen nach Art. 33 Datenschutz-Grundverordnung.

Es lässt sich ganz klar sagen: Alles beherrschendes Thema war 2021 wie auch schon im Vorjahr die Corona-Pandemie. Die Verantwortlichen in Thüringen sahen sich vor der Herausforderung, dass viele Leistungen nun in der aus Infektionsschutzgründen gebotenen Distanz erbracht werden mussten, sei es die Arbeitsleistung von Beschäftigten aus dem Homeoffice oder der Schulunterricht.
Die Arbeitgeber wurden durch die Corona-Arbeitsschutzverordnung verpflichtet, ihren Beschäftigten Homeoffice anzubieten, sofern nicht zwingende betriebliche Gründe dem entgegenstehen. Wer vorher noch keine Vorbereitungen und die erforderlichen Festlegungen getroffen hatte, musste nun schnell reagieren und hatte teilweise das Problem,

dass weder die erforderliche Hardware noch Verbindungen zum betrieblichen oder dienstlichen Server von heute auf morgen zur Verfügung standen. Darüber hinaus mussten selbstverständlich auch die weiteren arbeitsschutzrelevanten Vorgaben eingehalten werden. Hier sahen sich die Verantwortlichen etlichen Problemen gegenüber (vergleiche Nummer 1.2).
Auch an den Thüringer Schulen war die Verunsicherung groß, welche onlinebasierte Software datenschutzkonform zum Einsatz kommen kann. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) war hier Ansprechpartner und hat die Schulen unter anderem in einer Serie von Rundschreiben und in Videokonferenzen beraten (vergleiche Nummer 1.5).
Nicht nur die zum Einsatz kommenden Systeme und Anwendungen stellten ein Problem dar, sondern auch die sonstigen Maßnahmen zur Corona-Pandemiebekämpfung. Mit den Änderungen im Infektionsschutzgesetz (IfSG) zur Verarbeitung personenbezogener Daten und im Nachgang den ergänzenden Bestimmungen auf Landesebene wurden kurzfristig gesetzliche Regelungen geschaffen, die auch kurzfristig umzusetzen waren. Unsicherheiten und Irrtümer bei der Verarbeitung von Gesundheitsdaten waren damit vorprogrammiert und es kam zu vielen Anfragen von Gastwirten, Schulen, Schülern, Eltern, Unternehmen und Beschäftigten (vergleiche dazu beispielsweise Beiträge Nr. 1.6, 1.10, 2.19, 2.20, 2.21, 2.23, 2.27, 3.1, 3.18). Einige Verantwortliche wollten ihre Sache zu gut machen und schossen dabei über das Ziel hinaus. Angesichts der besonderen Situation versuchte der TLfDI in diesen Fällen in erster Linie zu beraten und zu vermitteln. Selten war es erforderlich, zu härteren Maßnahmen zu greifen, um datenschutzkonforme Zustände herzustellen.
Wie immer stellte auch die Videoüberwachung einen weiteren Schwerpunkt der Aufsichtstätigkeit dar (vergleiche Nummer 1.9, 2.14, 3.11, 3.13, 3.14).
Es ist unmöglich, alle Fälle, die der TLfDI im Berichtszeitraum bearbeitet hat zu schildern. Der Bericht stellt eine repräsentative Auswahl dar, die einen guten Überblick über die Vielfalt des Tätigkeitsgebietes liefert, von sogenannten Fischfangkarten (Nummer 2.9) über ein digitales Grabstättensuchsystem (Nummer 2.27) bis hin zur GPS-Überwachung der Ex-Frau (Nummer 3.5).
Einige statistische Angaben:
Im Jahr 2021 gab es 21.226 Posteingänge beim TLfDI. Davon waren 4.670 solche in Beschwerdeverfahren nach Art. 77 Datenschutz-

Grundverordnung (DS-GVO), das ist gegenüber dem Vorjahr eine Steigerung um über 50 %. Es handelt sich dabei um Fälle, in denen die Person, die sich an den TLfDI wandte, persönlich betroffen war. Die übrigen Posteingänge setzen sich aus Beratungsanfragen, Anzeigen, Hinweisen und Abstimmungsverfahren zwischen den Aufsichtsbehörden auf innerdeutscher Ebene zusammen. Nicht zu vergessen sind die zahlreichen Telefonate, die die Mitarbeiterinnen beim TLfDI täglich mit Betroffenen und Verantwortlichen führen. Diese werden statistisch nicht erfasst, machen aber einen nicht unerheblichen Teil der Arbeitszeit aus, da sich viele Ratsuchende (zunächst) telefonisch an den TLfDI wenden. So manches Problem kann auf diese Weise auf kurzem Wege gelöst werden.
Es wurden im Berichtsjahr 115 Bußgeldverfahren neu eröffnet, insgesamt 72 Bußgeldbescheide erlassen, also über 70 % mehr als im Vorjahr. Die Höhe der insgesamt festgesetzten Bußgelder betrug 61.325 Euro, das ist über 3,5-mal mehr als im Vorjahr. Darlegungen zum Ablauf eines Bußgeldverfahrens finden sich in Beitrag Nummer 1.11.
Insgesamt gab es 283 Meldungen der Verletzung des Schutzes personenbezogener Daten nach Art. 33 DS-GVO. Dies ist eine Steigerung gegenüber dem Vorjahr von fast 40 %. Für weitere Einzelheiten hierzu wird auf Beitrag Nummer 1.2 verwiesen.

1.2 Meldungen über Verletzungen des Schutzes personenbezogener Daten nach Art. 33 DS-GVO

Die rechtzeitige Meldung der Verletzung des Schutzes personenbezogener Daten innerhalb von 72 Stunden nach ihrer Feststellung erspart den Verantwortlichen ein mögliches Ordnungswidrigkeitsverfahren und Bußgeld. Verantwortliche sind daher gut beraten, einen Datenschutzverstoß zu melden; denn erfährt der TLfDI anderweitig von diesem Datenschutzverstoß, droht regelmäßig ein Bußgeld. Ein Formular zum Ausfüllen findet sich auf der Internetseite des TLfDI. Im Berichtszeitraum wurde der Verpflichtung zur Meldung verstärkt nachgekommen.

Im 3. Tätigkeitsbericht des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) für das Jahr 2020 un-

ter 2.19 wurden die Voraussetzungen für die Verpflichtung zur Meldung durch die Verantwortlichen und die Auswirkungen bereits ausführlich dargelegt.
Im Jahr 2021 gingen beim TLfDI insgesamt 283 Meldungen von öffentlichen und nicht-öffentlichen Stellen ein. Dies ist ein Zuwachs von fast 40 % gegenüber dem Vorjahr.
Die Meldungen sind beim TLfDI vor allem hinsichtlich der Geeignetheit der getroffenen oder noch zu treffenden technischen und organisatorischen Maßnahmen zu prüfen, damit derartige Vorfälle für die Zukunft ausgeschlossen werden können. Immer wieder kommt es auch vor, dass die Verantwortlichen von einer Benachrichtigung der von dem Vorfall betroffenen Personen nach Art. 34 Datenschutz-Grundverordnung absehen, weil sie das Risiko für deren Rechte und Freiheiten als nicht hoch einschätzen. Entsprechenden Hinweisen des TLfDI und Aufforderungen wurde im Berichtszeitraum aber jeweils nachgekommen.
Die häufigsten Fälle waren wiederum Hacker-Angriffe im nicht-öffentlichen Bereich, die zur Verschlüsselung der dort verarbeiteten Bestände von personenbezogenen Daten führten. Nach wie vor ist es daher wichtig, die eigene IT bestmöglich gegen Angriffe von außen und damit auch die Rechte und Freiheiten der von der Datenverarbeitung Betroffenen zu schützen. Dies schließt ein, dass die Mitarbeiter gut informiert und geschult sind, um insbesondere bei Eingang verdächtiger E-Mails richtig zu reagieren.
Ein großer Teil der Meldungen wurde wegen eines „Versehens“ der Mitarbeiter erforderlich, weil personenbezogene Daten an falsche Empfänger gesandt wurden sowohl per Post als auch per E-Mail, vor allem, wenn E-Mail-Verteiler zur Verfügung standen und diese versehentlich genutzt wurden. Es erhielten die falschen Patienten Arztbriefe oder die für andere bestimmten Rechnungen über ärztliche Leistungen (inklusive Diagnose) zusammen mit der für sie bestimmten Rechnung. Angaben zu Personalangelegenheiten wurden ungewollt über Verteiler oder gar versehentlich an völlig unzuständige Personen geschickt.
Immer wieder kommt es auch zum Verlust von Datenträgern durch Einbrüche, zielgerichtete Diebstähle oder Unachtsamkeit, was verdeutlicht, wie wichtig es ist, eine sichere Aufbewahrung zu schaffen und geeignete Festlegungen zum Umgang mit personenbezogenen Daten zu haben.

Ein weiterer recht hoher Anteil der Meldungen betraf festgestellte unberechtigte Zugriffe auf automatisiert gespeicherte Daten in Dateisystemen. In verschiedenen Krankenhäusern wurden durch Unberechtigte Patientendaten eingesehen. Auch im Polizeibereich war immer noch festzustellen, dass es nicht bekannt ist oder ignoriert wurde, dass man auf polizeiliche Dateien nur dann zugreifen und Abfragen tätigen darf, wenn dies aus dienstlichen Gründen erforderlich und auch nachvollziehbar ist. Persönliches Interesse zählt nicht dazu.
Über einzelne besonders interessante Fälle wird in diesem Tätigkeitsbericht informiert.

1.3 JI-Richtlinie reloaded? – Die Evaluation der Richtlinie (EU) 2016/680 und ihre Bedeutung

„Klappern gehört zum Handwerk“: Obwohl der TLfDI schon oft gegenüber der Thüringer Landesregierung, gegenüber dem Thüringer Landtag und im Berichtszeitraum auch gegenüber dem Europäischen Datenschutzausschuss und der Europäischen Kommission dargelegt hat, dass seine Befugnisse bei Datenschutzverstößen im Anwendungsbereich der sogenannten JI-Richtlinie deutlich hinter den Vorgaben aus Art. 47 Abs. 2 Buchstaben a) bis c) der JI-Richtlinie zurückbleiben, ist dieser Mangel bisher nicht gesetzlich behoben worden. Also muss der TLfDI hier weiter „klappern“!

Im Mai 2016 – also vor über sechs Jahren – lief nicht nur die Europäische Datenschutz-Grundverordnung (DS-GVO) „vom Stapel“, auch „ihre kleine Schwester“, 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 sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (kurz: die JI-Richtlinie), trat am 5. Mai 2016 in Kraft. Ein wesentlicher Unterschied zwischen diesen beiden Regelungswerken besteht seitdem darin, dass die JI-Richtlinie im Gegensatz zur DS-GVO nicht unmittelbar gilt, sondern von jedem EU-Mitgliedstaat in das nationale Recht eingefügt werden muss.

Für den Freistaat Thüringen geschah dies mit dem Thüringer Gesetz zur Anpassung des Allgemeinen Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Thüringer Datenschutz-Anpassungs- und Umsetzungsgesetz EU [ThürDSAnpUG-EU]). Leider wurde in dieser Gesetzesnovelle – was die Implementierung der JI-Richtlinie in das heute geltende Thüringer Datenschutzgesetz (ThürDSG) betrifft – entweder vergessen, wesentliche Normen der JI-Richtlinie in das ThürDSG zu überführen oder aber der Thüringer Gesetzgeber versäumte bewusst bestimmte Regelungen der JI-Richtlinie in das ThürDSG aufzunehmen. Dies belegen die folgenden zwei Beispiele anschaulich:

1. In Art 4. Abs. 1 Buchstaben a) bis f) JI-Richtlinie sind sechs Grundsätze der Datenverarbeitung aufgelistet (Grundsatz der Rechtmäßigkeit der Datenverarbeitung, Grundsatz der Zweckfestlegung und Zweckbindung, Grundsatz der Verhältnismäßigkeit der Datenerhebung, Grundsatz der Richtigkeit der Daten, Grundsatz der zeitlichen Begrenzung der Speicherdauer und Grundsatz der Integrität und Vertraulichkeit). Obwohl diese sechs genannten Verarbeitungsgrundsätze der JI-Richtlinie als rechtsverbindliche und durchsetzbare Handlungsanweisungen anzusehen sind und nicht als unverbindliche Programmsätze (so Kugelmann/Skobel, LDSG-Rheinland-Pfalz, § 28 Rn. 8.), hat sie weder die Thüringer Landesregierung in ihrem Gesetzentwurf in der Drucksache 6/4943 noch der Thüringer Landtag in seiner Beschlussempfehlung in der Drucksache 6/5722 dem § 33 Thüringer Datenschutzgesetz eingefügt.

2. Noch gravierender, weil bewusst unterlassen, wirkt die mangelhafte Umsetzung des Regelungsgehalts von Art. 47 Abs. 2 JI-Richtlinie: Hier sind in den Buchstaben a) bis c) die Abhilfebefugnisse in Form der Warnung, der Anweisung und der vorübergehenden oder der endgültigen Beschränkung der Verarbeitung aufgelistet, über die jede Datenschutzaufsichtsbehörde im Anwendungsbereich der JI-Richtlinie verfügen muss. Obwohl der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) sowohl im Kabinettanhörungsverfahren als auch im parlamentarischen Anhörungsverfahren des Thüringer Landtags darauf hingewiesen hatte, dass der genannte Gesetzentwurf der Landesregierung in der Drucksache 6/4943 nur das Sanktionselement der Beanstandung für den TLfDI vorsieht, änderte der Thüringer Landtag im Sommer 2018 den Wortlaut des § 7 Abs. 6 ThürDSG, sodass der TLfDI seitdem im An-

wendungsbereich der §§ 31 ff. ThürDSG, die die Inhalte der JI-Richtlinie in das Thüringer Landesrecht überführt haben, bei Datenschutzverstößen lediglich ein Beanstandungsrecht besitzt. So weit, so schlecht!
Im Herbst 2021 startete die Europäische Kommission eine Evaluierung der JI-Richtlinie. Auch der TLfDI beteiligte sich an der Evaluierung, indem er die insgesamt über 40 Fragen aus dem Fragebogen der Europäischen Kommission beantwortete und sie über den Arbeitskreis Sicherheit der Datenschutzkonferenz des Bundes und der Länder (DSK) zurück an den Europäischen Datenschutzausschuss (EDSA) übermittelte. Auch im Rahmen dieser Evaluierung wiest der TLfDI erneut darauf hin, dass seine in § 7 Abs. 6 ThürDSG ausgestalteten Befugnisse weit hinter dem Rechtsrahmen zurückbleiben, den Art. 47 Abs. 2 Buchstaben a) bis c) der JI-Richtlinie offeriert.
Am 14. Dezember 2021 nahm der Europäische Datenschutzausschuss (EDSA) seinen Beitrag zur Evaluation der JI-Richtlinie durch die Europäische Kommission an (siehe dazu: https://edpb.europa.eu/system/files/2021-12/edpb_contribution_led_review_en.pdf). Obwohl auch in diesem Beitrag auf Seite 9, und hier insbesondere in dem Tortendiagramm, klar zum Ausdruck gebracht wird, dass neben den Deutschen Datenschutzaufsichtsbehörden auch die dänischen Kolleginnen und Kollegen längst nicht über alle Befugnisse verfügen, die Art. 47 Abs. 2 JI-Richtlinie für Datenschutzverstöße vorsieht, hat der EDSA es bisher offensichtlich nicht für erforderlich erachtet, hier weitere Maßnahmen einzuleiten. Daher wird der TLfDI sich im Anwendungsbereich der JI-Richtlinie weiterhin mit seinem Beanstandungsrecht begnügen müssen, es sei denn, die Thüringer Landesregierung wird in der nächsten Zeit eine Novellierung des Thüringer Datenschutzgesetzes anschieben.

1.4 Sormas oder wie ein staatlich bundesweit gefördertes Projekt seinen wahren Auftrag sucht …

Gemäß Art. 5 Abs. 1 Buchstabe a) und Buchstabe b) DS-GVO dürfen personenbezogene Daten nicht ohne Rechtsgrundlage und nur für festgelegte, eindeutige und legitime Zwecke erhoben und verarbeitet werden. Die verarbeiteten personenbezogenen Daten müssen gemäß Art. 5 Abs. 1 Buchstabe c) DS-GVO dem Verarbeitungszweck angemessen und auf das dafür notwendige Maß beschränkt werden. Diese datenschutzrechtlichen Vorgaben gelten in besonderem Maße für die

Verarbeitung besonderer Kategorien von Daten nach Art. 9 Abs. 1 DS-GVO. In diesem Sinne unterliegen personenbezogene Gesundheitsdaten einem besonderen Schutz und auch staatliche Stellen sind verpflichtet, diesen Schutz zu respektieren und nicht gegen die verordnungsrechtlichen Vorgaben zur Datenverarbeitung zu verstoßen.

Spätestens im Frühjahr 2020 begann die Corona-Pandemie, sukzessive die Bundesrepublik Deutschland und damit auch den Freistaat Thüringen zu erfassen. Von den zuständigen Behörden wurden umfassende Hygienevorschriften erlassen, Quarantäneanordnungen getroffen und Formulare oder digitale Programme zur Kontaktnachverfolgung von betroffenen Personen, die an Corona erkrankt waren, entwickelt. Die Versuche, hierbei den Datenschutz zu wahren, die Daten betroffener Personen nicht an unbefugte Dritte weiterzugeben, waren mal mehr und mal weniger erfolgreich. Die staatlichen Gesundheitsämter sammelten die Daten, die von kulturellen und Gastronomieeinrichtungen im Freistaat gemäß der jeweils gültigen Coronaverordnung des Thüringer Gesundheitsministeriums verarbeitet, das heißt erhoben werden mussten. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) versuchte nach besten Kräften, die Beschwerde- und Anfrageflut zu bewältigen. Mit dem hehren Ziel, die Kontaktnachverfolgung im Rahmen der Maßnahmen zur Eindämmung der Corona-Pandemie für die staatlichen Gesundheitsämter zu erleichtern, beschloss das Bundesgesundheitsministerium (BMG), eine einheitliche Software zur Kontaktnachverfolgung für alle Gesundheitsämter in der Bundesrepublik zu entwickeln beziehungsweise entwickeln zu lassen und als Grundlage hierfür eine bereits existierende, sogenannte OpenSourceSoftware namens SORMAS zu nutzen. Diese Software wurde bereits in Afrika zur Nachverfolgung der Übertragungswege verschiedener Viruserkrankungen eingesetzt. Allerdings erfolgte dies in wesentlich kleineren regionalen Gebieten und aufgrund geringer Besiedelungsstruktur mit weitaus weniger betroffenen Personen als im Falle der Corona-Pandemie in Deutschland.
Somit war es erforderlich, sowohl die technischen Konfigurationen der Software zu ändern als auch die konkreten personenbezogenen Daten, die mittels der Software erhoben wurden, um SORMAS-X, so der neue Name, für Zwecke der Kontaktnachverfolgung hinsichtlich der Coronaausbreitung in Deutschland einsetzen zu können. Mit die-

ser Entwicklungsaufgabe beauftragte das BGM das Helmholtz-Zentrum für Infektionsforschung (HZI) und reichte dafür eine sehr hohe Summe Finanzmittel an das HZI aus. Doch erst, als die technischen und inhaltlichen Anpassungen der Software SORMAS-X bereits in vollem Gange waren, kam es zu einer Beteiligung der Datenschutzaufsichtsbehörden. Unter der Federführung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) wurde eine „SORMAS-AG“ der Datenschutzbehörden ins Leben gerufen, an der sich auch der TLfDI beteiligte.

Ende November 2020 gab es ein Auftakttreffen der „SORMAS-AG“, das unter Corona-Bedingungen als Videokonferenz stattfand. Teilnehmer waren Datenschutzaufsichtsbehörden, das HZI, verschiedene Subunternehmen, die das HZI seinerseits mit der Anpassung der Software beauftragt hatte sowie das BMG. Bereits bei diesem Treffen wurde den Datenschutzaufsichtsbehörden als „Auftakt“ die „Datenfeldertabelle“ vom „angepassten“ SORMAS-X präsentiert. Die Tabelle enthielt eine hohe Zahl von Datenfeldern, die im Rahmen der Kontaktnachverfolgung mit personenbezogenen Daten der jeweils betroffenen Person und zugehörigen (Corona-)„Falldaten“ auszufüllen waren. Das lag daran, dass die in der ursprünglichen Version der Software bereits enthaltenen Datenfelder einfach recht umfassend „aufgestockt“ worden waren. Der BfDI stimmte am Januar 2021 einem Betrieb von SORMAS-X in den Gesundheitsämtern nur unter Vorbehalt zu. Voraussetzung dafür war eine schriftliche Zusicherung, dass die Unterlagen im laufenden Betrieb nachgebessert und vervollständigt werden (vergleiche Tätigkeitsberichte des BfDI Nr. 4.1.2 unter https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Taetigkeitsberichte/30TB_21.pdf;jsessionid=23B1EB1AED7A73BB9A124E3958A3F9D2.intranet231?__blob=publicationFile&v=8).

Diese Nachbesserung und Vervollständigung wurde durch die SORMAS-AG in etlichen Sitzungen begleitet. Die Datenschützer waren sich einig, dass eine effiziente digitale Kontaktnachverfolgung durch die Gesundheitsämter als Bestandteil der Maßnahmen zur Eindämmung der Corona-Pandemie mit bestimmten Datenfeldern notwendig sei und die dementsprechend zu erhebenden personenbezogenen Daten sowohl erforderlich als auch dem Zweck angemessen sein und entsprechende Rechtgrundlagen im Infektionsschutzgesetz (IfSG) bestehen müssen.

In der Sitzung im Januar 2021 teilten die Datenschutzaufsichtsbehörden dem HZI das Ergebnis ihrer ersten Prüfung der Datenfeldertabelle und ihre Auffassung zur erforderlichen Anzahl der Datenfelder für eine effiziente Kontaktnachverfolgung mit. Es wurden Änderungen am Löschkonzept, am Pseudonymisierungskonzept und hinsichtlich der Zugriffs- und Rollenrechte in den Gesundheitsämtern gefordert. Der notwenige Umsetzungsprozess erforderte etliche Sitzungen zur Abstimmung der notwendigen Einzelheiten. Im Sommer 2021 teilte das HZI mit, dass die Software nicht ausschließlich der Kontaktnachverfolgung diene, sondern die erhobenen Daten der betroffenen Personen auch für (weitergehende) wissenschaftliche Zwecke genutzt werden sollen.
Im Rahmen von SORMAS-X werden besondere Kategorien von Daten, vorliegend Gesundheitsdaten nach Art. 9 Abs. 1 Datenschutz-Grundverordnung (DS-GVO) verarbeitet. Für die Verarbeitung dieser Daten gilt ein besonderer Schutz hinsichtlich der Einhaltung der Vorgaben aus Art. 5 Abs. 1 DS-GVO, das heißt, die Daten müssen auf auf das notwendige Maß beschränkt, auf rechtmäßige Weise, für eindeutig festgelegte Zwecke und integritätswahrend verarbeitet werden. Gemäß Art. 89 DS-GVO in Verbindung mit Erwägungsgrund 159 DS-GVO können personenbezogene Daten, auch Gesundheitsdaten, zu wissenschaftlichen Forschungszwecken verarbeitet werden, wenn sichergestellt ist, dass die Datenminimierung mittels technischer und organisatorischer Maßnahmen, vorzugsweise durch Pseudonymisierung der Daten, gewährleistet ist und dadurch die Rechte und Freiheiten der betroffenen Personen gewahrt werden (Art. 89 Abs. 1 DS-GVO).
Um die Entwicklung einer rechtlich und technisch datenschutzkonformen Struktur und Konfiguration der Software SORMAS-X voranzutreiben, wurde zusätzlich zur SORMAS-AG eine AG-Technik, eine AG-Recht und eine AG-Datenfeldertabelle ins Leben gerufen. Durch die fachliche AG-Aufteilung und die daraus resultierenden effizienteren Arbeitsstrukturen konnten bis Ende Dezember 2021 kleine Entwicklungsfortschritte in Richtung einer datenschutzkonformen Software SORMAS-X erzielt werden. Dennoch blieben die Fortschritte bis Ende Dezember 2021 hinter den Forderungen und Erwartungen zurück.
Vor diesem Hintergrund führte der TLfDI eine Umfrage unter den Thüringer Gesundheitsämtern durch, ob sie zur Kontaktnachverfolgung bereits die neue Software SORMAS-X oder datenschutzkon-

forme Vorgängerversionen beziehungsweise ganz andere Softwareprogramme nutzen. Bis Ende Dezember 2021 hatten von den 23 Thüringer Gesundheitsämtern 17 die Anfrage des TLfDI beantwortet. Hiervon nutzten lediglich sechs Ämter die Software SORMAS-X. Die übrigen Gesundheitsämter nutzten entweder andere SORMAS-Versionen oder völlig andere Software. Die Gesundheitsämter, die eine andere Software nutzten, haben durchgängig erklärt, dass sie die genutzte Software präferieren und damit sehr gut in der Lage seien, die Kontaktnachverfolgungen zur Eindämmung der Corona-Pandemie durchzuführen und zugehörige präventive Maßnahmen umzusetzen. Vergleichbar äußerten sich auch die Gesundheitsämter, die andere SORMAS-Versionen nutzten. Der TLfDI teilte das Ergebnis seiner Umfrage im Januar 2022 dem Thüringer Ministerium für Arbeit, Soziales, Gesundheit, Frauen und Familie als oberster Fachaufsicht über die Thüringer Gesundheitsämter mit und wies auf die noch bestehenden datenschutzrechtlichen Defizite beim Einsatz von SORMAS-X hin.
Die Arbeit der SORMAS-AG war zum Ende des Berichtszeitraums noch nicht abgeschlossen. Daher wird im nächsten Tätigkeitsbericht über den Ausgang des Verfahrens berichtet werden.

1.5 Rundschreiben des TLfDI an die Schulen und ViKos mit Schulleitungen

An den Thüringer Schulen war die Verunsicherung groß, welche onlinebasierte Software datenschutzkonform zum Einsatz kommen kann. Mit der Umstellung auf häusliches Lernen aufgrund der Corona-Pandemie wurde das besonders deutlich. Obwohl eigentlich der Dienstherr hierzu Vorgaben treffen müsste, war der TLfDI einmal mehr erster Ansprechpartner und hat die Schulen unter anderem in einer Serie von Rundschreiben beraten.

Plötzlich Unterricht von zu Hause statt auf der Schulbank. Laptop statt Schreibblock, Schulcloud statt Tafel, Videokonferenz statt Klassenzimmer – das brachte ab 2020 enorme Herausforderungen für Schülerinnen und Schüler, Lehrkräfte, Schulleitungen und Eltern. Und diese Herausforderungen haben sichtbar gemacht, was mit hohem Engagement aller Beteiligten geht in den Thüringer Schulen, aber auch, wo es hakt. Neben den technischen Aspekten stand für viele Lehrkräfte die Frage, mit welchen Onlinetools häusliches Lernen attraktiv und

erfolgreich gestaltet werden kann. Da richtet sich der erste Blick naturgemäß aufs Inhaltliche: Welches Videokonferenz-System ist praktikabel und stabil genug? Mit welchem Werkzeug bekomme ich Aufgaben und Informationen schnell in meine Klasse? Schnell und dankbar griff man da zu Tools, die Kollegen empfahlen oder die bei Google ganz oben stehen. Fast allen webbasierten Angeboten ist gemeinsam, dass personenbezogene Daten verarbeitet werden, sei es bei der Anmeldung, den individuellen Arbeitsergebnissen und natürlich dem, was das (private) Endgerät über den Nutzer „nebenbei“ in die Welt schickt. Erfreulich für den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) war und ist, dass man sich in den Schulen neben dem Funktionalen auch mehr und mehr Gedanken darüber macht, ob ein Tool xy datenschutzrechtlich in Ordnung ist oder nicht. Die Flut von Anfragen an den TLfDI war sichtbarer Beleg. Obwohl die Landesdatenschutzbehörden keine Zertifizierungsstellen für Schulsoftware sind, hat der TLfDI die Hilferufe aus den Schulen aufgegriffen und viele Tools kursorisch geprüft, von A wie Anton über Padlet und Youtube bis Z wie Zoom. Neben vielen Antworten auf Einzelanfragen richtete der TLfDI im Zeitraum von Januar bis August 2021 insgesamt sieben Rundschreiben an alle Thüringer Schulen, um mit der notwendigen Reichweite aufzuklären. Leider wurde bei den Prüfungen sichtbar, dass viele Tools transatlantische Verbindungen, namentlich in die USA, aufbauen, wobei der TLfDI die dafür notwendigen Garantien für die Einhaltung des europäischen Datenschutzniveaus nicht gewährleistet sieht. Genau das fordert jedoch das bedeutsame „Schrems II“-Urteil des Europäischen Gerichtshofs vom 16. Juli 2020 (Rechtssache C 311/18), das weitreichende Folgen auch für die Schulen hat. Sie müssten als datenschutzrechtlich Verantwortliche gegebenenfalls die Betroffenenrechte (hier von Schülern, Lehrkräften, Eltern) vor amerikanischen Gerichten auf Basis der dortigen Rechtslage durchsetzen, was aus Sicht des TLfDI unmöglich ist. Auch der inflationäre Einsatz von nicht abschaltbaren Trackingmechanismen auf vielen Websites oder die Nutzung von Werbeplattformen sind Hinderungsgründe, welche die Nutzung von Online-Plattformen im Schulunterricht oft unmöglich machen – aber leider gerade bei kostenlosen Plattformen weit verbreitet sind. So musste der TLfDI leider manche Euphorie über das eine oder andere pädagogisch sinnvolle Tool dämpfen. Dass es durchaus datenschutzkonforme Lösun-

gen für den schulischen Einsatz gibt, beweisen Angebote wie Edupage, Anton, Moodle, Mundo, School.cloud und andere[1], die natürlich auch Gegenstand in den besagten Rundschreiben waren.
Neben diesen Rundschreiben setzte der TLfDI auch weiterhin auf regelmäßige Videokonferenzen mit Schulleitungen, in denen allgemeine und aktuelle schuldatenschutzrechtliche Probleme dargestellt, diskutiert und in FAQs zusammengefasst wurden.
Durchweg positive Rückmeldungen signalisieren, dass der TLfDI hiermit für Thüringen einen guten Weg gefunden hat, der bundesweit einmalig ist.

1.6 Mund-Nasen-Bedeckung in der Schule

Eine Befreiung von der Maskenpflicht muss laut Verordnung „glaubhaft“ gemacht werden – wie genau das erfolgen kann, ist nicht festgelegt. Ob ein Attest zur „Masken-Befreiung“ eine Diagnose enthalten muss, ist strittig. Unstrittig ist, dass beim Verdacht auf ein Gefälligkeitsattest die Schule die Unterlagen zur Prüfung an das zuständige Schulamt weiterleiten darf.

Seit Beginn der Maskenpflicht in den Thüringer Schulen erreichen den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) regelmäßig Beschwerden, dass einzelne Schulen Atteste zur Befreiung von der Verpflichtung zum Tragen einer medizinischen Mund-Nasen-Bedeckung nicht anerkennen, weil sie entweder keine Diagnose enthalten oder vermutet wird, dass es sich um ein sogenanntes Gefälligkeitsattest handelt. Außerdem würden Schulen die Atteste zur Prüfung an die zuständigen Schulämter weiterleiten und damit Gesundheitsdaten Dritten zugänglich machen.
Besonders problematisch bei diesen Fällen ist der Umstand, dass für die Kinder, sofern sie keine Maske tragen und der Befreiungsgrund – noch – nicht als glaubhaft anerkannt ist, trotz Schulpflicht ein Betretungsverbot für die Schule gilt.
So beschwerte sich auch die Mutter eines Kindes, die der Schule ein ärztliches Attest zur Befreiung von der Maskenpflicht vorgelegt hatte. Als Antwort erhielt sie eine Nachricht der Schulleitung, dass das At-

[1] Die Aussagen beziehen sich auf die jeweils geprüfte Version und den Prüfzeitpunkt.

test mangels Diagnose nicht glaubhaft wäre und daher an das Schulamt weitergeleitet worden sei, um dort eine abschließende Prüfung vorzunehmen.
Die Verpflichtung zur Verwendung einer qualifizierten Gesichtsmaske gilt gemäß § 6 Abs. 5 Nr. 2 der Thüringer Verordnung zur Regelung infektionsschutzrechtlicher Maßnahmen zur Eindämmung des Coronavirus SARS-CoV-2 (ThürSARS-CoV-2-IfS-MaßnVO) nicht für Personen, denen die Verwendung einer qualifizierten Gesichtsmaske wegen Behinderung oder aus gesundheitlichen oder anderen Gründen nicht möglich oder unzumutbar ist; dies muss in geeigneter Weise glaubhaft gemacht werden.
Zur Frage, in welcher Weise die Glaubhaftmachung erfolgen kann, heißt es in der Begründung zur Verordnung: „Dies kann z. B. durch das Vorweisen eines ärztlichen Zeugnisses (…) geschehen.“ Da keine konkreten Anforderungen an die Ausgestaltung eines ärztlichen Zeugnisses vom Gesetzgeber gestellt werden, muss der unbestimmte Rechtsbegriff „in geeigneter Weise“ ausgelegt werden.
Aus datenschutzrechtlicher Sicht gilt der Grundsatz der Datenminimierung (Art. 5 Abs. 1 Buchstabe c) Datenschutz-Grundverordnung (DS-GVO)), wonach die Verarbeitung personenbezogener Daten auf das für die Zwecke notwendige Maß zu beschränken ist. Danach muss das Attest nur so viele Informationen enthalten, wie zur Glaubhaftmachung erforderlich sind. Bei medizinischen Diagnosen handelt es sich um besondere Kategorien von personenbezogenen Daten gemäß Art. 9 DS-GVO, in diesem Fall um Gesundheitsdaten. Diese unterliegen einem besonderen Schutz und dürfen ohne Einwilligung der betroffenen Person nur unter ganz bestimmten, strengen Voraussetzungen verarbeitet werden (Art. 9 Abs. 2 DS-GVO).
In einigen Bundesländern (zum Beispiel Bayern) enthalten die entsprechenden Corona-Verordnungen klare Vorgaben, dass ein solches Attest eine medizinische Diagnose enthalten muss; für die Verarbeitung der Gesundheitsdaten ist damit gemäß Art. 9 Abs. 2 Buchstabe g) DS-GVO eine Rechtsgrundlage vorhanden. In Ländern, in denen diese Vorgaben fehlen, sind zwischenzeitlich mehrere gerichtliche Urteile zur Ausgestaltung eines Attests zur Vorlage bei der Schule ergangen. So kommt das Oberlandesgericht Dresden in seiner Entscheidung vom 6. Januar 2021 (6 W 939/20) zu der Auffassung, dass ärztliche Atteste, die vom Tragen eines Mund-Nasenschutzes befreien, zwar keine Diagnose enthalten, aber zumindest nachvollziehbar dokumentieren

müssen, welche „konkreten gesundheitlichen Beeinträchtigungen aufgrund der Tragepflicht in der Schule alsbald zu erwarten sind und woraus diese im Einzelnen resultieren".
Auch in Baden-Württemberg fehlen, vergleichbar wie in Thüringen, in der entsprechenden Verordnung konkrete Vorgaben zur Glaubhaftmachung eines Ausnahmetatbestandes. Hier hat das Verwaltungsgericht Sigmaringen mit Urteil vom 22. Juni 2021 (4 K 1827/21) für die Anforderungen an ein ärztliches Attest zur Befreiung von der Maskenpflicht zur Vorlage bei der Schule Folgendes festgestellt: „Die Glaubhaftmachung des Vorliegens eines Ausnahmetatbestands durch eine ärztliche Bescheinigung, der dazu berechtigt, die Schule ohne Maske zu besuchen, setzt grundsätzlich nicht voraus, dass ein qualifiziertes ärztliches Attest vorgelegt werden muss." Bei der Prüfung des Ausnahmetatbestandes sei grundsätzlich zu beachten, dass die Corona-Verordnungen keine ausdrückliche Definition des Begriffs der ärztlichen Bescheinigung oder qualitative Vorgaben hierzu enthalten; darüber hinaus werde ärztlichen Attesten im Rechtsverkehr grundsätzlich eine gehobene Beweiswirkung zugesprochen. Die Preisgabe von Gesundheitsdaten sei besonders sensibel und dem Schüler stehe grundsätzlich ein Recht auf Teilnahme am Unterricht zu.
In Thüringen gab es zum Zeitpunkt der Bearbeitung der Beschwerde noch kein Gerichtsurteil zur Ausgestaltung der Atteste. Um auf die Situation zu reagieren, haben einige kreisfreie Städte und Landkreise in Thüringen in Bezug auf die nicht eindeutige Regelung in § 6 Abs. 3 Nr. 2 der ThürSARS-CoV-2-IfSGrundVO – wonach Personen, denen die Verwendung einer Mund-Nasen-Bedeckung nicht möglich oder unzumutbar ist dies in geeigneter Weise glaubhaft zu machen haben – eigene Allgemeinverfügungen erlassen und darin beispielsweise die Regelung getroffen, dass das ärztliche Attest zur Befreiung von der Maskenpflicht im zuständigen Gesundheitsamt vorgelegt werden muss und das Gesundheitsamt eine eigene Bescheinigung ausstellt, die die Kontraindikation zum Tragen einer Maske bestätigt. Die medizinische Diagnose ist in diesem Falle nur der/dem befugten Mitarbeiter/in des Gesundheitsamts nach dem Infektionsschutzgesetz (IfSG) vorzulegen. Sofern es sich um den/die Amtsarzt/-ärztin handelt, ist diese/r zudem Berufsgeheimnisträger aufgrund § 203 Abs. 1 Strafgesetzbuch (StGB). Damit wird der Schutz sensibler personenbezogener Gesundheitsdaten im Sinne von Art. 9 Abs. 1 DS-GVO sicher gewahrt. Wenngleich eine Allgemeinverfügung schon aufgrund ihres

Rechtcharakters nicht als Rechtsgrundlage für dieses Verfahren gelten kann, stellt dieses Vorgehen für die beteiligten Seiten – also Sorgeberechtigte und Schulleitung – einen Hinweis dar, der – sofern im Einklang mit dem Gesetz stehend – zu einer rascheren Klärung führen kann, als dies durch ein Gerichtsverfahren möglich ist. Gerade angesichts der Schulpflicht und des bei einem Betretungsverbot für das Kind potentiell versäumten Unterrichtsstoffs riet der TLfDI daher der Beschwerdeführerin, sich an das zuständige Gesundheitsamt zu wenden und dort um eine entsprechende Bescheinigung zu bitten.
Bei der Bewertung der Weiterleitung der Namen der Beschwerdeführerin und ihres Kindes sowie des Attests durch die Schule an das zuständige Schulamt handelte es sich ebenfalls um die Verarbeitung von personenbezogenen Gesundheitsdaten. Dies ist nur rechtmäßig, wenn mindestens eine der Voraussetzungen des Art. 9 Abs. 2 DS-GVO vorliegt. Im konkreten Fall kam Art. 9 Abs. 2 Buchstabe g) DS-GVO in Verbindung mit einer nationalen Vorschrift in Betracht, wonach die Schule die Unterlagen aus Gründen eines erheblichen öffentlichen Interesses aufgrund der bestehenden Corona-Pandemie übermittelt haben könnte. Um von der bestehenden Maskenpflicht befreit zu werden, bedarf es der Vorlage eines Attests bei der Schulleitung. Gemäß § 4 Abs. 3 Satz 1 Thüringer Gesetz über die Schulaufsicht (ThürSchulAG) haben die staatlichen Schulämter als untere Schulaufsichtsbehörden die Fachaufsicht über die Schulen; eine Übermittlung an und eine Überprüfung durch die zuständige Aufsichtsbehörde ist daher, sofern bei der Schulleitung Unklarheit über die Anerkennung des Attests besteht, zulässig.
Unabhängig von der Frage, ob ein Attest eine Diagnose oder mögliche gesundheitliche Folgen durch das Tragen einer Mund-Nase-Bedeckung enthalten muss, soll sichergestellt werden, dass ein sogenanntes Gefälligkeitsattest ausgeschlossen werden kann. Dies kann zum Beispiel dann der Fall sein, wenn Ärzte solche Atteste zugunsten von Personen ausstellen, die in erheblicher Entfernung wohnen und über ihren angestammten Patientenkreis hinausgehen.
Nach Auskunft des Schulleiters enthielt das Attest keine Diagnosen oder anderen Gesundheitsdaten des Kindes und war von einem Arzt ausgestellt, dessen Praxis sich nicht in einem mittleren Umkreis um den Standort der Schule befindet. Da für das Kind, sofern es keine Maske trägt und kein glaubhaft gemachter Befreiungsgrund vorliegt, einerseits ein Betretungsverbot für die Schule, andererseits aber gemäß § 17 Abs. 1 Satz 1 Thüringer Schulgesetz Schulpflicht besteht,

hatte sich der Schulleiter mit der Bitte um Prüfung der Angelegenheit an das zuständige staatliche Schulamt gewandt und um Prüfung gebeten. Die Weiterleitung des Attests erfolgte gemäß Art. 9 Abs. 2 Buchstabe g) DS-GVO in Verbindung mit § 4 Abs. 3 ThürSchulAG also aufgrund einer gültigen Rechtsgrundlage und ist damit aus datenschutzrechtlicher Sicht nicht zu bemängeln.

1.7 AG KMK und Datenschützer zu Microsoft 365

Wie andere Onlinedienste muss auch Microsoft 365 die datenschutzrechtlichen Bestimmungen der Europäischen Datenschutz-Grundverordnung einhalten, damit der Dienst in den Thüringer staatlichen Schulen eingesetzt werden darf. Derzeit gibt es zu viele Fragen und Unklarheiten bei Microsoft 365, um von einer Zulässigkeit der Nutzung zu schulischen Zwecken ausgehen zu können.

Die Onlinedienste der Firma Microsoft stehen bereits seit langer Zeit aus datenschutzrechtlichen Gründen in der Kritik. Dies gilt insbesondere für das Produkt „Microsoft 365“ (bisher: „Office 365“), welches häufig in Schulen bei Lehrkräften sowie Schülerinnen und Schülern zum Einsatz kommt und in einigen Bundesländern sogar von den dortigen Kultusministerien empfohlen, in jedem Fall aber geduldet wird. Dieses Paket enthält unter anderem Tools für die Erstellung von Dokumenten, Tabellenkalkulationen, Präsentationen, Videokonferenzen, E-Mails, das Teilen von Dateien und Fotos und so weiter. In diesem Zusammenhang hatte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) gemeinsam mit der Kultusministerkonferenz (KMK) eine Arbeitsgruppe (AG) „Datenschutz“ gegründet. Im Mittelpunkt dieser Arbeitsgruppe stehen die Belange und die Rolle des Datenschutzes im Rahmen der Digitalisierung der Schule. Die Corona-Pandemie bewirkte einen großen Schub bei der Nutzung von Schulsoftware-Anwendungen, die die Lehrkräfte teilweise ohne jegliche datenschutzrechtliche Prüfung zur Nutzung im Unterricht einsetz(t)en. Insbesondere wird nicht beachtet, dass spätestens mit dem Urteil des Europäischen Gerichtshofs zur Rechtssache C-311/18 „Schrems II“ personenbezogene Daten nicht in Drittländer übermittelt werden dürfen, die über keinen im Wesentlichen gleichwertigen Schutz für personenbezogene Daten verfügen wie in der Europäischen Union. Bereits die Beachtung dieses Urteils stellt eine hohe Hürde für US-amerikanische Onlinedienste dar. Dies ist daher

auch von den staatlichen Schulen bei der geplanten Nutzung des cloudbasierten Produkts Microsoft 365 zu beachten.
Für die Arbeit der oben genannten Arbeitsgruppe mit der KMK war eine datenschutzrechtliche Auswertung eines Pilotprojekts des baden-württembergischen Kultusministeriums zur Nutzung des Cloud-Dienstes Microsoft 365 in Schulen von Baden-Württemberg durch den Landesbeauftragten für Datenschutz und Informationsfreiheit Baden-Württemberg sehr hilfreich. Die Bewertungen des Pilotprojekts von der Datenschutzaufsichtsbehörde aus Baden-Württemberg sind unter https://fragdenstaat.de/anfrage/neubewertung-des-lfdi-bezuglich-der-dsfa-von-microsoft-office-365-1/626585/anhang/2021-04-23_Empfehlung_LfDI.pdf nachzulesen. Als Ergebnis des vorliegenden Gutachtens hatte das baden-württembergische Kultusministerium erklärt, auf den Einsatz des Softwarepakets Microsoft Office 365 zu verzichten https://www.swr.de/swraktuell/baden-wuerttemberg/kultusministerium-verzichtet-auf-microsoft-produkte-bei-schulplattform-100.html.
In einer vom TLfDI organisierten Konferenz zu diesem Produkt ergaben sich Zweifel daran, ob Microsoft bei der Nutzung des Cloud-Dienstes Microsoft 365 als Auftragsverarbeiter nach Art. 28 Datenschutz-Grundverordnung (DS-GVO) für die Verantwortlichen, also zum Beispiel die Schulen, tätig wird. Dies würde voraussetzen, dass die Schulen selbst über den Umfang der zu verarbeitenden Daten der Schülerinnen und Schüler sowie der Lehrkräfte und auch über den Verarbeitungszweck entscheiden können. Dies ist aber offensichtlich nicht der Fall. Vielmehr muss beim Einsatz von Microsoft 365 den von Microsoft erlassenen Verarbeitungsbedingungen zugestimmt werden. Ebenso kritikwürdig ist es, dass nicht ausreichend transparent wird, ob und welche Daten von Microsoft zu eigenen Zwecken verarbeitet werden. Da die staatlichen Schulen öffentliche Stellen des Freistaats Thüringen sind, darf sich das Unternehmen gemäß Art. 6 Abs. 1 Satz 2 DS-GVO nicht auf seine berechtigten Interessen berufen. Deshalb ist etwa die Verarbeitung zur Verbesserung des Produkts nicht zulässig. Die Schulen müssen darauf achten, nur Datenverarbeitungen zu ermöglichen, die zur Erfüllung ihrer gesetzlichen Aufgaben erforderlich sind. Deshalb müssen alle darüber hinausgehenden Verarbeitungen von Microsoft vertraglich und auch insbesondere durch eine entsprechende Systemeinstellung ausgeschlossen sein. Wie weiterhin festgestellt werden konnte, versucht Microsoft von den Nutzern Ein-

willigungen in bestimmte Verarbeitungen einzuholen, die das Unternehmen durchführt. Bei der Nutzung einer staatlichen Lernplattform ist es aber fragwürdig, ob solche Einwilligungen durch ein privates Unternehmen zulässigerweise bei den betroffenen Schülerinnen und Schülern sowie den Lehrkräften eingeholt werden dürfen. Letztlich wird dabei ein vertraglich zwischen Schule und Microsoft abgeschlossenes Vertragsverhältnis um weitere Datenverarbeitungsmöglichkeiten erweitert.
Nachdem die AG unter Beteiligung des TLfDI sowie einigen Vertretern von anderen Landesdatenschutzbehörden mit Vertretern der KMK sich bereits Ende 2021 erstmalig zu verschiedenen datenschutzrechtlich relevanten Schulthemen ausgetauscht hatte, erfolgte Anfang 2022 eine weitere Sitzung speziell zum Thema Microsoft 365. Dabei wurden alle datenschutzrechtlichen Kritikpunkte ausführlich erläutert und bestehende Fragen beantwortet. Der TLfDI hat zur weiteren Arbeitsweise vorgeschlagen, dass die KMK zunächst direkt ein Gespräch mit Microsoft zu allen Kritikpunkten führt oder Microsoft mit Terminsetzung um die schriftliche Beantwortung aller aufgeworfenen Fragen bittet. Der TLfDI und die in der Arbeitsgruppe vertretenen Datenschutzaufsichtsbehörden stehen dabei der KMK beratend zur Seite.

1.8 Homeoffice in Pandemiezeiten

Im Rahmen der Bekämpfung der Corona-Pandemie wurden die Arbeitgeber nach der Corona-Arbeitsschutzverordnung dazu verpflichtet, ihren Beschäftigten Homeoffice anzubieten, sofern nicht zwingende betriebliche Gründe dem entgegenstehen. Der Verarbeitung personenbezogener Daten im häuslichen Bereich konnten allerdings auch datenschutzrechtliche Gründe entgegenstehen.

Mit der verstärkten Wahrnehmung von Homeoffice durch all jene Mitarbeiter, die nicht zwingend vor Ort arbeiten mussten, bestand teilweise das Problem, dass weder die erforderliche Hardware noch Verbindungen zum betrieblichen oder dienstlichen Server von heute auf morgen zur Verfügung standen. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) hat im Rahmen seiner Aufgabenwahrnehmung Anfragen insbesondere von öffentlichen Stellen hierzu beantwortet und Hinweise gegeben.

Homeoffice konnte als Telearbeit oder mobile Arbeit ausgestaltet werden, sofern die datenschutzrelevanten Vorgaben eingehalten werden konnten. Stand die Bearbeitung von Akten im häuslichen Umfeld zur Debatte, musste die verantwortliche Stelle entscheiden, ob auch in der Ausnahmesituation der Pandemiebekämpfung die Gefahren unbefugter Kenntnis und insbesondere der Verlust von sensiblen personenbezogenen Daten von Antragstellern und Dritten in Akten, die für die Bearbeitung erforderlich waren, beim Transport von der Dienststelle in den häuslichen Bereich und dort bei der Bearbeitung durch strenge technische und organisatorische Maßnahmen soweit minimiert werden konnten, dass man von einem angemessenen Schutz der personenbezogenen Daten im Sinne des Art. 5 Abs. 1 Buchstabe f) Datenschutz-Grundverordnung ausgehen konnte.
Zunächst war zu prüfen, ob die Voraussetzungen für einen häuslichen Arbeitsplatz beziehungsweise Telearbeit gegeben waren. Ein Punkt dabei ist, dass die Arbeitsaufgabe für Telearbeit/mobile Arbeit oder Homeoffice überhaupt geeignet sein muss, was bei der Verarbeitung besonders schützenswerter personenbezogenen Daten von der verantwortlichen Stelle einzuschätzen ist. Kommt die verantwortliche Stelle zu dem Schluss, dass Arbeitsplätze, an denen nur oder vorwiegend Papierakten bearbeitet werden, für die häusliche Bearbeitung nicht geeignet sind, weil die erforderlichen vorgeschriebenen technischen und organisatorischen Maßnahmen zum Schutz der zu verarbeitenden personenbezogenen Daten nicht ausreichend getroffen werden können, kann Telearbeit/Homeoffice/mobile Arbeit nicht genehmigt werden.
Weitergehende Informationen rund um das Thema „Telearbeit und Mobiles Arbeiten“ finden sich im 3. TB des TLfDI zum Datenschutz nach der DS-GVO (2020) unter Punkt 3. 22 ab Seite 112 und die veröffentlichten Ausführungen des TLfDI „pandemiebedingtes_Homeffice_.pdf“ vom 13. Januar 2021 https://www.tlfdi.de/search?tx_kesearch_pi1%5Bsword%5D=telearbeit im gleichlautenden Datenschutz-Wegweiser des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, herausgegeben im Juli 2020, veröffentlicht unter: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Flyer/Telearbeit.html.
Weitere Hinweise zu dem Thema finden sich beim Bundesamt für Sicherheit in der Informationstechnik, im „IT-Grundschutz-Kompendium“ (Stand 2021), hier ab Seite 231 „OPS.1.2.4: Telearbeit“ und ab Seite 775 „INF.8: Häuslicher Arbeitsplatz“, abrufbar unter:

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2021.pdf?__blob=publicationFile&v=6.

1.9 Maklertätigkeit und Auftragsverarbeitung – geht das zusammen?

Muss zur betrieblichen Altersvorsorge in Kooperation mit einem Maklerbüro mit diesem ein Auftragsverarbeitungsvertrag geschlossen werden?

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) erhielt von einem Unternehmen eine Anfrage, ob bei der betriebsinternen Umgestaltung zur betrieblichen Altersvorsorge mit einem Maklerbüro ein Auftragsverarbeitungsvertrag nach Art. 28 Datenschutz-Grundverordnung (DS-GVO) abgeschlossen werden muss. Hintergrund war, dass das Unternehmen den Mitarbeitern umfassende betriebliche Leistungen, insbesondere vermögenswirksame Leistungen und eine betriebliche Altersvorsorge (bAV) zur Verfügung stellte. Mit Wirkung des Reformpakets des Betriebsrentenstärkungsgesetzes seien die Arbeitgeber zu weiterführenden Leistungen im Bereich der bAV gesetzlich verpflichtet. Darin sei auch geregelt, dass über das grundlegende Angebot der bAV hinaus die vom Arbeitgeber eingesparten Sozialversicherungskosten dem Arbeitnehmer als Zuschuss gewährt werden müssen. Kompliziert sei dies im Unternehmen, da auch Altverträge, die eine Entgeltumwandlung des Arbeitnehmers beinhalten, von dieser Vorgabe nachträglich partizipieren sollen. Das bedeute, dass der jahrealte Bestand angefasst werden müsse.
Um die Verwaltung und den Informationsfluss im Sinne der Mitarbeiter und des Unternehmens künftig zu verbessern, sollte ein Portal eines Cloud-Anbieters zur Administration aller bestehenden und neuen bAV-Verträge eingesetzt werden. Sowohl die Mitarbeiter als auch die zugehörigen Versicherungsgesellschaften hätten für ihre eigenen Verträge Zugang auf die entsprechenden Daten. Hierzu wären bereits Auftragsverarbeitungsverträge geschlossen worden. Nun sei vorgesehen, in Zusammenarbeit mit einem Maklerbüro eine umfassende Versorgungsordnung zu erstellen. Dieses Werk solle dann die Grundlage für die Auswahl künftiger Versicherungen bilden.

Ein Makler war bereits gefunden. Er sollte ein Mandat für eine umfassende Beratung, Versorgung und Betreuung auf diesem Gebiet erhalten. Er sollte als Dienstleister des Unternehmens weisungsunabhängig agieren, sich als organisatorisch frei verstehen. Er sollte Zugang auf das Portal bekommen, um die vorhandenen Verträge prüfen zu können. Das Unternehmen stellte nun die Frage, ob mit dem Makler ein separater Auftragsverarbeitungsvertrag geschlossen werden müsse. Der Portalanbieter habe diese Notwendigkeit nicht gesehen.
Der TLfDI teilte dem Unternehmen mit, dass die Verarbeitung von Beschäftigtendaten nach § 26 Abs. 1 Bundesdatenschutzgesetz zulässig ist, wenn sie für die Begründung, Durchführung oder Beendigung eines Beschäftigtenverhältnisses oder zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung (Kollektivvereinbarung) ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten erforderlich ist. Die Datenverarbeitung bezieht sich jedoch ausschließlich auf die Verarbeitung des jeweils Verantwortlichen, also des Arbeitgebers. Werden die Daten an einen Makler übermittelt und dort verarbeitet, ist dieser grundsätzlich Dritter nach Art. 4 Nr. 10 DS-GVO. Eine Datenweitergabe an Dritte außerhalb des Unternehmens bedarf einer ausdrücklichen Rechtfertigung. Diese kann mit einem bestehenden Vertrag über die Auftragsdatenverarbeitung vorliegen. In diesem Fall wäre der Makler nicht mehr Dritter im Sinne der DS-GVO.
Ob eine datenverarbeitende Stelle als Verantwortlicher im Sinne des Art. 4 Nr. 7 DS-GVO oder als Auftragsverarbeiter eingestuft werden kann, ist auch wesentlich auf der Grundlage der Definition des Verantwortlichen zu beurteilen. Danach ist Verantwortlicher die natürliche oder juristische Person, die über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Ein Auftragsverarbeiter ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet (Art. 4 Nr. 8 DS-GVO). Letztlich kommt es darauf an, ob dem Empfänger der personenbezogenen Daten auch ein Entscheidungsspielraum hinsichtlich der Zwecke und Mittel der Datenverarbeitung zustehen soll oder nicht. Das Working-Paper 169 der Art. 29-Datenschutzgruppe führt hierzu aus, dass insbesondere dann, wenn eine Stelle Entscheidungen über Fragen trifft, die den Kern der Rechtmäßigkeit der Verarbeitung betreffen, als Verantwortlicher einzuordnen ist. Wesentlich ist beispielsweise, wer darüber entscheidet, wie lange Daten aufbewahrt werden, wer Zugang zu

den Daten hat, was damit geschehen soll oder ob die Verarbeitung zu eigenem Nutzen erfolgen soll. Wenn auch eigene Interessen seitens des Dienstleisters verfolgt werden, ist davon auszugehen, dass dieser als eigener Verantwortlicher handelt und eine Rechtsvorschrift die Übermittlung der Daten an diesen rechtfertigen muss.
Es ist anhand der Umstände des Einzelfalls zu bestimmen, ob der Makler als eigener Verantwortlicher oder Auftragsverarbeiter handelt. Der TLfDI ist nicht der Auffassung, dass es sich bei der Maklertätigkeit immer um eine weisungsfreie Tätigkeit handelt. Im Rahmen der reinen Vermittlungstätigkeit wird der Versicherungsmakler seitens des TLfDI als eigener Verantwortlicher eingeordnet. Vorliegend soll der Makler Zugriff auf die im Unternehmen genutzte Beraterplattform und somit auf sämtliche Beschäftigtendaten (Lohn- und Gehaltsabrechnung, Sozialversicherungsdaten, Bankdaten et cetera) Zugriff haben. Sofern der Makler die Verwaltung der einzelnen Altersvorsorgeverträge übernehmen soll, wird er umfassend in die Unternehmensstruktur eingebunden. Inwieweit hier Entscheidungsspielräume bleiben, kann nur anhand der Struktur des abgeschlossenen Maklervertrages beurteilt werden. Nach der geschilderten Fallkonstellation war jedoch nicht davon auszugehen, dass die personenbezogenen Daten der Beschäftigten seitens des Maklers zu eigenen Zwecken verwendet werden dürfen. Damit ist der Abschluss eines Auftragsverarbeitungsvertrags erforderlich.
Wenn der Makler zur Schaffung der Versorgungsordnung beziehungsweise Erfüllung des geschlossenen Maklervertrages Zugang zu den Daten benötigt, so muss in einem Auftragsverarbeitungsvertrag eindeutig geklärt werden, mit welchen Handlungsbefugnissen er bezüglich dieser Daten ausgestattet ist.

1.10 Auswirkungen der Corona-Pandemie auf die Verarbeitung von Beschäftigtendaten

Im Zuge der Maßnahmen zur Corona-Pandemiebekämpfung wurden insbesondere mit den Änderungen im Infektionsschutzgesetz (IfSG) zur Verarbeitung personenbezogener Daten kurzfristig gesetzliche Regelungen geschaffen, die auch kurzfristig umzusetzen waren. Unsicherheiten und Irrtümer bei der Verarbeitung von Gesundheitsdaten der Beschäftigten durch die hierzu verpflichteten Arbeitgeber vor Ort waren damit – man kann schon fast sagen – vorprogrammiert.

Der Tätigkeitsberichtszeitraum war geprägt von ansteigenden und fallenden Corona-Inzidenzzahlen mit Lockdown, Maskenpflicht, Absonderung/Quarantäne, 2G- und 3G-Regelungen am Arbeitsplatz, möglichen Lockerungen und damit jeweils verbunden Verarbeitungen von Gesundheitsdaten der Beschäftigten in verschiedener Hinsicht. Dies zog eine Unmenge von Beschwerden und Anfragen betroffener Personen sowie Beratungsanfragen von Verantwortlichen beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) als Datenschutzaufsicht nach sich.
Festzustellen war, dass immer dann, wenn die Bundesregierung eine Einigung zur Verschärfung oder Lockerung der Maßnahmen erzielte, bereits ohne das konkrete Vorliegen gesetzlicher Regelungen sich insbesondere Arbeitgeber darauf schnellstmöglich einstellen wollten und schon einmal interne Festlegungen trafen, die teilweise über das Ziel hinausschossen. Einerseits verständlich, denn im Angesicht der Pandemie war es wichtig, dass den Verpflichtungen schnellstmöglich nachgekommen wurde. Andererseits sorgte dies auch für Unverständnis der von (vorgesehenen) Datenverarbeitungen Betroffenen, weil der Arbeitgeber nun plötzlich mit Angaben im Impf-, Genesenen- und Testnachweis Gesundheitsdaten in einem nie dagewesenen Umfang verarbeiten dürfen sollte. Unzählige Anfragen per Telefon und E-Mail von Beschäftigten öffentlicher und nicht-öffentlicher Stellen an den TLfDI, denen Gerüchte oder schon konkrete Vorhaben zu Ohren gekommen waren, waren an der Tagesordnung. Aber auch der TLfDI war darauf angewiesen, dass die gesetzlichen Regelungen oder die Ausführungen in den Bundes- oder Landesverordnungen hierzu zur Verfügung standen, um die Vorhaben und Vorbereitungen oder vorgreifend bereits tatsächlich durchgeführten Verarbeitungen der Beschäftigtendaten auf Rechtmäßigkeit überprüfen zu können. Die personellen Kapazitäten beim TLfDI reichten allerdings nicht aus, flächendeckende Überprüfungen vorzunehmen.
Die Konferenz der unabhängigen Datenschutzaufsichtsaufsichtsbehörden des Bundes und der Länder (DSK) hat nach vorherigen allgemeinen Beschlüssen zum Umgang mit Gesundheitsdaten im Rahmen der Pandemie-Bekämpfung im Dezember 2021 eine Anwendungshilfe für den praktischen Vollzug als Hilfestellung zur Verarbeitung von Beschäftigtendaten im Zusammenhang mit der Corona-Pandemie im Anwendungsbereich der Datenschutz-Grundverordnung veröffentlicht (https://www.datenschutzkonferenz-online.de/media/oh/20211220_oh_dsk_anwendungshilfe.pdf). Damit sollten die

bis dahin bekannt gewordenen Fragen und Probleme beantwortet werden. Mit Stand vom 9. Dezember 2021 hat der TLfDI darüber hinaus weitere FAQ veröffentlicht (https://www.tlfdi.de/fileadmin/tlfdi/datenschutz/Corona-Pandemie_und_DS/211209_FAQ_TLfDI.pdf), insbesondere zu dem mit den zum 24. November 2021 in Kraft getretenen Änderungen zum Infektionsschutzgesetz (IfSG) hinsichtlich des Betretungsverbots für die Arbeitsstätte durch Beschäftigte nach dem § 28b IfSG, die den 3G-Status nicht nachweisen konnten. (Anmerkung: Die Regelungen sind im Übrigen seit Frühjahr 2022 wieder entfallen.) Dies war insbesondere aus dem Grund angezeigt, weil Arbeitgeber bei der Dokumentation der Vorlage der Nachweise auf Nummer sicher gehen wollten und deshalb verbreitet Kopien der vorzulegenden Dokumente verlangten. Die Dokumente mussten jedoch nur **vorgelegt** werden und es durfte lediglich festgehalten werden, dass eine Vorlage geeigneter Nachweise stattgefunden hatte. Diese Dokumentation meist in Listenform zum Abhaken, durfte auch nur sehr kurzfristig aufbewahrt werden und konnte bereits am folgenden Tag der Löschung unterfallen. Lediglich in den Fällen, in denen Beschäftigte nicht täglich ihren Impf- oder Genesenennachweis vorlegen wollten und von der Möglichkeit der „Hinterlegung“ Gebrauch machten, konnte darüber hinaus ein Verfallsdatum gespeichert werden und die Angaben bis zum Wegfall der Vorlagefrist (Ende März 2022) aufbewahrt werden. Da es auch hierzu immer wieder Missverständnisse und Nachfragen gab, hat der TLfDI auch zum Herunterladen ein Muster für die Hinterlegung nach § 28b IfSG veröffentlicht, das individuell angepasst werden konnte.

Ein weiteres Beispiel:

In Anbetracht einer damaligen rückläufigen Entwicklung des Infektionsgeschehens hatte ein Arbeitgeber die (teilweise) Befreiung von der Maskenpflicht am Arbeitsplatz für Personen mit den sogenannten 3G-Merkmalen – geimpft, genesen, getestet – vorgesehen unter der Bedingung, dass die übrigen Hygieneschutzmaßnahmen (Abstand, Desinfektion, ausreichende Größe der Räume, Spuckschutz und Lüftung) eingehalten werden. Per Aushang informierte man die Beschäftigten, sie könnten dafür den jeweiligen Bereichsleiter auf freiwilliger Basis über das Vorliegen der drei Voraussetzungen informieren, um einen sogenannten 3G-Ausweis zu erhalten. Das ginge ohne jegliche Verarbeitung der personenbezogenen Daten des jeweils betreffenden Mitarbeiters, also datenschutzrechtlich völlig unproblematisch. In der Tat wäre mangels Verarbeitung personenbezogener Daten damit auch

keine datenschutzrechtliche Problematik verbunden gewesen. Das wäre aber nur dann der Fall gewesen, wenn weder die Informationen „ich bin geimpft, genesen oder getestet“ personenbezogen verarbeitet werden, noch in entsprechende Nachweise Einsicht genommen wird. Der angesprochene Ausweis müsste also auf Zuruf „ich möchte einen 3G-Ausweis!“ ohne jegliche Nachprüfung, ob die Voraussetzung bei dem Mitarbeiter vorliegt, ausgestellt werden. Selbst die Ausgabe der Ausweise dürfte nicht erfasst oder dokumentiert werden. Der Ausweis selbst dürfte auch nicht namentlich ausgestellt werden und könnte von jedem genutzt werden. Alle diese Vorgänge wären jedoch als Verarbeitung personenbezogener Daten zu bewerten. Sollte eine der genannten Datenverarbeitungen stattfinden, zum Beispiel eine Nachprüfungsmöglichkeit vorgesehen werden, bedürfte dies einer Rechtsgrundlage.
Nach § 26 Abs. 1 Bundesdatenschutzgesetz (BDSG) ist die Verarbeitung personenbezogener Daten Beschäftigter zulässig, wenn dies für die Durchführung des Beschäftigungsverhältnisses oder sich aus einem Gesetz oder einer Betriebsvereinbarung ergebenden Rechte und Pflichten der Interessensvertretung der Beschäftigten erforderlich ist. Eine Erforderlichkeit für die Erhebung und Verarbeitung eines „3G-Status“ und der Ausstellung eines 3G-Ausweises zur Durchführung des Beschäftigungsverhältnisses sah der TLfDI zum damaligen Zeitpunkt nicht. Auch das Infektionsschutzgesetz sah hierzu keine Verpflichtung vor. Eine Betriebsvereinbarung, die die Verarbeitung von Beschäftigtendaten in diesem Zusammenhang und die den Umgang mit den genau zu bezeichnenden Kategorien von personenbezogenen Daten zum Gegenstand hatte, lag ebenfalls nicht vor.
Insoweit wäre die Verarbeitung der personenbezogenen Daten nur auf der Grundlage einer inhaltlich und formell den Anforderungen genügenden Einwilligung der Betroffenen denkbar gewesen (vgl. § 26 Abs. 2 BDSG, auch Kurzpapier Nr. 14 der DSK, abzurufen unter https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_14.pdf). Die Wirksamkeit einer Einwilligung im Beschäftigungsverhältnis setzt voraus, dass die Betroffenen ausführlich über den Zweck und die Verarbeitung personenbezogener Daten sowie über die Möglichkeit des jederzeitigen Widerrufs informiert sind (sogenannte informierte Einwilligung). Die Einwilligung muss zudem aktiv in Schriftform (soweit nicht wegen besonderer Umstände eine andere Form angemessen ist) erteilt und dokumentiert werden. Dabei ist auch § 26 Abs. 3 BDSG in Verbindung mit Art. 9 Abs. 1 DS-GVO

zu beachten, da es sich bei den Angaben zum Impfstatus, „genesen“ oder „aktuell getestet“ um Gesundheitsdaten und damit um besondere Kategorien von Daten handelt.
Davon hat man aber doch Abstand genommen oder die tatsächlichen Gegebenheiten, die eine Lockerung zugelassen hätten, hatten sich zwischenzeitlich wieder geändert.

1.11 Bußgeldverfahren beim TLfDI

Vom Anfangsverdacht über den Bußgeldbescheid bis hin zum Urteil – die einzelnen Verfahrensabschnitte eines Bußgeldverfahrens sind so vielschichtig, wie die ihm zugrundeliegenden Fälle. Das Verfahren verfolgt dabei ebenso wie das Verwaltungsverfahren in erster Linie die Sachverhaltsaufklärung.

Im Berichtszeitraum entdeckte der Hauswart eines Studentenwohnheimes in Thüringen in den zu der Einrichtung gehörenden Papiercontainern, welche öffentlich zugänglich und nicht verschlossen waren, unverschlossene Pappkartons und Papiertüten, die mit insgesamt 675 vollständigen Patientenakten einer Arztpraxis für Allgemeinmedizin gefüllt waren. Nachdem die zuständige Staatsanwaltschaft das Ermittlungsverfahren in dieser Angelegenheit wegen des Verdachts der Verletzung von Privatgeheimnissen nach § 203 Strafgesetzbuch gemäß § 170 Abs. 2 Strafprozessordnung (StPO) eingestellt und die Sache gemäß § 43 Abs. 1 Ordnungswidrigkeitengesetz (OWiG) an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) abgegeben hatte, wurde umgehend ein Bußgeldverfahren gegen den Arzt als Verantwortlichen gemäß Art. 4 Nr. 7 Datenschutz-Grundverordnung (DS-GVO) eingeleitet.
Der TLfDI ist gemäß § 61 Abs. 1 und 6 Thüringer Datenschutzgesetz (ThürDSG) zuständig für die Verfolgung von Ordnungswidrigkeiten nach Art. 83 DS-GVO in Verbindung mit § 41 Abs. 1 Bundesdatenschutzgesetz (BDSG) sowie nach dem ThürDSG selbst, soweit die Ordnungswidrigkeiten gemäß § 37 Abs. 1 Ziffer 1 OWiG im Freistaat Thüringen begangen wurden. Hierbei ist der TLfDI in der Regel auf die Verfolgung von Ordnungswidrigkeiten im nicht-öffentlichen Bereich beschränkt, da der Thüringer Gesetzgeber auf Grundlage der Regelungsbefugnis des Art. 83 Abs. 7 DS-GVO mit § 61 Abs. 4 ThürDSG bestimmt hat, dass gegen öffentliche Stellen keine Geldbußen verhängt werden. Von diesem Privileg sind lediglich diejenigen

öffentliche Stellen ausgenommen und damit der Privatwirtschaft gleichgesetzt, die am Wettbewerb teilnehmen, vergleiche § 26 ThürDSG. Auch ist nach § 61 Abs. 1 ThürDSG als weitere Ausnahme die Verhängung von Geldbußen gegenüber Mitarbeitern öffentlicher Stellen möglich, wenn diese vorsätzlich im Zusammenhang mit dienstlichen Zwecken gegen das Datenschutzrecht verstoßen. Verstoßen Mitarbeiter öffentlicher Stellen hingegen zu eigenen (privaten) Zwecken gegen datenschutzrechtliche Regelungen, werden diese Mitarbeiter als eigene Verantwortliche nach den Regelungen der DS-GVO verfolgt, da sie durch ihr Handeln selber Mittel und Zwecke der Datenverarbeitung festgelegt haben, Art. 4 Nr. 7 DS-GVO (sogenannter Exzess).

Doch nicht immer kommt es vor, dass – wie im Fall des Arztes – zunächst die Thüringer Staatsanwaltschaften Ermittlungsverfahren wegen Straftaten gegen Verantwortliche durchführen und nach deren Einstellung die Verfahren an den TLfDI zur Verfolgung einer Ordnungswidrigkeit abgeben. Häufig gehen die Bußgeldverfahren beim TLfDI auch auf Ordnungswidrigkeitenanzeigen zurück, die betroffene Personen bei der Polizei eingereicht haben und die von dieser zuständigkeitshalber an den TLfDI abgegeben werden. Auch kommt es vor, dass Bußgeldverfahren auf Grundlage von (anonymen) Anzeigen eingeleitet werden, die direkt per E-Mail oder postalisch beim TLfDI eingehen. Oftmals werden Ordnungswidrigkeitenverfahren auch einfach im Anschluss an Verwaltungsverfahren, die durch den TLfDI selbst bearbeitet wurden, eingeleitet.

Im Verwaltungsverfahren überwacht der TLfDI unter anderem die Einhaltung der Vorschriften über den Datenschutz und setzt die Anwendung der entsprechenden Normen durch (Art. 57 Abs. 1 Buchstabe a) DS-GVO, § 6 Abs. 2 Nr. 1 ThürDSG). Voraussetzung für die Durchführung eines Verwaltungsverfahrens ist die Kenntnis von einem möglichen datenschutzrechtlichen Verstoß. Diese Kenntnis erlangt der TLfDI entweder selbst oder aufgrund einer Beschwerde der von der Datenverarbeitung betroffenen Person (Art. 77 DS-GVO, § 8 ThürDSG). Sodann wird der Sachverhalt nach dem Untersuchungsgrundsatz gemäß § 24 des Thüringer Verwaltungsverfahrensgesetzes (ThürVwVfG) von Amts wegen ermittelt. Hierbei greift der TLfDI auf die Untersuchungsbefugnisse nach Art. 58 Abs. 1 DS-GVO und hierbei insbesondere auf das „Auskunftsersuchen“ zurück. So hat der TLfDI das Recht, den Verantwortlichen oder den Auftragsverarbeiter

gemäß Art. 58 Abs. 1 Buchstabe a) DS-GVO anzuweisen, alle Informationen bereitzustellen, die für die Erfüllung der Aufgaben einer Aufsichtsbehörde erforderlich sind. Zudem hat nach § 40 Abs. 4 BDSG die der Aufsicht unterliegende Stelle der Aufsichtsbehörde auf Verlangen die für die Erfüllung ihrer Aufgaben erforderlichen Auskünfte zu erteilen. In der Praxis werden aber auch häufig Datenschutzüberprüfungen hinsichtlich des Datenschutz- und Datensicherheitsniveaus gemäß Art. 58 Abs. 1 Buchstabe b) DS-GVO durchgeführt, mit denen die technisch-organisatorischen Maßnahmen und das Sicherheitskonzept überprüft werden. Zur aufsichtsbehördlichen Tätigkeit des TLfDI gehört aber auch der Zugang zu den Geschäftsräumen, einschließlich der Datenverarbeitungsanlagen und -geräte (Art. 58 Abs. 1 Buchstabe f) DS-GVO). Dementsprechend sind anlasslose Überprüfungen grundsätzlich möglich und für eine wirksame Anwendung und Durchsetzung der DS-GVO sogar geboten. Kommt der TLfDI schließlich zu dem Ergebnis, dass Verstöße gegen die Vorschriften über den Datenschutz oder sonstige Mängel bei der Verarbeitung personenbezogener Daten einer Behörde vorliegen, teilt er dies dem Verantwortlichen oder Auftragsverarbeiter vor Ausübung der nachfolgend exemplarisch ausgesuchten Befugnisse gemäß Art. 58 Abs. 2 DS-GVO mit und fordert diesen in einer angemessenen Frist zur Stellungnahme auf. Wenn der TLfDI die zur Verfügung stehenden Abhilfebefugnisse ergreift, müssen die rechtsverbindlichen Maßnahmen nach Erwägungsgrund 129 formale Voraussetzungen erfüllen. Jede Person wird vor dem Erlass einer Maßnahme mit nachteiligen Auswirkungen gemäß § 28 ThürVwVfG grundsätzlich angehört. Überflüssige Kosten und übermäßige Unannehmlichkeiten für die Betroffen werden vermieden. Die Maßnahmen (Verwaltungsakte) des TLfDI werden schriftlich erlassen und darüber hinaus klar und eindeutig formuliert. Darin muss das Datum, an dem die Maßnahme erlassen wurde, angegeben werden und das Schreiben muss vom Leiter oder einem von ihm bevollmächtigten Mitglied der Aufsichtsbehörde unterschrieben sein. Die Entscheidung des TLfDI enthält zudem eine Begründung für die getroffenen Maßnahmen sowie einen Hinweis auf das Recht eines wirksamen Rechtsbehelfs, denn die Maßnahme ist gerichtlich überprüfbar. Zu den am häufigsten angewendeten Abhilfebefugnissen zählt die Verwarnung gemäß Art. 58 Abs. 2 Buchstabe b) DS-GVO. Sie kann als Ermahnung verstanden werden und wird vom TLfDI in den Fällen ausgesprochen, in denen ein unerheblicher Verstoß gegen die DS-GVO festgestellt wurde. **Die Verwarnung stellt**

eine Vorstufe zu den nachfolgenden Abhilfebefugnissen dar und darf keinesfalls mit einer bußgeldrechtlichen Verwarnung nach § 56 OWiG, welche weiter unten näher erläutert wird, verwechselt werden. Mit Anweisungen gemäß Art. 58 Abs. 2 Buchstabe c) DS-GVO, Anträgen von Betroffenen zu entsprechen, können die Betroffenenrechte (zum Beispiel Auskunftsanspruch nach Art. 15 DS-GVO, Löschanspruch nach Art. 17 DS-GVO und Widerspruchsrecht nach Art. 21 DS-GVO) direkt durchgesetzt werden. Der TLfDI kann aber gemäß Art. 58 Abs. 2 Buchstabe d) DS-GVO auch Anweisungen treffen, wie bestimmte Verarbeitungsvorgänge auszuführen sind, oder gemäß Art. 58 Abs. 2 Buchstabe f) DS-GVO auch eine vorübergehende oder endgültige Beschränkung der Verarbeitung verhängen. Schließlich können zusätzlich oder anstelle der vorgenannten Maßnahmen gemäß Art. 58 Abs. 2 Buchstabe i) DS-GVO auch Geldbußen nach Art. 83 DS-GVO verhängt werden. Vor der Verhängung einer Geldbuße muss jedoch zunächst das Verfahren eingeleitet werden.
Ob ein solches Bußgeldverfahren eingeleitet wird, hängt davon ab, ob gemäß § 152 Abs. 2 StPO in Verbindung mit § 46 Abs. 1 OWiG zureichende tatsächliche Anhaltspunkte für eine Ordnungswidrigkeit vorliegen, also ein Anfangsverdacht besteht. Aufgrund des im deutschen Ordnungswidrigkeitenrecht geltenden Opportunitätsgrundsatzes gemäß § 47 Abs. 1 Satz 1 OWiG steht die Einleitung des Bußgeldverfahrens im pflichtgemäßen Ermessen der Verwaltungsbehörde. Sie entscheidet insoweit, ob die Ahndung einer Ordnungswidrigkeit im öffentlichen Interesse geboten ist. Ob der Opportunitätsgrundsatz auch im datenschutzrechtlichen Bußgeldverfahren zur Anwendung kommt, ist in Literatur und Rechtsprechung höchst umstritten. Nach der ablehnenden Meinung kann die Aufsichtsbehörde nicht nach dem Opportunitätsprinzip entscheiden, ob sie bußgeldbewährte Verstöße gegen die DS-GVO verfolgt und Geldbußen verhängt oder nicht. Begründet wird diese Ansicht mit dem Gesetzgebungsverfahren und dem Wortlaut des Art. 83 Abs. 2 Satz 1 DS-GVO und des Erwägungsgrundes 148 Satz 1, wonach die Verhängung von Geldbußen verpflichtend sei und sogar sonstigen Maßnahmen nach Art. 58 Abs. 2 DS-GVO vorgehe. Obgleich die Vertreter dieser Meinung anerkennen, dass mit der Verhängung einer Geldbuße allein noch kein rechtmäßiger Zustand hergestellt ist, so meinen sie auch, dass dies als Entscheidung des Gesetzgebers hinzunehmen sei. Eine genaue Analyse der Entwurfsfassungen der DS-GVO und des heutigen Wortlauts würde zeigen, dass die Formulierungen in den Absätzen 2, 4, 5 und 6 des

Art. 83 DS-GVO („werden verhängt“) tatsächlich eine bewusste Entscheidung des Gesetzgebers für eine verpflichtende Verhängung von Geldbußen und kein Redaktionsversehen darstellen. Eine noch in der Entwurfsfassung enthaltene Formulierung, dass eine Geldbuße verhängt werden „kann“, habe sich schließlich nicht durchgesetzt. Eine Ausnahme hiervon bilden lediglich diejenigen Fälle, in denen ein geringfügiger Verstoß festgestellt wurde oder die zu verhängende Geldbuße eine unverhältnismäßige Belastung für eine natürliche Person bewirken würde. In diesen Fällen kann die Aufsichtsbehörde nach Erwägungsgrund 148 Satz 2 anstelle einer Geldbuße eine Verwarnung erteilen. Demgegenüber geht die zustimmende Meinung davon aus, dass die Aufsichtsbehörden bei der Verhängung von Geldbußen sehr wohl in weitem Umfang Ermessen walten lassen können und bejaht die Anwendbarkeit des Opportunitätsprinzips. Begründet wird diese Meinung zunächst damit, dass dem Wortlaut des Art. 83 Abs. 2 S. 1 DS-GVO keine klare Verpflichtung zur Ahndung eines Verstoßes mit einer Geldbuße zu entnehmen sei beziehungsweise dass er in seiner Formulierung nicht eindeutig sei. Hieran ändere auch die Formulierung in Erwägungsgrund 148 S. 2 „kann anstelle einer Geldbuße eine Verwarnung erteilt werden“ im Kontext des Wortlauts des Art. 83 Abs. 2 S. 1 DS-GVO nichts, der den Eindruck erwecke, dass der Aufsichtsbehörde nur ein Auswahlermessen hinsichtlich der Höhe eines Bußgeldes und nicht ein Entschließungsermessen hinsichtlich der Verfolgung mittels Geldbuße als solche zukommen solle. Begründet wird dies mit Erwägungsgrund 150 S. 1, wonach jede Aufsichtsbehörde nur „befugt sein (sollte)“ Geldbußen zu verhängen. Die zustimmende Meinung weist zudem auf den Wortlaut des beziehungsweise die Verweisung in Art. 58 Abs. 2 Buchstabe i) auf Art. 83 DS-GVO hin, wonach die Aufsichtsbehörde neben oder gar anstelle einer Geldbuße ihre übrigen Befugnisse ausüben könne. Die Geldbuße stünde daher als Sanktionsmittel neben den sonstigen Befugnissen der Aufsichtsbehörde. Mit dieser Thematik setzt sich zurzeit im Kern auch der Europäische Gerichtshof auseinander, nachdem sich das Verwaltungsgericht Wiesbaden im Rahmen eines Vorabentscheidungsverfahrens zum Aktenzeichen c-768/21 EuGH an diesen gewandt hatte. Hierbei geht es um die Frage, ob Art. 57 Abs. 1 Buchstaben a) und f) sowie Art. 58 Abs. 2 Buchstabe a) bis j) in Verbindung mit Art. 77 Abs. 1 DS-GVO dahingehend auszulegen sind, dass die Aufsichtsbehörde im Falle der Feststellung der Verletzung der Rechte eines Betroffenen durch eine Datenverarbeitung stets verpflichtet ist, nach

Art. 58 Abs. 2 DS-GVO einzuschreiten. Bis zum Vorliegen einer abschließenden Entscheidung wird daher beim TLfDI bei jedem festgestellten Verstoß immer eine Maßnahme nach Art. 58 Abs. 2 DS-GVO ergriffen.
Da die Verfahrenseinleitung nicht auf die Ahndung, sondern auf die Sachverhaltsaufklärung gerichtet ist, der dann die Ahndung folgen kann, reichen in der Regel relativ geringe Anforderungen an den Anfangsverdacht aus. Dieser war im Fall des Arztes zu bejahen, da die aufgefundenen Patientenakten aufgrund ihres Inhaltes einen direkten Bezug zu der Arztpraxis des Verantwortlichen aufwiesen und eine Rechtmäßigkeit der Entsorgung der Akten auf diesem Wege de facto ausgeschlossen war.
Nach Einleitung des Ordnungswidrigkeitenverfahrens geht der TLfDI den Anhaltspunkten für das Vorliegen einer Ordnungswidrigkeit im sogenannten Vorverfahren nach. Ziel des Verfahrens ist die Feststellung, ob eine Bußgeldentscheidung zu erlassen oder das Verfahren einzustellen ist. Hierfür wird beim TLfDI ein Ermittlungsverfahren nach den Grundsätzen des Strafverfahrens durchgeführt, welches in sinngemäßer Anwendung des § 160 StPO im Wesentlichen der Aufklärung des Sachverhalts und der Beweissicherung dient. Obgleich der Gesetzgeber eine freie Gestaltung des Ermittlungsverfahrens vorsieht, wird in aller Regel auf Ermittlungshandlungen wie die Vernehmung von Zeugen, auf die Auskünfte anderer Behörden oder die Beiziehung entsprechender Akten zurückgegriffen. Eher selten ist dagegen die Beschlagnahme von Beweisgegenständen oder gar die Durchsuchung beim Betroffenen anzutreffen, obgleich der TLfDI die Möglichkeit hat, hiervon Gebrauch zu machen und diese Maßnahmen, wenn notwendig, auch einsetzt. Soweit erforderlich, stehen auch die Technikexperten des entsprechenden Referats beim TLfDI mit Rat und Tat zur Seite, geben Stellungnahmen ab und sichern Beweise. Da die zuständige Kriminalpolizeiinspektion im Fall des Arztes bereits Zeugen vernommen und die Patientenakten umfassend ausgewertet und im Anschluss und nach Rücksprache mit der Staatsanwaltschaft einer datenschutzkonformen Entsorgung zugeführt hatte, konnte der TLfDI auf die so gewonnenen Erkenntnisse unmittelbar zurückgreifen und den Fall einer umfassenden rechtlichen Würdigung unterziehen.
Das Vorverfahren endet beim TLfDI schließlich – je nach Ergebnis der durchgeführten Ermittlungen – mit der Einstellung des Bußgeldverfahrens, einer Verwarnung nach § 56 OWiG, wenn diese zulässig oder geboten ist oder mit dem Erlass eines Bußgeldbescheides. Gemäß

§ 41 Abs. 2 Satz 2 BDSG finden bei Bußgeldverfahren wegen Verstößen gegen die Art. 83 Abs. 4 bis 6 DS-GVO unter anderem die Vorschriften der §§ 56 bis 58 OWiG (Verwarnung durch die Verwaltungsbehörde) keine Anwendung. Die Erteilung einer Verwarnung nach dem OWiG ist daher bei DS-GVO-Bußgeldverfahren ausgeschlossen. Im Gegensatz zum Bundesgesetzgeber (BDSG) hat der Thüringer Gesetzgeber im ThürDSG die Anwendbarkeit der §§ 56 bis 58 OWiG gerade nicht ausgeschlossen. Hierbei ist zu beachten, dass die Adressaten des Bundesdatenschutzgesetzes gemäß § 1 Abs. 1 Satz 1 Nr. 1 BDSG die öffentlichen Stellen des Bundes (zum Beispiel Behörden, Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen des Bundes) sowie gemäß § 1 Abs. 1 Satz 2 BDSG mit einigen Einschränkungen die nicht-öffentlichen Stellen (privater Bereich) sind. Dementsprechend gelangt bei DS-GVO-Bußgeldverfahren, die sich ausschließlich gegen die nicht-öffentlichen Stellen richten können, das BDSG zur Anwendung, womit – wie zuvor beschrieben – einige Regelungen des Ordnungswidrigkeitengesetzes nicht angewendet werden. Im Gegensatz dazu richtet sich das Thüringer Datenschutzgesetz gemäß § 2 Abs. 1 ThürDSG an die öffentlichen Stellen des Landes (zum Beispiel Behörden und Gerichte des Landes). Entsprechende Bußgeldverfahren nach § 61 ThürDSG, bei denen die Möglichkeit der Erteilung einer Verwarnung nicht ausgeschlossen ist, werden wegen der Regelung in § 61 Abs. 4 ThürDSG entweder gegen die Bediensteten der öffentlichen Stellen oder gegen diejenigen öffentlichen Stellen geführt, die am Wettbewerb teilnehmen. Voraussetzungen für eine Verwarnung ist, dass die begangene Ordnungswidrigkeit als geringfügig einzuordnen ist. Dies richtet sich nach der Bedeutung der Handlung und dem Grad der Vorwerfbarkeit, wobei die Gesamtbetrachtung entscheidet (vgl. Gürtler in Göhler / Ordnungswidrigkeitengesetz, 17. Aufl. 2017, § 56 Rn. 6). Da aber wegen der Regelung in § 10 OWiG nur vorsätzliches Handeln nach dem ThürDSG als Ordnungswidrigkeit geahndet werden kann, ist die Verwarnung in aller Regel nicht das Mittel der Wahl.
Ergeben die Ermittlungen keinen zum Erlass eines Bußgeldbescheides hinreichenden Tatverdacht gegen den Betroffenen, kann also die Unschuldsvermutung nicht widerlegt werden, so ist das Bußgeldverfahren aus tatsächlichen Gründen gemäß § 170 Abs. 2 Satz 1 StPO in Verbindung mit § 46 Abs. 1 OWiG einzustellen. Möglich, in der Praxis aber weitaus weniger relevant ist darüber hinaus auch eine Einstellung des Verfahrens aus rechtlichen Gründen wegen des Bestehens

eines dauernden Verfolgungshindernisses. Wichtigstes Beispiel ist in diesem Zusammenhang der Eintritt der Verfolgungsverjährung.
Im Fall des Arztes kam keiner der vorgenannten Einstellungsgründe in Betracht, da insbesondere auch Gesundheitsdaten in erheblichem Umfang verarbeitet worden waren und der Tatnachweis praktisch als gesichert galt.
Kommt im Bußgeldverfahren weder eine Einstellung noch eine Verwarnung in Betracht, ergeht gegen den Betroffenen nach vollständiger Aufklärung des Sachverhalts ein Bußgeldbescheid mit entsprechender Festsetzung der Geldbuße. Dem Betroffenen ist allerdings vor Erlass einer Bußgeldentscheidung gemäß § 55 Abs. 1 OWiG, § 163a Abs. 1 StPO Gelegenheit zu geben, sich zur Beschuldigung zu äußern. Die Anhörung soll dem Betroffenen die Möglichkeit des rechtlichen Gehörs zum Tatvorwurf der Ordnungswidrigkeit und bezüglich der Rechtsfolgen zu seiner wirtschaftlichen Leistungsfähigkeit geben. Der Arzt hatte hiervon Gebrauch gemacht und die Ordnungswidrigkeit im Rahmen der Anhörung gegenüber dem TLfDI vollumfänglich eingeräumt und sich für die nicht datenschutzkonforme und damit unrechtmäßige Entsorgung der Patientenakten entschuldigt. Dies wurde bei der Zumessung der Geldbuße durch den TLfDI, welcher gemäß Art. 83 Abs. 5 DS-GVO Geldbußen bis zu einer Höhe von 20.000.000 Euro beziehungsweise im Falle von Unternehmen bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres verhängen kann, ebenso gebührend berücksichtigt wie die Art und Schwere des Verstoßes, der Kooperation mit der Aufsichtsbehörde, die vorsätzliche Begehungsweise der Tat sowie der Umstand, dass in überaus hoher Zahl besondere Kategorien personenbezogener Daten von der Tat betroffen waren. Das hier verhängte Bußgeld im mittleren vierstelligen Bereich war damit im Ergebnis wirksam, verhältnismäßig und abschreckend im Sinne von Art. 83 Abs. 1 DS-GVO.
Doch warum war die Entsorgung der Patientenakten in dieser Form überhaupt rechtswidrig? In den Patientenakten waren personenbezogene Daten gemäß Art. 4 Nr. 1 DS-GVO sowie besondere Kategorien personenbezogener Daten nach Art. 9 Abs. 1 DS-GVO (sogenannter Gesundheitsdaten) wie beispielsweise ärztliche Diagnosen und Befunde enthalten. Durch die Entsorgung der Patientenakten in den öffentlich zugänglichen und nicht verschlossenen Müllcontainern wurden die personenbezogenen Daten gegenüber Dritten offengelegt.

Nach der Systematik der DS-GVO ist eine Datenverarbeitung grundsätzlich untersagt, außer sie wird durch einen oder mehrere Erlaubnistatbestände des Art. 6 DS-GVO ausdrücklich gestattet. Hierbei spricht man von einem sogenannten Verbot mit Erlaubnisvorbehalt. Hinzu kommt das Prinzip der sogenannten Zweckbindung nach Art. 5 Buchstabe b) DS-GVO, wonach personenbezogene Daten nicht für andere als die im Vorhinein festgelegten Zwecke verwendet werden dürfen. Eine Datenverarbeitung ist beispielsweise dann rechtmäßig, wenn sämtliche betroffene Personen vorab und in Kenntnis des Zweckes der Verarbeitung in die Offenlegung ihrer Daten einwilligen (Art. 6 Abs. 1 Satz 1 Buchstabe a) DS-GVO). Weiter kann die Datenverarbeitung rechtmäßig sein, wenn sie zur Erfüllung eines Vertrages beziehungsweise zur Durchführung vorvertraglicher Maßnahmen nach Art. 6 Abs. 1 Satz 1 Buchstabe b) DS-GVO oder zur Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten gemäß Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO erforderlich ist, soweit nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Personen überwiegen. Die Einlassungen des Arztes im Rahmen der Anhörung und die vorliegenden Zeugenaussagen schlossen jedoch die Annahme des Vorliegens jedweder Erlaubnistatbestände des Art. 6 Abs. 1 DS-GVO aus. Demnach hatte die Ehefrau und Mitarbeiterin des Arztes die Patientenakten in den Müllcontainern entsorgt, da ein Teil der Räumlichkeiten der Arztpraxis aufgrund anstehender Renovierungsarbeiten umgehend beräumt werden musste. Die Ehefrau des Arztes habe sich dann aufgrund des Zeitdrucks und in angeblicher Unwissenheit in Bezug auf eine ordnungsgemäße Entsorgung dafür entschieden, die nicht mehr benötigten und archivierten Patientenakten in die Müllcontainer zu werfen. Hierbei sei ihr jedoch klar gewesen, dass es sich um sensible Daten gehandelt habe. Im Ergebnis stellte die Entsorgung der Patientenakten in den öffentlich zugänglichen und nicht verschlossenen Müllcontainern eine unrechtmäßige Verarbeitung personenbezogener Daten dar. Der Arzt hat damit die Bußgeldvorschrift des Art. 83 Abs. 5 Buchstabe a) DS-GVO verletzt, wonach derjenige ordnungswidrig handelt, der vorsätzlich oder fahrlässig gegen die Grundsätze für die Verarbeitung, einschließlich der Bedingungen für die Einwilligung gemäß den Artikeln 5, 6, 7 und 9 DS-GVO, verstößt.

Auch wenn die Verletzung des Art. 83 Abs. 5 Buchstabe a) DS-GVO seit dem 25. Mai 2018 und der damit einhergehenden Anwendbarkeit

der Datenschutz-Grundverordnung mittlerweile den weit überwiegenden Teil der Arbeit des TLfDI in Bußgeldverfahren ausmacht, so finden sich auch außerhalb der Datenschutz-Grundverordnung relevante Bußgeldvorschriften die Datenschutzverstöße betreffen. So beispielsweise in § 43 BDSG, wonach Verstöße gegen § 30 BDSG, der die Datenverarbeitung bei Verbraucherkrediten regelt, mit Bußgeldern bis zu 50.000 Euro sanktioniert werden können. Auch das ThürDSG enthält wie oben bereits dargelegt eine Bußgeldvorschrift: Nach § 61 Abs. 1 ThürDSG handelt ordnungswidrig, wer entgegen den Bestimmungen der DS-GVO, des ThürDSG oder anderer Rechtsvorschriften zum Schutz personenbezogener Daten solche Daten erhebt, speichert, verändert, übermittelt, nutzt, sie mithilfe von automatisierten Verfahren abrufbereit hält oder sich beziehungsweise Dritten aus Dateien mit personenbezogenen Daten verschafft oder sonst verarbeitet. Dies kann gemäß § 61 Abs. 2 ThürDSG mit einer Geldbuße bis zu 50.000 Euro geahndet werden. In Abgrenzung zu Art. 83 DS-GVO, in welchem die Bedingungen und Tatbestände für die Verhängung von Geldbußen ausschließlich gegenüber den Verantwortlichen und den Auftragsverarbeitern geregelt sind, hat der Thüringer Gesetzgeber damit auf Grundlage der Öffnungsklausel des Art. 84 Abs. 1 DS-GVO eine Regelung geschaffen, nach der die Verhängung von Geldbußen auch gegenüber Mitarbeitern öffentlicher Stellen möglich ist (vgl. § 43 Abs. 1 ThürDSG a. F.).

Zurück zur Datenschutz-Grundverordnung: Neben Verletzungen des Art. 83 Abs. 5 Buchstabe a) DS-GVO sind in der täglichen Arbeit des TLfDI auch Verletzungen des Art. 83 Abs. 4 Buchstabe a) DS-GVO anzutreffen, wonach ordnungswidrig handelt, wer vorsätzlich gegen die Pflichten der Verantwortlichen und der Auftragsverarbeiter gemäß den Artikeln 8, 11, 25 bis 39, 42 und 43 DS-GVO verstößt. So etwa im Fall einer Rechtsanwältin mit Kanzleisitz in einer Stadt im Süden Thüringens, welche unter anderem auch als Berufsbetreuerin tätig ist. In dieser Funktion hatte sie per Post Unterlagen eines verstorbenen Betreuten an eine Erbin geschickt. Diese stellte bei der Sichtung der Unterlagen fest, dass sich in den Unterlagen auch Kontoauszüge einer dritten Person befanden, welche ebenfalls unter Betreuung der Rechtsanwältin stand. Über diesen Umstand informierte die Erbin die Rechtsanwältin umgehend per E-Mail. Der TLfDI verhängte hier schließlich ein Bußgeld in Höhe von mehreren hundert Euro, da nach dem Ergebnis der Ermittlungen festzustellen war, dass die Rechtsan-

wältin es vorsätzlich unterlassen hatte, dem TLfDI die (versehentliche) Versendung und den damit verbundenen Besitz der Kontoauszüge durch die Erbin zu melden. Um eine angemessene Reaktion der Behörden zu gewährleisten, ist die Verletzung des Schutzes personenbezogener Daten gemäß Art. 33 Abs. 1 DS-GVO an die gemäß Art. 55 DS-GVO zuständige Aufsichtsbehörde zu melden. Die Meldung muss unverzüglich gemacht werden, möglichst innerhalb von 72 Stunden. Hinsichtlich des Fristbeginns für die Meldung ist auf die Kenntnis des Verantwortlichen abzustellen. Die relevanten Kontoauszüge enthielten mit dem Namen und der Adresse der Betreuten wie auch mit den Zahlungsein- und -ausgängen personenbezogene Daten gemäß Art. 4 Nr. 1 DS-GVO. Der Schutz dieser personenbezogenen Daten wurde gemäß Art. 4 Nr. 12 DS-GVO verletzt, da diese für den Zweck der Durchführung des Betreuungsverfahrens vorgesehen waren, jedoch in Bezug auf die Erbin offengelegt wurden. Hinsichtlich der erforderlichen Kenntnis über die Verletzung des Schutzes personenbezogener Daten konnte sich die Rechtsanwältin nicht auf die Schutzbehauptung zurückziehen, die E-Mail der Erbin mit dem Hinweis über den Erhalt der Kontoauszüge nicht erhalten zu haben. Ausweislich der dem TLfDI vorliegenden Unterlagen wurde die E-Mail der Erbin ohne technischen Fehler an die Rechtsanwältin versandt. Zudem hatten die Rechtsanwältin und die Erbin vor und nach der relevanten E-Mail stets erfolgreich per E-Mail kommuniziert, was es nach allgemeiner Lebenserfahrung und unter Berücksichtigung der hierzu ergangenen Rechtsprechung höchst unwahrscheinlich machte, dass ausgerechnet diese E-Mail nicht zugegangen sein sollte (vgl. LG Stuttgart, Urteil vom 7. März 2018, Az. 13 S 159/17). Selbst für den Fall, dass die E-Mail der Erbin im Spam-Filter hängen geblieben sein sollte, so hätte die Rechtsanwältin spätestens am nächsten Werktag Kenntnis von dieser E-Mail erlangt, da die im geschäftlichen Verkehr erforderliche Sorgfalt es erfordert, den Spam-Filter täglich zu kontrollieren (vgl. LG Bonn, Urteil vom 10. Januar 2014, Az. 15 O 189/13). In diesem Zusammenhang ist darauf hinzuweisen, dass der Verantwortliche aufgrund einer Meldung nach Art. 33 Abs. 1 DS-GVO über die Verletzung des Schutzes personenbezogener Daten kein Ordnungswidrigkeitenverfahren befürchten muss, § 43 Abs. 4 BDSG. Der Gesetzgeber hat ein solches nur in den Fällen vorgesehen, in denen der Verantwortliche eine entsprechende Meldung unterlässt. Ein Bußgeld im Rahmen einer Verletzung des Art. 83 Abs. 4 Buchstabe a) DS-GVO kann daher grundsätzlich nicht wegen der eigentlichen Verletzung des

Schutzes personenbezogener Daten verhängt werden, sondern nur wegen des weiteren Umgangs mit dieser Verletzung gegenüber der Aufsichtsbehörde.
Wie bereits dargelegt, macht jedoch die Verfolgung von Verletzungen des Art. 83 Abs. 5 Buchstabe a) DS-GVO den weit überwiegenden Teil der Arbeit des TLfDI in Bußgeldverfahren aus. Hierbei geraten auch immer wieder Polizisten in den Fokus der Ermittlungen des TLfDI, die aus rein privaten Gründen Abfragen in polizeilichen Recherche- und IT-Systemen tätigen. So hatte ein Polizist, welcher seinen Dienst in einer Polizeidienststelle im Westen Thüringens versieht, unter Nutzung seiner ihm persönlich zugewiesenen Benutzerkennung insgesamt zehn Abfragen zu einer Zeugin und einem mit ihr im Zusammenhang stehenden Ermittlungsverfahren in dem Recherchesystem „IGVP“ (Integrierte Vorgangsbearbeitung Polizei) vorgenommen. Der TLfDI verhängte auch hier ein Bußgeld in Höhe von mehreren hundert Euro und stellte im Ergebnis seiner Ermittlungen fest, dass der betroffene Polizeibeamte in allen Fällen unbefugt personenbezogene Daten erhoben und verarbeitet hatte, da diese Abfragen ohne Zusammenhang zu seiner dienstlichen Tätigkeit standen. Dies ergab sich unter anderem aus dem Umstand, dass alle gegen die Zeugin geführten Verfahren von einer anderen Polizeidienststelle im Norden Thüringens bearbeitet wurden. Auch war der Polizeibeamte nicht als Sachbearbeiter oder sonst in die Bearbeitung einzelner Vorgänge mit Bezug zu der Zeugin eingebunden. Der darüberhinausgehende Verdacht, dass der Polizeibeamte die so gewonnenen Informationen an Dritte weitergegeben haben könnte, konnte weder durch die zuvor eingebundene Staatsanwaltschaft, noch durch den TLfDI nachgewiesen werden. Mit dem Abfragen in dem polizeilichen Recherchesystem „IGVP“ fand ein sogenannter Exzess statt (siehe oben). Ein solcher liegt vor, sobald Polizeibeamte dienstliche Informationen zu **privaten** Zwecken verarbeiten, da die handelnden Polizeibeamten selbst die Zwecke und Mittel der Verarbeitung dieser Daten festlegen und sie damit als eigene Verantwortliche handeln.
So unterschiedlich die Sachverhalte der zuvor dargestellten Fälle waren, so unterschiedlich gestalteten sich auch die Verfahren. Während der Arzt und die Rechtsanwältin die verhängten Bußgelder sofort akzeptierten und auch bezahlten, erhob der Polizeibeamte Einspruch gegen den Bußgeldbescheid. Der Einspruch nach § 67 OWiG ist der statthafte Rechtsbehelf des Bußgeldverfahrens gegen den Bußgeldbe-

scheid. Dieser verhindert den Eintritt der Rechtskraft des Bußgeldbescheides und insoweit auch dessen Vollstreckbarkeit. Der Betroffene hat hier nochmals die Möglichkeit Stellung zu nehmen. Der Einspruch eröffnet das Zwischenverfahren gemäß § 69 Abs. 2 und 3 OWiG, bei dem der TLfDI prüft, ob er den Bußgeldbescheid aufrechterhält oder zurücknimmt. Zu diesem Zweck kann er weitere Ermittlungen durchführen oder dem Betroffenen Gelegenheit geben sich dazu zu äußern, ob und welche Tatsachen und Beweismittel er im weiteren Verfahren vorbringen will. Nimmt der TLfDI den Bußgeldbescheid nicht zurück, übersendet er die Bußgeldakte über die Staatsanwaltschaft an das in Thüringen hierfür einzig zuständige Amtsgericht Erfurt. Mit Übergabe der Akte gehen sämtliche Aufgaben auf die Staatsanwaltschaft über. Diese entscheidet sodann selbst, ob sie das Verfahren einstellt, weitere Ermittlungen durchführt oder die Bußgeldakte dem Richter beim Amtsgericht vorlegt, wobei eine Einstellung des Verfahrens durch die Staatsanwaltschaft nur mit Zustimmung des TLfDI möglich ist, § 41 Abs. 2 Satz 3 BSDG in Verbindung mit § 69 Abs. 4 Satz 2 OWiG. Durch den Übergang der Aufgaben auf die Staatsanwaltschaft ist der TLfDI nicht unmittelbar an dem sich an das Zwischenverfahren anschließenden Verfahren vor dem Amtsgericht beteiligt. Der Richter am Amtsgericht entscheidet schließlich auf Grundlage des im Bußgeldbescheid geschilderten Tathergangs, ob eine Ordnungswidrigkeit vorliegt, keine Verfahrenshindernisse vorliegen und eine Ahndung geboten erscheint. Im Fall des Polizisten hat der TLfDI auf den Einspruch hin den Bußgeldbescheid nach erneuter Überprüfung nicht zurückgenommen und die Bußgeldakte über die Staatsanwaltschaft an das Amtsgericht Erfurt versendet. Dieses hat den Bußgeldbescheid des TLfDI im Ergebnis bestätigt, jedoch die Höhe des Bußgeldes wegen der Einlassungen des Polizisten zu seinen wirtschaftlichen Verhältnissen, welche er erst in der Hauptverhandlung vorgetragen hatte, reduziert.

Damit endete das Bußgeldverfahren neben vielen rechtskräftigen Bußgeldbescheiden im Berichtszeitraum 2021 auch mit einem Urteil des Amtsgerichts. Dabei stellt der Erlass eines Bußgeldbescheids keineswegs die Regel dar. Viele Verfahren werden nach dem Ergebnis der durchgeführten Ermittlungen eingestellt, wenn sich ein hinreichender Tatverdacht nicht ergeben hat.

1.12 Kein Spaß mit der versteckten Kamera: Videoüberwachung im öffentlichen Bereich

Jede Form von Videoüberwachung führt zur Einschränkung des Grundrechts auf informationelle Selbstbestimmung. Sie ist daher an strenge Voraussetzungen gebunden. Der TLfDI veröffentlichte dazu im Jahr 2021 den Leitfaden für die Videoüberwachung durch öffentliche Stellen in Thüringen und die Orientierungshilfe Flugdrohnen im öffentlichen Bereich auf seiner Internetseite.

Der Ruf nach Videoüberwachung im öffentlichen Bereich nimmt auch in Thüringen stetig zu. So hatte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) auch im Jahr 2021 dazu eine Vielzahl von Beschwerden und Anfragen im Rahmen seiner Beratungstätigkeit zu bearbeiten. Dies nahm er zum Anlass, einen Leitfaden für die Videoüberwachung durch öffentliche Stellen in Thüringen und eine Orientierungshilfe zu Flugdrohnen im öffentlichen Bereich auf seiner Internetseite zu veröffentlichen unter
https://www.tlfdi.de/fileadmin/tlfdi/datenschutz/Kommunales/Leitfaden_OH_Video_oeffentl_Stellen.pdf
und
https://www.tlfdi.de/fileadmin/tlfdi/gesetze/orientierungshilfen/Orientierungshilfe_Drohnen_Stand_August_2021.pdf.
Nachfolgend soll kurz – ohne Anspruch auf Vollständigkeit – auf die wichtigsten Voraussetzungen der Videoüberwachung eingegangen werden. **Die einzelnen Zulässigkeitsvoraussetzungen sind jeweils für jede Kamera gesondert zu prüfen.** Die Details entnehmen Sie bitte den o.g. Orientierungshilfen.

1. Videoüberwachung nach § 30 Thür-DSG in Verbindung mit Art. 6 Abs. 1 Satz 1 Buchstabe e), Abs. 2 DS-GVO

Jede Verarbeitung personenbezogener Daten – so auch die Videoüberwachung – braucht eine Rechtsgrundlage. § 30 Thüringer Datenschutzgesetz (ThürDSG) in Verbindung mit Art. 6 Abs. 1 Satz 1 Buchstabe e), Abs. 2 Datenschutz-Grundverordnung (DS-GVO) regelt die Videoüberwachung durch öffentliche Stellen in Thüringen. Ausgenommen davon ist die Videoüberwachung durch die Ordnungsbehörden, durch öffentliche Stellen mittels Drohnen, durch öffentliche Stellen, die am Wettbewerb teilnehmen (§ 26 ThürDSG) und durch

die Polizei, für welche jeweils gesonderte Vorschriften anzuwenden sind.

Bevor eine Videoüberwachung eingerichtet werden kann, ist ihre datenschutzrechtliche Zulässigkeit zu prüfen. § 30 Abs. 1 ThürDSG erlaubt die Videoüberwachung unter folgenden Voraussetzungen:

„(1) Die Videobeobachtung oder -aufzeichnung mit Hilfe optisch-elektronischer Einrichtungen (Videoüberwachung) ist zulässig, wenn dies zur Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe oder in Ausübung öffentlicher Gewalt

1. *zum Schutz von Personen, die der überwachenden Stelle angehören oder sie aufsuchen, oder*
2. *zum Schutz von Sachen, die der zu überwachenden Stelle oder den Personen nach Nummer 1 gehören,*

erforderlich ist. Es dürfen keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der betroffenen Person überwiegen.“

Erste Voraussetzung ist also, dass die Videoüberwachung zur **Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe oder in Ausübung öffentlicher Gewalt** zulässig ist. Diese Aufgabe/Ausübung öffentlicher Gewalt muss klar definiert sein und eine Rechtsgrundlage haben.

Aus dem Grundsatz der Verhältnismäßigkeit als Teil des Rechtsstaatsprinzips folgt, dass jede staatliche Maßnahme – so auch die Videoüberwachung – einen **legitimen Zweck** haben sowie **geeignet, erforderlich** und **verhältnismäßig im engeren Sinne (angemessen)** sein muss.

Wie bei jeder Verarbeitung von personenbezogenen Daten ist also der **Zweck** der Videoüberwachung festzulegen. Nach § 30 ThürDSG kann dies der Schutz von Personen, die der überwachenden Stelle angehören oder sie aufsuchen beziehungsweise der Schutz von Sachen, die der zu überwachenden Stelle oder den genannten Personen gehören, sein.

Im nächsten Schritt ist zu prüfen, ob die Videoüberwachung **geeignet** ist, diesen Zweck zu erreichen. Geht es um den Schutz von Personen und Sachen ist insbesondere zu prüfen, ob die direkte Möglichkeit zum Eingriff in die schädigende Situation mit der Videoüberwachung geschaffen werden kann.

Erst wenn die Geeignetheit bejaht wird, ist im nächsten Schritt zu prüfen, ob die Videoüberwachung **erforderlich** ist. Hierbei genügt eine rein theoretisch eintretende Schädigung oder ein allgemeines Unsicherheitsgefühl nicht. Vielmehr muss eine **konkrete Gefährdung**

vorliegen und eine Verletzung von Rechtsgütern wahrscheinlich eintreten. Anhand von sicherheitsrelevanten Vorkommnissen ist eine Prognose für die Zukunft zu erstellen.
Es ist zu prüfen, ob mildere Mittel als eine Videoüberwachung eingesetzt werden können. Wenn dies bejaht wird, sind sie zunächst einzusetzen und im Hinblick auf ihren Erfolg zu evaluieren.
Zu prüfen ist ferner die räumliche und zeitliche Erforderlichkeit von Aufnahmen jeder Kamera sowie die Art und Weise der Videoüberwachung (reines Monitoring, Monitoring mit händisch ausgelöster Aufzeichnung, Black-Box-Verfahren). Die datenschutzrechtlichen Grundsätze der Datenminimierung (Art. 5 Abs. 1 Buchstabe c) DS-GVO) und der Speicherbegrenzung (Art. 5 Abs. 1 Buchstabe e) DS-GVO) sind zu wahren, das heißt es ist nur so umfangreich zu überwachen, wie dies unbedingt zur Zweckerreichung notwendig ist.
Liegt die Erforderlichkeit vor, ist zu prüfen, ob die Videoüberwachung **verhältnismäßig (angemessen)** ist und die von § 30 Abs. 1 S. 2 ThürDSG geforderte **Interessenabwägung** vorzunehmen. Je mehr personenbezogene Daten erhoben werden, umso größer ist der Eingriff in die Rechte der betroffenen Person, umso sorgfältiger hat die Interessenabwägung zu erfolgen. Die öffentliche Stelle muss begründen, warum sie welchem Interesse den Vorzug gibt und erneut prüfen, ob die Videoüberwachung räumlich und zeitlich angemessen ist.
Ist die Videoüberwachung durch die öffentliche Stelle für zulässig erachtet worden, hat sie zeitgleich mit der Inbetriebnahme der Kameras ihre Informationspflichten gemäß § 30 Abs. 2 ThürDSG zu erfüllen. Eine „heimliche“ Videoüberwachung ist hiernach unzulässig. Hierbei ist zu beachten, dass Hinweisschilder so anzubringen sind, dass sie **vor dem Betreten des videoüberwachten Bereichs** wahrgenommen werden können (circa auf Augenhöhe, mit Piktogramm, farblich abgehoben von der Umgebung). Ein Muster finden Sie auf der Homepage des TLfDI unter:
https://www.tlfdi.de/mam/tlfdi/datenschutz/video/informationsblatt_videoueberwachung_oeffentliche_stellen.pdf
Die weitergehenden Informationen nach Art. 13 DS-GVO können gemäß § 30 Abs. 2 ThürDSG zur Einsicht beim Verantwortlichen hinterlegt werden.
Die Grundsätze und Ausnahmen zur Zweckbindung sind einzuhalten (§ 30 Abs. 2, 3 ThürDSG). Die Löschung eventueller Aufnahmen nach § 30 Abs. 5 ThürDSG ist zu regeln und durchzuführen. Es sind

geeignete technische und organisatorische Maßnahmen nach Art. 32 DS-GVO zu ergreifen.
Die öffentliche Stelle unterliegt einer Vielzahl von Dokumentationspflichten im Rahmen der Videoüberwachung, zum Beispiel dem Führen eines Verzeichnisses von Verarbeitungstätigkeiten nach Art. 30 DS-GVO einschließlich eines Erfassungsblattes für jede Kamera, der Durchführung einer Risikoabschätzung und gegebenenfalls einer Datenschutz-Folgeabschätzung gemäß Art. 35 DS-GVO, dem Abschluss von Dienstvereinbarungen mit den eigenen Mitarbeitern und von Auftragsverarbeitungsverträgen mit Dritten nach Art. 28 Abs. 3 DS-GVO.

2. Videoüberwachung zur Gefahrenabwehr nach § 26 Abs. 2 OBG

Für die Thüringer Ordnungsbehörden gilt hinsichtlich der Videoüberwachung § 26 Abs. 2 Thüringer Ordnungsbehördengesetz (OBG):
„(2) 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.“
Wer Ordnungsbehörde ist, regelt § 1 OBG. Auch im Rahmen der Videoüberwachung nach § 26 Abs. 2 OBG ist das Vorliegen der gesetzlichen Voraussetzungen zu prüfen:
Die Videoüberwachung muss bei oder im Zusammenhang mit öffentlichen Veranstaltungen und Ansammlungen, die nicht dem Versammlungsgesetz unterliegen, stattfinden oder zur „Erfüllung der sonstigen Aufgaben“ erfolgen. Im Rahmen der Erfüllung sonstiger Aufgaben ist zu beachten, dass diese einer gesetzlichen Grundlage bedürfen. Nur wenn die Aufgabe tatsächlich der Kommune nach § 2 OBG zugewiesen ist, darf die Ordnungsbehörde tätig werden.
Auch im Rahmen des OBG ergibt sich aus dem Grundsatz der Verhältnismäßigkeit, dass die Videoüberwachung einen **legitimen Zweck** haben, **geeignet, erforderlich** und **verhältnismäßig im engeren**

Sinne (angemessen) sein muss. Zusätzlich ergibt sich aus dem Gesetzestext des § 26 Abs. 2 OBG „die Ordnungsbehörden **können“,** dass der Gesetzgeber den Ordnungsbehörden ein Ermessen einräumt. Auch aus diesem Ermessen ergibt sich, dass der Grundsatz der Verhältnismäßigkeit einzuhalten ist.
Somit ist der **Zweck** festzulegen. Ordnungsbehörden dürfen nicht die Aufgaben der Strafverfolgung übernehmen. Diese obliegt Polizei und Staatsanwaltschaft. Auch im Bereich des § 26 OBG dient die Videoüberwachung nur als Nebeneffekt der Aufklärung von Ordnungswidrigkeiten. Der Zweck ist in erster Linie die **Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung**. Die Definitionen der öffentlichen Sicherheit und Ordnung sowie der verschiedenen Gefahreneinstufungen befinden sich in § 54 OBG.
Die **Geeignetheit** der Videoüberwachung in ihrer konkreten Ausgestaltung zur Erreichung des Zwecks der Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung ist zu prüfen.
Die **Erforderlichkeit** muss gegeben sein. Es müssen **tatsächliche Anhaltspunkte** für das Entstehen von Gefahren für die öffentliche Sicherheit oder Ordnung bestehen. Die Prognose erfordert konkrete Kenntnisse der Ordnungsbehörde, zum Beispiel Indizien für Straftaten, Aufruf zu Gewaltakten. Lediglich Verdachtsmomente, Vermutungen, vage Andeutungen Dritter oder allgemeine Erfahrungssätze genügen nicht. Es ist zudem zu prüfen, ob mildere Mittel existieren. Diese sind vorrangig einzusetzen.
Nach pflichtgemäßem Ermessen ist außerdem zu entscheiden, wie die Videoüberwachung durchgeführt wird. Im Rahmen der **Angemessenheit** sind die widerstreitenden Interessen festzustellen und zu gewichten. Das Übermaßverbot ist zu beachten. Angesichts des Eingriffsgewichts einer Videoüberwachung (Eingriff in Grundrechte) muss sie dem Schutz von Rechtsgütern von zumindest erheblichem Gewicht oder einem vergleichbar gewichtigen öffentlichen Interesse dienen. (vgl. BVerfG, Entscheidung vom 18. Dezember 2019, 1 BvR 142/15, Rdn. 95; siehe auch juris BVerfG, 1 BvR 142/15, Rdn. 95). Die Abwehr jeder (noch so kleinen) Gefahr für die Rechtsordnung und damit der ganz allgemeine Schutz der öffentlichen Sicherheit und Ordnung rechtfertigt eine Videoüberwachung nicht.
Bis zur Einleitung eines konkreten Ordnungswidrigkeitenverfahrens gelten auch für diese Videoüberwachung die Grundsätze des ThürDSG in Verbindung mit der DS-GVO. Daher gelten auch hier zunächst die datenschutzrechtlichen Grundsätze, wie zum Beispiel das

Transparenzgebot gemäß Art. 5 Abs. 1 Buchstabe a) DS-GVO. Insbesondere sind Hinweisschilder anzubringen. Ferner gelten die Datenminimierung nach Art. 5 Abs. 1 Buchstabe c) DS-GVO und die Speicherbegrenzung nach Art. 5 Abs. 1 Buchstabe e) DS-GVO. Erst wenn das Ordnungswidrigkeitenverfahren gegen eine bestimmte Person eingeleitet wird, sind ab Einleitung des Ordnungswidrigkeitenverfahrens die Vorschriften ab Abschnitt 3 des ThürDSG anzuwenden, welche die JI-Richtlinie umsetzen.
Die Vernichtung der Daten hat gemäß § 26 Abs. 2 S. 2 OBG **spätestens** zwei Monate nach Ablauf des auslösenden Ereignisses zu erfolgen. Es handelt sich um eine **Höchstfrist.** Nach § 35 ThürDSG hat die Ordnungsbehörde die personenbezogenen Daten unverzüglich zu löschen, wenn die Verarbeitung unzulässig ist, wenn sie zur Erfüllung einer rechtlichen Verpflichtung gelöscht werden müssen oder ihre Kenntnis für die Aufgabenerfüllung nicht mehr erforderlich ist. Es hat also eine Prüfung im Einzelfall zu erfolgen, ob die Daten noch zur Aufgabenerfüllung erforderlich sind.

3. Videoüberwachung mittels Flugdrohnen

Der Einsatz einer Drohne fällt nur dann unter die DS-GVO und das ThürDSG, wenn personenbezogene oder -beziehbare Daten erhoben werden. Personenbezogene Daten definiert Art. 4 Nr. 1 DS-GVO:
„Im Sinne dieser Verordnung bezeichnet der Ausdruck:
1. „personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.“
Der Begriff des personenbezogenen Datums ist also weit gefasst. Nach der Entscheidung des Bundesverfassungsgerichts vom 15. Dezember 1983, Az. 1 BvR 209/83, gibt es unter den Bedingungen der automatisierten Datenverarbeitung kein belangloses Datum mehr. Dabei ist es gleichgültig, ob die verantwortliche Stelle eine Identifizierbarkeit anstrebt (vgl. Scholz in Simitis, Hornung, Spiecker, Datenschutzrecht, 1. Auflage 2019, Anhang zu Art. 6 Rn. 40). Entscheidend

ist nur, ob eine Identifizierung direkt oder indirekt tatsächlich **möglich** ist (siehe auch Europäische Leitlinien 3/2019 zur Verarbeitung personenbezogener Daten durch Videogeräte). Somit fallen neben eindeutigen Aufnahmen von Gesichtern zum Beispiel auch Kleidung, Gangbild, körperliche Merkmale, mitgeführte Gegenstände, Fahrzeugkennzeichen, Gebäude, Anschriften unter den Begriff des personenbezogenen Datums. Es genügt, wenn die Identifizierung erst durch Beiziehung weiterer Informationen möglich wird.
Lediglich Aufnahmen aus großer Höhe, bei denen Personendaten aufgrund der Entfernung und fehlender technischer Möglichkeiten, wie geringe Bildauflösung oder fehlende Zoom-Möglichkeit oder dauerhafte irreversible Verpixelung, fallen nicht unter die DS-GVO (vgl. Scholz in: Simitis, Hornung, Spiecker, Datenschutzrecht, 1. Auflage 2019, Anhang zu Art. 6, Rn. 42).
Auch der Einsatz einer Drohne bedarf einer **Rechtsgrundlage**.
§ 30 ThürDSG kommt hier nicht in Betracht, weil der Thüringer Gesetzgeber eine zumindest vorübergehende Ortsgebundenheit verlangt, die bei Flugdrohnen jedoch nicht vorliegt (siehe dazu die Begründung zu § 30 Abs. 1 ThürDSG aus dem Gesetzentwurf der Landesregierung in der Drucksache 6/4943, Seite 116). In den Spezialgesetzen, zum Beispiel zum Brand- und Katastrophenschutz und zu Umweltimmissionen sind keine datenschutzrechtlichen Regelungen enthalten. Die Aufnahmen und weitere Verarbeitung der Bilder von Flugdrohnen müssen daher den allgemeinen Anforderungen der DS-GVO und des ThürDSG entsprechen.
Somit wäre gemäß Art. 6 Abs. 1 S. 1 Buchstabe a) DS-GVO eine Einwilligung der betroffenen Person eine Rechtsgrundlage für die Verarbeitung personenbezogener Daten. Hierbei ist jedoch besonderes Augenmerk auf die tatsächliche Freiwilligkeit der Abgabe einer Einwilligungserklärung zu legen. Allein der Aufenthalt einer Person in einem durch eine Drohne videoüberwachten Bereich stellt keine Einwilligung dar. Das Über-Unter-Ordnungsverhältnis zwischen Bürger und Behörde ist ebenfalls zu beachten.
Im Einsatzbereich des Brand- und Katastrophenschutzes beziehungsweise bei allen Behörden und Organisationen mit Sicherheitsaufgaben (BOS) kann Art. 6 Abs. 1 S. 1 Buchstabe d) DS-GVO als Rechtsgrundlage in Betracht kommen, wobei dieser einen Ausnahmetatbestand darstellt. Der Gesetzgeber zählt humanitäre Zwecke einschließlich Epidemien, Naturkatastrophen und vom Menschen verursachte Katastrophen auf (siehe dazu Erwägungsgrund 46 der DS-GVO). Der

Einsatz zum Beispiel in Hochwassergebieten kann also auf diese Rechtsgrundlage gestützt werden.
Im Einsatzbereich von Umweltimmissionen kann Rechtsgrundlage Art. 6 Abs. 1 S. 1 Buchstabe d) DS-GVO ebenfalls nur im Ausnahmefall sein. Dies kann der Fall sein, wenn die Verarbeitung personenbezogener Daten beispielweise für humanitäre Zwecke einschließlich der Überwachung von Epidemien und deren Ausbreitung oder in humanitären Notfällen, insbesondere bei Naturkatastrophen oder vom Menschen verursachten Katastrophen erforderlich zum Schutz lebenswichtiger Interessen der betroffenen Person ist, siehe Erwägungsgrund 46 zur DS-GVO. Ansonsten kommt ausschließlich Art. 6 Abs. 1 S. 1 Buchstabe e), Abs. 3 DS-GVO in Verbindung mit § 16 ThürDSG als Rechtsgrundlage in Betracht.
Für andere Einsätze kann Art. 6 Abs. 1 S. 1 Buchstabe e), Abs. 3 DS-GVO in Verbindung mit § 16 Abs. 1 ThürDSG Rechtsgrundlage sein. § 16 Abs. 1 ThürDSG bestimmt:
„Die Verarbeitung personenbezogener Daten durch eine öffentliche Stelle ist zulässig, wenn sie zur Erfüllung der in der Zuständigkeit des Verantwortlichen im öffentlichen Interesse liegenden Aufgabe erforderlich ist oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde.“
Die im öffentlichen Interesse liegende Aufgabe definieren §§ 3, 6 und 7 Thüringer Brand- und Katastrophenschutzgesetz. Beispiele sind die Erkundung eines brennenden Gebäudes oder Waldes mittels Drohne, um festzustellen, ob sich hier noch (verletzte) Personen aufhalten oder der Einsatz bei unübersichtlichen Verkehrsunfällen. Die Anwendbarkeit der Regelungen des Art. 6 Abs. 1 S. 1 Buchstabe e), Abs. 3 DS-GVO in Verbindung mit § 16 ThürDSG ist immer vor jeder Entscheidung einer Behörde, ob ein Drohneneinsatz erfolgen soll, im Einzelfall zu prüfen. Es bedarf einer verfassungskonformen Auslegung (Verhältnismäßigkeitsprinzip) dieser Rechtsgrundlage (siehe auch Art. 1 Abs. 3, 20 Abs. 3 Grundgesetz (GG)). Zu berücksichtigen ist dementsprechend der Grundsatz der Datenminimierung (Art. 5 Abs. 1 Buchstabe c) DS-GVO). Die personenbezogenen Daten müssen für die Zwecke, zu denen sie verarbeitet werden, angemessen und erheblich sowie auf das für die Zwecke ihrer Verarbeitung notwendige Maß beschränkt sein (vgl. Erwägungsgrund 39 DS-GVO).
Im Bereich des Ordnungswidrigkeitenrechts kann § 100h Abs. 1 Nr. 1 Strafprozessordnung in Verbindung mit § 46 Abs. 1 Ordnungswidrig-

keitengesetz als Rechtsgrundlage für Bild- und Videoaufnahmen angewendet werden. § 33 Abs. 1 Halbsatz 2 ThürDSG verweist ausdrücklich darauf, dass speziellere Regelungen in anderen Gesetzen vorgehen. Es müssen die Grundsätze der Verhältnismäßigkeit der Ermittlungshandlungen beachtet werden. Der Einsatz ist nur dann zulässig, wenn andernfalls die Ermittlung des Aufenthaltsortes des Betroffenen auf andere Weise weniger erfolgversprechend oder erschwert wäre.
Für Ordnungsbehörden kommt § 26 Abs. 2 OBG als Rechtsgrundlage in Betracht. Es gelten hier die allgemeinen Grundsätze der Videoüberwachung, insbesondere die verfassungskonforme Auslegung, die Grundsätze der Datenminimierung und der Speicherbegrenzung und der Verhältnismäßigkeitsgrundsatz, siehe Ausführungen unter 2.
Auch im Rahmen der Videoüberwachung mittels Drohnen sind die jeweiligen gesetzlichen Voraussetzungen zu prüfen.
Aus dem Grundsatz der Verhältnismäßigkeit – der als Teil des Rechtsstaatsprinzips selbstverständlich auch für den Einsatz von Drohnen gilt – folgt, dass die Videoüberwachung mittels Drohnen einen **legitimen Zweck** haben, **geeignet, erforderlich** und **verhältnismäßig im engeren Sinne (angemessen)** sein muss. Der Grundsatz der Verhältnismäßigkeit leitet sich aus **Art. 1 Abs. 3 und Art. 20 Abs. 3 GG** ab. Um die Verhältnismäßigkeit zu wahren, ist zunächst somit der **Zweck** festzulegen und dessen Legitimität (Rechtsgrundlage) zu prüfen. Andernfalls ist die Videoüberwachung bereits rechtswidrig. Die **Geeignetheit**, die **Erforderlichkeit** und die **Angemessenheit**, um den angestrebten Zweck zu erreichen, sind zu prüfen. Es ist im Rahmen der Erforderlichkeit zu prüfen, ob mildere Mittel existieren, zum Beispiel Begehung vor Ort.
Im Rahmen der **Angemessenheit** ist zu prüfen, ob die schutzwürdigen Interessen der betroffenen Personen, das heißt das Recht auf informationelle Selbstbestimmung, überwiegen. Dies ist zum Beispiel beim Überfliegen mit Drohnen zu Ausbildungs- und Übungszwecken gegeben. Hier ist dafür Sorge zu tragen, dass Personen et cetera nicht erkennbar sind beziehungsweise kameraseits unkenntlich gemacht werden durch entsprechende Flughöhe oder Verpixelung.
Es sind die bei jeder Videoüberwachung einzuhaltenden datenschutzrechtlichen technischen, organisatorischen und dokumentarischen Pflichten zu erfüllen, wie zum Beispiel technische und organisatori-

sche Maßnahmen nach Art. 32 DS-GVO, Risikoabschätzung beziehungsweise Datenschutzfolgen-Abschätzung nach Art. 35 DS-GVO, Verzeichnis von Verarbeitungstätigkeiten nach § 30 DS-GVO.
Die Löschfristen sind unter Berücksichtigung der Grundsätze der Datenminimierung und der Speicherbegrenzung festzulegen.
Der behördliche Datenschutzbeauftragte ist gemäß Art. 38 DS-GVO, § 14 Abs. 1 ThürDSG ordnungsgemäß und frühzeitig einzubinden.
Der TLfDI ist für Videoüberwachungen nicht Genehmigungsbehörde. Diese Aufgabe wurde ihm seitens des Gesetzgebers nicht übertragen. Im Rahmen seiner Beratungsfunktion steht er jedoch bei Überlegungen zur Einrichtung von Videoüberwachungsanlagen gern für Rückfragen zur Verfügung.
Im Einzelfall hat der TLfDI im Rahmen der Bearbeitung von Beschwerden die Zulässigkeit einer Videoüberwachung ebenfalls sorgfältig im Rahmen seiner Befugnisse nach Art. 58 Abs. 1 DS-GVO zu prüfen und kann bei datenschutzrechtlichen Verstößen von seinen Abhilfebefugnissen nach Art. 58 Abs. 2 DS-GVO Gebrauch machen.
Die Videoüberwachung ist daher kein Spaß – erst recht nicht mit fliegender Kamera.

1.13 Stand zu Office 365/Microsoft 365 (neuer Name für das gleiche Produkt)

Das Thema Office 365/Microsoft 365 beschäftigt den TLfDI und die Datenschutzkonferenz der Datenschutzbehörden des Bundes und der Länder (DSK) bereits seit vielen Jahren. Trotz erkennbarer Änderungen seitens Microsoft gibt es immer noch problematische Datenverarbeitungsvorgänge in der Online-Version des Produkts. Daher ist der TLfDI nach wie vor bestrebt, einen datenschutzgerechten Zustand des Produktes zu erwirken und sieht immer noch großen Gesprächsbedarf mit Microsoft.

In seinen letzten Tätigkeitsberichten berichtete der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) schon ausführlich über die datenschutzrechtlichen Bedenken beim Einsatz von Office 365. Den TLfDI erreichten auch 2021 wieder einige Nachfragen bezüglich des Einsatzes von Office 365 (jetzt in Microsoft 365 umbenannt). Selten wird bei den Anfragen unterschieden, ob hiermit die lokal installierten Programme und deren Funktio-

nalitäten gemeint sind oder die (gleichnamigen) Cloud-Dienste. Häufig sind auch die lokal installierten Programme mit den Cloud-Diensten verbunden, sodass hier für die Nutzer auch schwer der eigentliche Verarbeitungsprozess feststellbar ist. So fließen lokal bearbeitete Inhalte, zum Beispiel über Cloud-Drive, automatisch auch in einen Microsoft-Cloud-Speicher oder werden direkt von einem Microsoft-Share-Point-Server geladen. Dabei ist diese Unterscheidung für die datenschutzrechtliche Beurteilung wesentlich. Für eine lokale Verarbeitung der Daten sind keine weiteren Datenflüsse notwendig und es kann ohne wesentliche Funktionseinschränkungen gelingen, diese Datenflüsse zu blockieren. Damit hat ein Nutzer oder ein Verantwortlicher potentiell die Datenverarbeitung sehr stark unter Kontrolle.
Diese Kontrolle liegt bei der Nutzung von Cloud-Diensten nicht mehr vor. Hier ist der Verantwortliche auf die Verarbeitung angewiesen, welche Microsoft anbietet – und an dieser Stelle gab es zahlreiche Probleme. Im Kern spielen die Online-Service-Terms von Microsoft eine Rolle, genauer das „Microsoft Professional Service Data Protection Addendum“ (siehe https://www.microsoft.com/licensing/docs/view/Professional-Services-Data-Protection-Addendum-DPA). Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hatte bereits 2020 die dem Einsatz des Produktes Microsoft Office 365 zu Grunde liegenden Online Service Terms sowie die Datenschutzbestimmungen für Microsoft-Onlinedienste (Data Processing Addendum / DPA) — jeweils Stand: Januar 2020 — geprüft und hinsichtlich der Erfüllung der Anforderungen von Art. 28 Abs. 3 Datenschutz-Grundverordnung (DS-GVO) bewertet. Sie kam zu dem Ergebnis, dass auf Basis dieser Unterlagen kein datenschutzgerechter Einsatz von Microsoft Office 365 möglich ist (siehe Protokoll der 3. Zwischenkonferenz der DSK am 22. September 2020, https://www.datenschutzkonferenz-online.de/media/pr/20201030_protokoll_3_zwischenkonferenz.pdf, Anlage 1). Seitdem hat auch Microsoft reagiert – viele der Kritikpunkte sind im aktuellen Data Protection Addendum nicht mehr zu finden (siehe erster Link). Also ist alles gut?
Der zuständige Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg (LfDI B-W) kam im Rahmen seiner Beratungstätigkeit bei einem schulischen Pilotprojekt in Baden-Württemberg in seiner Analyse der Online-Version von Office 365 zum Ergebnis, dass viele Datenflüsse zu Servern keinem funktionalen

Grund dienen, sondern reine Aktivitätsverfolgung der Nutzer darstellen und dass Nutzer für die Nutzung von bestimmten Funktionen plötzlich um Einwilligungen gebeten werden, welche sie gegenüber Microsoft abgeben. Damit wird gerade für öffentliche Stellen das Konstrukt der Auftragsverarbeitung ins Absurde geführt (der Auftraggeber/Verantwortliche – also zum Beispiel die Schule oder das Ministerium – bestimmt den nutzbaren Funktionsumfang gegenüber Microsoft, der Funktionsumfang der Nutzer unterliegt der Kontrolle des Auftraggebers/Schule/Ministerium und nicht Microsoft, während im Falle von Einwilligungen Microsoft als Verantwortlicher agieren möchte).
Laut der Untersuchung bricht Microsoft also aus der Rolle des Auftragnehmers aus, auch wenn auf dem Papier alle Kritikpunkte nach und nach behoben werden – eine faktische Änderung der Datenverarbeitung ist durch die Untersuchung aber nicht erkennbar. Der LfDI B-W kam im Ergebnis des Pilotprojektes April 2021 dazu, dass aus seiner Sicht die Risiken beim Einsatz der nun erprobten Microsoft-Dienste im Schulbereich als inakzeptabel hoch zu bewerten waren. Auch er riet deswegen davon ab, diese im Schulbereich zu nutzen (siehe Tätigkeitsbericht 2021 LfDI B-W, Seite 45, https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2022/02/22020225_Taetigkeitsbericht_TB-Datenschutz_2021_V1.pdf und https://fragdenstaat.de/anfrage/neubewertung-des-lfdi-bezuglich-der-dsfa-von-microsoft-office-365-1/626585/anhang/2021-04-23_Empfehlung_LfDI.pdf).
Es wird aufgrund der festgestellten Mängel weiterhin der Dialog mit Microsoft über verschiedene Kanäle und verschiedene Gremien gesucht, mit dem Ziel, eine Änderung der Datenverarbeitung herbeizuführen. Der TLfDI wird sich auch im Schulterschluss mit der Kultusministerkonferenz weiter an diesen Gesprächen beteiligen und versuchen, eine datenschutzgerechte Verarbeitung zu bewirken, bevor an andere Mittel zu denken ist. Dies setzt natürlich eine bemerkbare Kooperation seitens Microsoft voraus.

1.14 Sicherheit bei Funkanlagen

Data protection by design (Datenschutz durch Technik) ist in Art. 25 DS-GVO geregelt. Für Funkanlagen plant die EU-Kommission, weiterführende Sicherheitsmaßnahmen bezüglich der EU-Funkanlagenrichtlinie vorzuschreiben.

Bei smarten Geräten, smarten Kameras, Mobiltelefonen, Laptops, Dongles, Alarmanlagen oder zum Beispiel Hausautomatisierungssystemen besteht die Gefahr, dass sie gehackt werden und dass Datenschutzprobleme entstehen können, wenn sie mit dem Internet verbunden sind. In den letzten Jahren wurde auch bei Kinderspielzeug zunehmend festgestellt, dass möglicherweise ein mangelhafter Schutz der Rechte der Kinder in Bezug auf die Privatsphäre vorliegt und der Schutz personenbezogener Daten und die Sicherheit der Daten nicht immer gewährleistet sind. So hat beispielsweise entsprechend einem Heise-Bericht die Bundesnetzagentur 2020 drei vernetzte Spielzeuge als „verbotene Sendeanlage“ eingestuft. Sie dürfen hierzulande nicht vertrieben und genutzt werden, da sie tief in die Privatsphäre der Anwender eingreifen.
Aber auch tragbare Funkanlagen (zum Beispiel in Form von Armbändern, Taschenclips, Headsets, Fitnesstrackern und so weiter) können eine Reihe sensibler Daten des Nutzers über einen längeren Zeitraum überwachen und registrieren (zum Beispiel Standortdaten, Temperatur, Blutdruck, Herzfrequenz) und diese nicht nur über das Internet, sondern auch über Nahbereichs-Kommunikationstechnologien weiter übertragen.
Die Europäische Kommission will deshalb die Cybersicherheit per Delegierter Verordnung erhöhen und hat am 21. Oktober 2021 einen entsprechenden Entwurf der Verordnung zur Ergänzung der bestehenden EU-Funkanlagenrichtlinie 2014/53/EU veröffentlicht, siehe https://ec.europa.eu/growth/system/files/2021-10/C_2021_7672_F1_COMMISSION_DELEGATED_REGULATION_DE_V6_P1_1428769_0.PDF. Natürlich regelt die Datenschutz-Grundverordnung (DS-GVO) für den Geltungsbereich innerhalb der EU die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre. Ziel ist es aber, mittelfristig durch umfassende Initiativen auf dem EU-Markt nur noch solche Funkanlagen zuzulassen, die ausreichend sicher sind.
Auch wenn noch keine konkreten Vorgaben/Normen im EU-Kommissions-Entwurf der Delegierten Verordnung benannt werden, das Europäische Parlament und der Europäische Rat auch noch Einwände erheben können, so ist die Veröffentlichung des Entwurfs schon jetzt ein Signal an die Wirtschaft, insbesondere an die Hersteller solcher Geräte. Denn die konkreten noch zu definierenden Anforderungen müssen dann frühestmöglich in den Produktentwicklungszyklus mit

einfließen, da nach Bekanntgabe der Verordnung nur 30 Monate Übergangsfrist geplant sind.
Aus datenschutzrechtlicher Sicht ist die geplante Regelung zu begrüßen, denn Art. 25 DS-GVO richtet sich nur an die Verantwortlichen, die beim Einsatz von solchen Systemen Data protection by design (Datenschutz durch Technik) umsetzen sollen, nicht aber unmittelbar an die Hersteller.

1.15 Das besondere elektronische Bürger- und Organisationenpostfach (eBO)

Mit der Einführung des eBO sollen zukünftig Bürgerinnen, Bürger und Organisationen elektronische Dokumente sicher und zuverlässig mit der Justiz austauschen können. Hierzu sind sichere Verfahren bezüglich der Authentifizierung der Nutzer und sichere Datenübertragungswege notwendig.

Für den sicheren elektronischen Rechtsverkehr gibt es schon das besondere elektronische Behördenpostfach, das besondere elektronische Notarpostfach und das besondere elektronische Anwaltspostfach.
Mit dem neuen Gesetz zum Ausbau des elektronischen Rechtsverkehrs mit den Gerichten und zur Änderung weiterer Vorschriften (Bundesgesetzblatt Nr. 71 vom 11. Oktober 2021) wurde auch die „Elektronischer-Rechtsverkehr-Verordnung“ geändert und es wurden gesetzliche Regelungen für das besondere elektronische Bürger- und Organisationenpostfach (eBO) geschaffen. Ab dem 1. Januar 2022 sollen nun mit dem eBO Bürgerinnen, Bürger und Organisationen elektronische Dokumente sicher und zuverlässig mit der Justiz austauschen können (§ 10 Elektronischer-Rechtsverkehr-Verordnung).
Der Webseite https://egvp.justiz.de/buerger_organisationen/index.php ist zudem zu entnehmen, dass künftig für die Kommunikation mit der Justiz auch das kostenfreie Nutzerkonto nach dem Onlinezugangsgesetz (OZG) verwendet werden kann. Der Funktionsumfang der Nutzerkonten wird hierfür erweitert und voraussichtlich im zweiten Quartal 2022 zur Verfügung stehen. Das OZG-Nutzerkonto selbst, auch oft Servicekonto genannt, ist im Onlinezugangsgesetz und Thüringer E-Government-Gesetz geregelt. Es dient dem Nutzer zur elektronischen Kommunikation zwecks Dienstleistungen mit der öffentlichen Verwaltung in Thüringen. Der Thüringer Landesbeauftragte für

den Datenschutz und die Informationsfreiheit (TLfDI) berichtete darüber bereits ausführlich in seinem Tätigkeitsbericht von 2018, Punkt 5.3).
Der TLfDI wird die weitere Entwicklung beobachten und steht auch gerne im Rahmen seiner Beratungsfunktion den entsprechenden Ministerien zur Verfügung.

1.16 Automatisierte Abrufe des Lichtbilds und der Unterschrift aus den Pass- oder Personalausweisregistern

Automatisierte Abrufe des Lichtbilds und der Unterschrift aus den Pass- oder Personalausweisregistern (durch befugte Behörden) bedürfen der strikten Einhaltung der DS-GVO. Zudem handelt es sich dabei um biometrische Daten gemäß Art. 9 DS-GVO.

Mögliche Datenübermittlungen und automatisierte Abrufe des Lichtbilds und der Unterschrift aus den Pass- und Personalausweisregistern sind in § 22a Passregistergesetz (PassG) und § 25 Personalausweisgesetz (PAuswG) geregelt.
Mit der im August 2021 veröffentlichten „Verordnung zu automatisierten Datenabrufen aus den Pass- und Personalausweisregistern sowie zur Änderung der Passverordnung, der Personalausweisverordnung und der Aufenthaltsverordnung“ wurde auch unter Artikel 1 die „Verordnung zu automatisierten Datenabrufen aus den Pass- und Personalausweisregistern (Pass- und Personalausweisdatenabrufverordnung – PPDAV)“ bekannt gemacht (Bundesgesetzblatt Nr. 56/2021 vom 24. August 2021). Diese PPDAV selbst tritt am 1. Mai 2022 in Kraft.
Mit der PPDAV wurden nun die Voraussetzungen für automatisierte Abrufe des Lichtbilds und der Unterschrift aus den Pass- oder Personalausweisregistern gesetzlich geregelt. So dürfen entsprechend § 1 Nummer 1 PPDAV automatisiert Lichtbilder aus den Pass- oder Personalausweisregister aufrufen: die Polizeibehörden des Bundes und der Länder, der Militärische Abschirmdienst, der Bundesnachrichtendienst, die Verfassungsschutzbehörden des Bundes und der Länder, die Steuerfahndungsdienststellen der Länder, der Zollfahndungsdienst und die Hauptzollämter. Weiterhin dürfen entsprechend § 1 Nummer 2 PPDAV das Lichtbild und die Unterschrift aus dem Pass- oder Personalausweisregister automatisiert abrufen: die zur Ausstellung

des Führerscheins, des Fahrerqualifizierungsnachweises oder der Fahrerkarte berechtigten Behörden.
Um diesen automatisierten Abruf des Lichtbilds und gegebenenfalls der Unterschrift bundesweit einheitlich zu gestalten, wurden in der PPDAV die technischen Grundlagen des Abrufverfahrens (unter anderem die Datenaustauschformate und Übermittlungsprotokolle) als auch die Auswahldaten, die bei einem Abruf verwendet werden dürfen, festgelegt.
Mit dem Artikel-Gesetz zur Einführung eines elektronischen Identitätsnachweises mit einem mobilen Endgerät (Bundesgesetzblatt Nr. 40/2021 vom 8. Juli 2021) wurde zuvor zudem in Artikel 1 ein § 22a Passgesetz aufgenommen. Dieser regelt, dass durch Landesrecht zentrale Passregisterdatenbestände zur Speicherung des Lichtbilds und der Unterschrift für die Durchführung eines automatisierten Abrufs des Lichtbilds nach § 22a Absatz 2 Satz 1 und 5 sowie eines automatisierten Abrufs des Lichtbilds und der Unterschrift nach § 22a Absatz 2 Satz 6 eingerichtet werden können. Macht ein Land von der Regelungsbefugnis Gebrauch, hat es dabei technisch sicherzustellen, dass die Lichtbilder und Unterschriften vor unbefugtem Zugriff geschützt sind. Die Lichtbilder und Unterschriften dürfen nur so gespeichert werden, dass keine Verknüpfung mit anderen als für den automatisierten Abruf benötigten Daten ermöglicht wird.
Diese Öffnungsklausel hatte der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) in seiner Stellungnahme zum Gesetzesentwurf zur Einführung eines elektronischen Identitätsnachweises mit einem mobilen Endgerät kritisiert und abgelehnt – erfolglos. Die nach § 27a PassG eingeräumte Befugnis, auf Länderebene zentrale Passregisterdatenbestände zum Zweck des automatisierten Abrufs des Lichtbilds und der Unterschrift einrichten zu können, wurde hauptsächlich damit begründet, dass es für viele Kommunen bereits eine große Herausforderung bedeuten würde, allein die technischen Voraussetzungen für den automatisierten Abruf sicherzustellen, und dass eine zentrale Datenhaltung neben einer Erleichterung der Umsetzung der Abrufe auch die Möglichkeit der Einbindung spezialisierter Einrichtungen zur Gewährleistung eines hohen Maßes an Datensicherheit biete.
Der BfDI sah dies anders: „Diesen Erwägungen steht allerdings gegenüber, dass der in den Pass- und Personalausweisbehörden für einen automatisierten Abruf vorhandene Datenbestand auf Landesebene zu-

sätzlich noch einmal gespiegelt und dauerhaft für die gesetzlich vorgesehenen Abrufzwecke vorgehalten würde. Da jeder neu und auf Dauer geschaffene Bestand an personenbezogenen Daten das Risiko einer zweckfremden Verwendung oder eines Missbrauchs potenziell deutlich erhöht, ist seine Einrichtung vor allem an den datenschutzrechtlichen Grundsätzen der Datenminimierung und Erforderlichkeit zu messen. Schon in dieser Hinsicht bedarf es unabweisbarer Gründe, um einen solchen zusätzlichen Datenbestand zu legitimieren.
Die Anforderungen an diesen Prüfungsmaßstab steigen noch, wenn – wie hier hinsichtlich des biometrischen Lichtbilds – eine Verarbeitung von besonderen Kategorien personenbezogener Daten nach Art. 9 DS-GVO erfolgt. An dieser Stelle sehe ich auch einen entscheidenden Unterschied zu den bereits etablierten zentralen (Spiegel-)Melderegistern der Länder zum Zweck eines automatisierten Abrufs bestimmter Meldedaten nach § 39 Abs. 3 Bundesmeldegesetz – denn hierbei handelt es sich nicht um eine Verarbeitung besonders sensibler Daten im Sinne des Art. 9 DS-GVO. Im Lichte dessen kann die Begründung des Änderungsantrags daher nicht überzeugen.“ (siehe https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Stellungnahmen/2021/StgN_elektr-Identit%C3%A4tsnachweis-mobil.pdf?__blob=publicationFile&v=1).
Für Thüringen wird der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit die Umsetzung der PPDAV im Blick behalten und steht für Beratungsbedarf den beteiligten Akteuren zur Verfügung.

1.17 Notruf-App „nora“

Mit der Notruf-App „nora“ der Bundesländer erreichen Sie Polizei, Feuerwehr und Rettungsdienst im Notfall schnell und einfach. Auch Menschen mit eingeschränkten Sprach- und Hörfähigkeiten können diese App nutzen. Die Datenschutzaufsichtsbehörden der Länder sind dabei beratend tätig.

Mit der Notruf-App „nora“ der Bundesländer erreichen Sie Polizei, Feuerwehr und Rettungsdienst im Notfall schnell und einfach. Überall in Deutschland. Über die App können Sie außerdem Notrufe absetzen, ohne sprechen zu müssen. Das ermöglicht Menschen mit eingeschränkten Sprach- und Hörfähigkeiten den direkten Kontakt zu den Leitstellen von Polizei, Feuerwehr und Rettungsdienst. Hinweise

hierzu finden Sie unter der Website: https://www.nora-notruf.de/de-as/startseite.
Die Geschäfts- und Koordinierungsstelle des Notruf-App-Systems ist dabei im Ministerium des Innern des Landes Nordrhein-Westfalen angesiedelt. Die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen war bei der Einführung der Notruf-App „nora“ datenschutzrechtlich beratend tätig und hatte keine datenschutzrechtlichen Bedenken gegen den regulären Start der Notruf-App „nora“.
Mit Schreiben vom 12. Juli 2021 teilte das Thüringer Ministerium für Inneres und Kommunales (TMIK) dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) mit, dass alle zwölf „Zentralen Leitstellen“ im Freistaat Thüringen und die Landeseinsatzzentrale der Polizei an das System angeschlossen sind. Zudem sei geplant, dass das Notruf-App-System Ende Juli 2021 in den bundesweiten Produktivbetrieb gehen solle und der „Go-Live“ für den 29. Juli 2021 geplant sei.
Auf Nachfrage Anfang 2022 teilte das TMIK mit, dass das Notruf-App-System am 28. September 2021 in den Wirkbetrieb gegangen ist. „Damit wurde auch die erste von drei Phasen des Projektes abgeschlossen. In der ersten Phase wurde „nora“ in den Leitstellen als Web-Anwendung implementiert. Die zweite Phase hat das Ziel, eine Schnittstelle zu den Einsatzleitsystemen zu entwickeln, sodass die Disponenten nur eine Benutzeroberfläche bedienen müssen. In der letzten Phase sollen sich auch Drittanbieter-Apps an eine noch zu definierende Schnittstelle anschließen können. Der Abschluss der Phasen und das Projektende sind noch nicht terminiert.“
Entsprechend der Datenschutzerklärung der App (https://www.nora-notruf.de/de-as/datenschutzbeauftragte) handelt es sich um ein Verfahren der gemeinsamen Verantwortlichkeit gemäß Art. 26 Datenschutz-Grundverordnung. Es wurde dabei festgelegt, dass die interne Verwaltung und Organisation der App durch die eingerichtete Geschäfts- und Koordinierungsstelle erfolgt, welche derzeit im Land Nordrhein-Westfalen (Ministerium des Innern) eingegliedert ist und die als direkter Ansprechpartner der Bürgerinnen und Bürger und durch die Datenverarbeitung Betroffener dient. Ungeachtet dessen kann man sich auch mit Datenschutzanfragen und bei Geltendmachung von Betroffenenrechten an jede verantwortliche Stelle wenden. Die Kontaktdaten der Datenschutzbeauftragten der jeweiligen Verantwortlichen der Bundesländer sind dazu in der Datenschutzerklärung

gelistet. Für Thüringen ist die verantwortliche Stelle das Thüringer Ministerium für Inneres und Kommunales. Somit können Sie Ihr Anliegen bei Bedarf an die Datenschutzbeauftragte im Thüringer Ministerium für Inneres und Kommunales richten.
Natürlich können Sie sich jederzeit auch an den TLfDI wenden.

1.18 Orientierungshilfe zu Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail

Die DSK hat im Berichtszeitraum die Orientierungshilfe „Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail“ überarbeitet. Ergänzend wurden Informationen zur Verarbeitung von Daten durch Berufsgeheimnisträger eingefügt. Diese sollten das Thema Ende-zu-Ende-Verschlüsselung besonders ernst nehmen, wenn personenbezogene Daten nach Art. 9 DS-GVO übertragen werden müssen.

Von der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) wurde eine überarbeitete „Orientierungshilfe zu Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail“ mit Stand 16. Juni 2021 veröffentlicht (https://www.datenschutzkonferenz-online.de/media/oh/20210616_orientierungshilfe_e_mail_verschluesselung.pdf).
Die Orientierungshilfe nimmt den Stand der Technik zum Veröffentlichungszeitpunkt als Ausgangspunkt für die Konkretisierung der Anforderungen.
Darin beschrieben sind Anforderungen an die Verfahren zum Versand und zum Empfang von E-Mail-Nachrichten durch Verantwortliche, ihre Auftragsverarbeiter und öffentliche E-Mail-Diensteanbieter. Dabei unterscheidet die Orientierungshilfe zwischen den Rollen des „Senders“ und des „Empfängers“. Für jede der Rollen wird wiederum unterschieden, ob ein „normales Risiko“ für Betroffene vorliegt oder ein „hohes Risiko“. Je nach Rolle und Risikostufe werden unterschiedlich umfangreiche Maßnahmen empfohlen.
Betrachtet werden in der Orientierungshilfe unter anderem die technischen Anforderungen an die Erbringung von E-Mail-Diensten bei Inanspruchnahme von E-Mail-Diensteanbietern (zum Beispiel die Einhaltung der Technischen Richtlinie 03108-1 des Bundesamts für Sicherheit in der Informationstechnik) sowie die gebotene Sorgfaltspflicht bei Nutzung derartiger Dienstleister (zum Beispiel Prüfung auf

hinreichende Garantien für die Einhaltung der Datenschutz-Grundverordnung (DS-GVO) und explizit der oben genannten Technischen Richtlinie).
Der Einsatz von Transportverschlüsselung bietet einen Basis-Schutz und stellt eine Mindestmaßnahme zur Erfüllung der gesetzlichen Anforderungen dar. In der Orientierungshilfe werden zudem unter dem Punkt 5.2 „Qualifizierte Transportverschlüsselung“ vier Voraussetzungen genannt, die einen ausreichenden Schutz gegen aktive Angriffe von Dritten bieten, die in der Lage sind, den Netzwerkverkehr auf der Übermittlungsstrecke zu manipulieren. Neben dem Einsatz kryptografischer Algorithmen und Protokolle entsprechend dem Stand der Technik wird auch aufgeführt, dass der empfangende Server im Zuge des Aufbaus der verschlüsselten Verbindung entweder zertifikatsbasiert authentifiziert wird oder anhand eines öffentlichen oder geheimen Schlüssels, der über einen anderen Kanal zwischen Sender und Empfänger abgestimmt wurde.
Durch den Einsatz von signierten Schlüsseln kann die Authentizität (das heißt: Identität) von Sender und Empfänger sichergestellt werden. In der Praxis werden hierzu zum Beispiel Zertifikate der sogenannten public-key-infrastructure genutzt. Dadurch kann der Empfänger erkennen, dass er wirklich mit dem Absender kommuniziert (und nicht , mit einem getarnten Angreifer). Andersherum kann auch der Sender erkennen, dass er mit dem richtigen Empfänger den Kommunikationskanal eröffnet hat.
Steigt das Risiko aber durch die Art der zu verarbeitenden Daten, muss zusätzlich eine Ende-zu-Ende-Verschlüsselung erwogen werden. Insgesamt hängen also die notwendigen Maßnahmen damit immer am Risiko für den Betroffenen und damit direkt vom Inhalt der E-Mail ab.
Die Orientierungshilfe weist zudem insbesondere darauf hin, dass bestimmte Personen wie Rechtsanwälte und Rechtsanwältinnen sowie Ärzte und Ärztinnen als Berufsgeheimnisträger besondere Pflichten zur Geheimhaltung ihnen anvertrauter Daten haben. Sie müssen neben dem Datenschutzrecht zusätzliche Strafvorschriften, zum Beispiel § 203 Strafgesetzbuch, und das Berufsrecht beachten. Es wird darauf hingewiesen, dass das Risiko bei Berufsgeheimnisträgern eher als „hoch“ angenommen werden kann, wenn diese besonders schützenswerte Daten verarbeiten. „Wenn Daten einem Berufsgeheimnis unterliegen, ist daher aus datenschutzrechtlicher Sicht stets zu prüfen, ob deren Verarbeitung zu einem hohen Risiko im Sinne der DS-GVO führt.“

In der Orientierungshilfe wird unter dem Punkt 4.2.3 „Versand von E-Mail-Nachrichten durch gesetzlich zur Verschwiegenheit Verpflichtete“ ergänzend ausgeführt: „Gemäß Erwägungsgrund 75 der DS-GVO können bei der Verarbeitung von personenbezogenen Daten, die einem Berufsgeheimnis unterliegen, durch einen Verlust der Vertraulichkeit Risiken für die Rechte und Freiheiten der betroffenen Person auftreten. Erhalten so Personen unbefugt Zugang zu den in einer E-Mail-Nachricht enthaltenen personenbezogenen Daten, stellt dies eine Verletzung des Schutzes personenbezogener Daten dar, die durch technische und organisatorische Maßnahmen (wie individuelle Adressierung und gegebenenfalls Verschlüsselung) zu verhindern ist.“ Die Orientierungshilfe: „Weil das Vorliegen eines Berufsgeheimnisses ein Indiz für ein hohes Risiko darstellen kann, haben Berufsgeheimnisträger die Höhe des jeweiligen Risikos besonders zu prüfen.“

1.19 SDM-Baustein „Nr. 41: Planen und Spezifizieren“

Der Arbeitskreis Technik der DSK hat zum Standard-Datenschutzmodel (SDM) einen weiteren Baustein „Planen und Spezifizieren“ veröffentlicht. Die Planung und Spezifikation einer Verarbeitung ist mit der Festlegung der Mittel ein aus datenschutzrechtlicher Sicht erforderlicher Schritt. Dieser Schritt hat sich an den Grundsätzen der Verarbeitung personenbezogener Daten nach Art. 5 DS-GVO zu orientieren.

Wie bereits im letzten Tätigkeitsbericht des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) mitgeteilt, verabschiedete die 99. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) das „*Standard-Datenschutzmodell – Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele*“ (SDM), in der Version 2.0b. Darin werden rechtliche Anforderungen der Datenschutz-Grundverordnung (DS-GVO) vollständig erfasst und systematisiert durch Gewährleistungsziele untersetzt. Mit dem SDM stellt die Konferenz ein Werkzeug bereit, mit dem die von der DS-GVO geforderten technischen und organisatorischen Maßnahmen rechtskonform abgeleitet werden können.
Auch wurde im Tätigkeitsbericht auf die sieben schon veröffentlichten Bausteine „Aufbewahren“, „Dokumentieren“, „Protokollieren“,

„Trennen“, „Löschen und Vernichten“, „Berichtigen“ und „Einschränken der Verarbeitung“ hingewiesen (3. Tätigkeitsbericht des TLfDI, Punkt 2.13).
Der Arbeitskreis Technik der DSK hat nun einen weiteren Baustein „Nr. 41: Planen und Spezifizieren“ veröffentlicht. Die Planung und Spezifikation einer Verarbeitung ist mit der Festlegung der Mittel (im Sinne des Art. 4 Satz 1 Nr. 7 DS-GVO) ein aus datenschutzrechtlicher Sicht erforderlicher Schritt. Dieser Schritt hat sich an den Grundsätzen der Verarbeitung personenbezogener Daten nach Art. 5 DS-GVO zu orientieren. Die DS-GVO fordert zudem in Art. 25 die Durchsetzung von Datenschutzanforderungen bereits im Prozess der Technikgestaltung und durch datenschutzfreundliche Voreinstellungen der verwendeten IT-Systeme („Data protection by design and by default“).
Dies bedeutet, dass beispielsweise in der Planungsphase die Verarbeitungstätigkeit und die mit ihr verbundenen Verarbeitungsvorgänge mit hinreichender Tiefe so zu spezifizieren sind, dass die Verarbeitungstätigkeit mit ihren wesentlichen Daten, Systemen und Diensten sowie Prozessen der Verarbeitung präzise und vollständig festgelegt sowie nachvollziehbar und prüfbar dokumentiert sind. Als ein wesentlicher Teil der Planungsphase einer Verarbeitungstätigkeit MUSS der Verantwortliche auch prüfen, ob eine Datenschutz-Folgenabschätzung (DS-FA) gemäß Art. 35 DS-GVO erforderlich ist. Zu diesem Zweck muss er eine Schwellwertanalyse durchführen. Mit einer Schwellwertanalyse wird die Risikostufe der Verarbeitungstätigkeit bestimmt. Wird ein „hohes Risiko“ für die Rechte und Freiheiten natürlicher Personen festgestellt, muss eine DS-FA durchgeführt werden.
Die Spezifikationen der technischen Komponenten einer Verarbeitungstätigkeit SOLLTEN die Form eines Lasten- und Pflichtenhefts annehmen. Der Auftraggeber (im Datenschutz immer der Verantwortliche) hat dabei im Lastenheft möglichst präzise die Gesamtheit der umzusetzenden Anforderungen festzulegen. Das Pflichtenheft beschreibt dann in konkreter Form, wie und womit – auch ein Auftragsverarbeiter – die Anforderungen des verantwortlichen Auftraggebers einzulösen beabsichtigt.
Der Baustein geht weiterhin insbesondere auf Aspekte ein, die bei einer Verarbeitung vom Verantwortlichen umgesetzt werden MÜSSEN, unabhängig von der Risikostufe. So sind beispielsweise neben der konkreten Beschreibung der Datenverarbeitung, die an der Verarbei-

tung beteiligten Organisationen/Akteure und die betroffenen Personen, Einsatzszenarien, Rechtsgrundlagen, Schutzmaßnahmen, Angreifermodelle sowie Kontrollphasen zu identifizieren. Der Baustein stellt diesbezüglich mögliche Maßnahmen vor.
Dabei ist nicht nur das IT-System allgemein, sondern auch die jeweilige Fachapplikation zu betrachten. Eine Fachapplikation muss in der Lage sein, Daten sicher zu speichern, zu verändern und zu löschen und ausgeführte Funktionalitäten im erforderlichen Umfang zu protokollieren.
Die aktuelle Version des SDM in der Version 2.0b mit den Bausteinen (Maßnahmenkatalog) ist unter https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/ abrufbar. Der TLfDI empfiehlt, bei Neuanschaffung von Systemen oder geplanten Entwicklungen oder Umstellungen von IT-Systemen diesen Baustein zu nutzen. Dies gilt sowohl für öffentliche Stellen als auch für den Bereich der Privatwirtschaft.

1.20 SDM-Baustein „Nr. 51: Zugriff auf Daten, Systeme und Prozesse regeln“

Der Arbeitskreis Technik der Datenschutzkonferenz der Aufsichtsbehörden des Bundes und der Länder hat zum Standard-Datenschutzmodell (SDM) einen weiteren Baustein „Zugriff auf Daten, Systeme und Prozesse regeln“ veröffentlicht. Wenn Verarbeitungstätigkeiten voneinander logisch beziehungsweise funktional getrennt sind, sollte eine Zweckbindung jeder beabsichtigten Verarbeitungstätigkeit und der dafür eingesetzten Daten, Systeme und Dienste sowie Prozesse insbesondere durch Trennungsmaßnahmen durchgesetzt werden.

Zum Stand des Standard-Datenschutzmodells (SDM) wurden bereits in diesem Tätigkeitsbericht entsprechende Ausführungen gemacht. Der Arbeitskreis Technik der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder hat neben dem Baustein „Nr. 41: Planen und Spezifizieren“ (Punkt 1.19) einen weiteren Baustein „Nr. 51: Zugriff auf Daten, Systeme und Prozesse regeln“ veröffentlicht.
Der Baustein bezieht sich hauptsächlich auf die Anforderungen an ein Rollen- und Berechtigungskonzept bei der Verarbeitung von Daten in der gesamten Organisation und bildet die entsprechenden Pflichten des Verantwortlichen ab. Durch die Vergabe von Rollen und die damit

einhergehende Erteilung von fachlichen Zuständigkeiten sowie technischen Berechtigungen soll das Risiko einer unrechtmäßigen Datenverarbeitung durch Zugriffe, die unbefugt beziehungsweise nicht vom Zweck der Datenverarbeitung gedeckt sind, unterbunden werden. Um ein entsprechendes Rollen-, Zuständigkeiten- und Berechtigungskonzept zu erstellen, muss der Verantwortliche die Verarbeitungstätigkeiten mit ihren Aktivitäten, den dafür erforderlichen Mitteln, den personenbezogenen Daten und den unterstützend zum Einsatz kommenden Systemen und Diensten analysieren und dokumentieren. Für alle möglichen Datenzugriffe müssen die Gewährleistungsziele mit Blick auf die Rollen beziehungsweise Personengruppen sowie auf die Systeme und Dienste erfüllt werden. Dies bedeutet insbesondere, dass nur solche Zuständigkeiten und Berechtigungen vergeben werden dürfen, welche für die Ausführung der jeweils erforderlichen Verarbeitungsschritte notwendig sind. Wenn Verarbeitungstätigkeiten voneinander logisch beziehungsweise funktional getrennt sind, sollte eine Zweckbindung jeder beabsichtigten Verarbeitungstätigkeit und der dafür eingesetzten Daten, Systeme und Dienste sowie Prozesse insbesondere durch Trennungsmaßnahmen durchgesetzt werden. So sind zum Beispiel im Rahmen der Personalverwaltung die erforderlichen Verarbeitungsprozesse und die dafür zuständigen Personen festzulegen. Nur diesen berechtigten Mitarbeitern sind die für die jeweilige konkrete Aufgabe erforderlichen Rechte zuzuweisen. So darf zum Beispiel ein Mitarbeiter, der nur die ordnungsgemäße Zeiterfassung sicherzustellen hat, nicht auf komplette Personalakten zugreifen. Technisch wird dies in der Regel dadurch unterstützt, dass jeder Mitarbeiter nur die tatsächlich notwendigen Zugriffsrechte auf die jeweiligen Daten erhält.
Die aktuelle Version des SDM in der Version 2.0b mit den Bausteinen (Maßnahmenkatalog) ist unter https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/ abrufbar.
Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit empfiehlt, regelmäßig das Konzept der Rollen, Zuständigkeiten und Berechtigungen zu überprüfen.

1.21 Künstliche Intelligenz muss dem Menschen dienen

Der Einsatz von Künstlicher Intelligenz wird zukünftig mehr und mehr zunehmen. Umso wichtiger ist es, dass die Einhaltung daten-

schutzrechtlicher Grundsätze auch für den Einsatz von KI sichergestellt werden und bestimmte Formen der Anwendung von KI frühzeitig als datenschutzrechtlich unzulässig erklärt werden.

Am 21. April 2021 legte die Europäische Kommission ihren Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (KI) vor.
Sowohl der EDSA (Europäische Datenschutzausschuss) als auch der EDSB (Europäische Datenschutzbeauftragte) begrüßten, dass die Verwendung von KI-Systemen in der Europäischen Union, darunter die Verwendung von KI-Systemen durch die Organe, Einrichtungen oder sonstigen Stellen der EU, reguliert werden soll. In ihrer gemeinsamen Stellungnahme (https://edpb.europa.eu/news/news/2021/edpb-edps-call-ban-use-ai-automated-recognition-human-features-publicly-accessible_de) zum Entwurf der Europäischen Kommission unterstrichen sie ausdrücklich die herausragende Bedeutung des Datenschutzes bei der Nutzung von KI. So forderten sie, dass klarzustellen ist, dass die bestehenden EU-Rechtsvorschriften zum Datenschutz (Datenschutz-Grundverordnung, EU-Datenschutz-Grundverordnung und Richtlinie zum Datenschutz bei der Strafverfolgung) auf jede Verarbeitung personenbezogener Daten anwendbar sein müssen, die in den Anwendungsbereich des Vorschlags für die KI-Verordnung fällt.
Angesichts der extrem hohen Risiken in Verbindung mit der biometrischen Fernidentifizierung von Personen im öffentlichen Raum forderten sie zudem ein generelles Verbot der Verwendung von KI für die automatisierte Erkennung menschlicher Merkmale im öffentlichen Raum, egal in welchem Kontext, darunter die Gesichts-, Gang-, Fingerabdruck-, DNA-, Stimm- und Tippverhaltenserkennung sowie die Erkennung anhand anderer biometrischer oder verhaltensbezogener Charakteristika.
Weiterhin empfahlen der EDSA und der EDSB ein Verbot von KI-Systemen, die Personen mithilfe von Biometrie aufgrund ihrer ethnischen Zugehörigkeit, ihres Geschlechts, ihrer politischen oder sexuellen Orientierung oder anderer Gründe in Gruppen einteilen, für die ein Diskriminierungsverbot gemäß Artikel 21 der Charta der Grundrechte besteht.
Auch sind sie der Auffassung, dass die Verwendung von KI für Rückschlüsse auf die Emotionen einer natürlichen Person keinesfalls wün-

schenswert ist und verboten werden sollte, wobei nur für sehr spezifische Fälle, wie zum Beispiel medizinische Zwecke, bei denen die Erkennung der Emotionen der Patienten wichtig ist, Ausnahmen vorgesehen werden sollten. Zudem sollte die Verwendung von KI für die Bewertung des sozialen Verhaltens („Social Scoring“) verboten werden.
Auch der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) hatte sich im EDSA dafür eingesetzt, dass der Einsatz von KI verboten wird, wenn sie die Persönlichkeit und Würde des Menschen nicht achtet. Entsprechend seiner Pressemitteilung im Juni 2021 weist er ausdrücklich darauf hin: „Denn solche Systeme verarbeiten häufig personenbezogene Daten, die große Risiken für die Rechte und Freiheiten von Menschen darstellen. Wir wollen keine KI im grundrechtlichen Graubereich. Ich setze mich für ein Verbot von KI ein, die einem freiheitlich-demokratischen Grundverständnis zuwiderläuft.“
Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit verfolgt die Diskussion auf europäischer Ebene ebenfalls und hat in seiner Pressemitteilung vom 22. Juni 2021 auf die Stellungnahme des BfDI hingewiesen, um so auch die Thüringer und Thüringerinnen für dieses Thema frühzeitig zu sensibilisieren (https://tlfdi.de/fileadmin/tlfdi/presse/Pressemitteilungen_2021/210622_PM_zur_PM_BfDI_KI_muss_dem_Menschen_dienen.pdf).

1.22 Sicherheitslücke bei Microsoft-Exchange-Server

Die Exchange-Lücke „Hafnium“ verursacht seit März 2021 auch innerhalb Thüringens weiter Probleme. Die Nachwirkungen sind auch Ende 2021 noch nicht ausgestanden. Der TLfDI empfiehlt allen Betreibern, weiterhin wachsam zu sein und grundlegende Sicherheitsvorkehrungen unbedingt einzuhalten.

Anfang März 2021 wurde praktisch über Nacht eine Sicherheitslücke bekannt, welche es Angreifern weltweit erlaubte, auf Exchange-Servern als unberechtigte Exchange-Administratoren umfassende Zugriffe und Manipulationen durchzuführen. Nach Angaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI) waren allein in Deutschland zehntausende Exchange-Server betroffen. Die Software Exchange ist eine von Microsoft entwickelte Software, um E-

Mail-Server zu betreiben, welche die E-Mails von Nutzern an andere Server verschicken oder von diesen empfangen kann. Daher ist diese Software häufig sehr eng mit dem Nutzermanagement verbunden und „kennt“ damit alle Benutzer, für welche der Exchange-Server seine Dienste verrichten soll.
Dass Sicherheitslücken für solch komplexe Software entdeckt werden, ist für sich genommen nichts Ungewöhnliches und passiert regelmäßig. Außergewöhnlich war diesmal aber, dass die Sicherheitslücke ohne Vorwarnung und Vorbereitungszeit veröffentlicht wurde. So hatte am Tag der Veröffentlichung weder Microsoft entsprechende Sicherheits-Updates zur Verfügung gestellt, welche die Lücke schließen konnten, noch gab es einen sinnvollen Workaround, welcher die Lücke vor Angreifern verstecken konnte. Im Ergebnis waren durch das verspätete Sicherheits-Update von Microsoft die betroffenen Exchange-Server für mehrere Tage praktisch schutzlos angreifbar. Details zum Angriff findet man zum Beispiel unter https://devco.re/blog/2021/08/06/a-new-attack-surface-on-MS-exchange-part-1-ProxyLogon/ (sehr technisch) oder auf der Website des BSI: https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2021/2021-197772-1132.html. Diese Sicherheitslücke ist auch unter dem Namen „Hafnium“ bekannt, da entsprechend einer Veröffentlichung auf „heise.de“ Microsoft eine mutmaßlich staatsnahe, aus China operierende Gruppe namens Hafnium für die Angriffe verantwortlich sieht.
Auch in Thüringen waren Exchange-Server betroffen. Dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) wurden zahlreiche Meldungen nach Art. 33 Datenschutz-Grundverordnung gemeldet, also, dass eine Verletzung des Schutzes personenbezogener Daten durch den Verantwortlichen festgestellt wurde. Häufig war aber den Meldenden gar nicht klar, ob das eigene Serversystem nun befallen war oder nicht, sondern die Meldungen erfolgten „auf Verdacht“, um nichts falsch zu machen. Hier wurde durch den TLfDI fallbezogen nachgefragt, welche Auffälligkeiten es eventuell gab oder welche Anhaltspunkte vorlagen, dass das gemeldete Exchange-System tatsächlich von Angreifern kompromittiert wurde. So können Spuren von ungewöhnlichen Zugriffen mit Administrationsrechten in Systemlogs gefunden werden oder auch direkt Schadcode an bestimmten Stellen des Exchange-Servers. In einigen Fällen konnten so tatsächlich Hinweise auf einen Angriff gefunden

werden – oftmals war die Suche aber erfolglos. Ursache könnte beispielsweise sein, dass bei geringen Aktivitäten der Angreifer, der Angriff nicht bemerkt wird, der Exchange-Server aber trotzdem unter Fremdkontrolle steht.
Auffällig wurde dies viele Monate später, als vermehrt erneut Meldungen beim TLfDI eintrafen, dass Exchange-Server plötzlich selbstständig E-Mails versenden oder Verschlüsselungstrojaner ganze Netzwerke außer Funktion gesetzt haben. Dem TLfDI liegen mehrere Untersuchungen vor, dass hier ein kompromittierter Exchange-Server die Ursache war. Die Angreifer konnten dabei jeweils unterschiedlich weit in die Systemlandschaften der betroffenen Organisation eindringen. Bei den meisten war aber ihr Zugriff nur auf den Exchange-Server beschränkt und so wurden dort lediglich E-Mails unter fremden Namen versendet oder die Kontakte der Nutzer ausgelesen. In Einzelfällen war jedoch auch die Ausbreitung der Angriffe auf das Netzwerk des Verantwortlichen möglich. Dann kam es zu Datendiebstahl, Verschlüsselung und umfänglichen Ausfällen. Die Ursachen für die tiefen Zugriffe auf andere Server sind im Nachgang schwer zu ermitteln, aber es dürften zu umfassende Nutzungsrechte des Exchange-Administrators am Rest der IT-Infrastruktur als Hauptursache wahrscheinlich sein. Aufgrund der so gesammelten überblicksmäßigen Erfahrungen des TLfDI können in Hinblick auf die Hafnium-Lücke folgende zwei Hinweise gegeben werden:

- Einschränkung der Rechte der Exchange-Administratoren auf ein Minimum an allen anderen Systemen im Netzwerk, bei welchen die Exchange-Administratoren auch Zugriffsrechte besitzen,
- Anlegen von Backups, sodass diese auf externen Datenträgern gespeichert, sowie vor Zugriff gesichert werden und nicht als Netzlaufwerke sichtbar sind (siehe dazu auch folgende Hinweise des BSI: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Gefaehrdungen/Fortschrittliche-Angriffe/Fortschrittliche-Angriffe_node.html, Maßnahmenkatalog Ransomware, Kapitel 2).

Natürlich können durch Monitoring, Anomalieerkennung und zentrales Logging weitere Maßnahmen getroffen werden, um schadhaftes Verhalten zu erkennen, aber die oben genannten zwei Maßnahmen sind grundlegend und sollten von jedem Verantwortlichen, welcher einen Exchange-Server einsetzt, beachtet werden.

1.23 Roboter für Gangtraining

Der TLfDI achtet auf Datenschutzkonformität im Rahmen eines Forschungsprojekts zum Einsatz eines mobilen Roboters im Klinikbereich. Dabei stellen sich zahlreiche Fragen zur Anonymisierung von personenbezogenen Daten, zur Sicherung der Patientendaten und Klärung, welche Daten nicht dem Patienten zuzuordnen sind. Der TLfDI achtet hier besonders auf eine datensparsame Verarbeitung, sodass nur die langfristig notwendigen Daten des Patienten gespeichert werden und der Rest nach kurzer Zeit anonymisiert wird.

Im Zuge der Digitalisierung werden neue Technologien auf alle denkbaren Lebensbereiche angewendet, wie auch im Bereich der Gesundheitsvorsorge und Diagnostik. Neben klassischen Messmethoden durch medizinische Geräte kommen auch eher ungewöhnliche Untersuchungsmethoden zunehmend zum Einsatz. So beobachtet der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) die Entwicklung eines Robotikprojektes, bei welchem ein mobiler Roboter im Krankenhaus zum Einsatz kommen und dort diagnostische Messungen und Beobachtungen an Patienten durchführen soll. Dabei ist der mobile Roboter nicht in einer abgeschlossenen, kontrollierten und menschenleeren Umgebung aktiv, sondern wird im normalen Krankenhausbetrieb in den öffentlich zugänglichen Bereichen eingesetzt. Hier müssen die Patienten bestimmte Aufgaben erfüllen und werden vom Roboter über klassische Kameras und Tiefenkameras beobachtet. Die Beobachtung dient der medizinischen Beurteilung des Gesundheitszustandes des Patienten, welche wiederum durch Ärzte erfolgt.
Natürlich stellen sich für den Einsatz eines solchen Systems zahlreiche datenschutzrechtliche Fragen. So kann der Roboter während seines Einsatzes nicht nur Patienten beobachten, sondern nimmt auch Besucher, Angestellte und andere Patienten wahr. Im fertig entwickelten Zustand speichert der Roboter keine der Wahrnehmungen, sondern fügt die Hindernisposition von Personen lediglich seiner internen Karte hinzu. Nur die beobachteten Patientendaten (zum Beispiel das Laufmuster) werden zur ärztlichen Auswertung gespeichert. Alle weiteren personenbeziehbaren Daten werden verworfen. In der Entwicklungsphase erfolgt auch eine Aufzeichnung der Rohdaten der Sensoren (Laserscanner, Tiefenkamera und optische Kameras). Im täglichen Einsatz fallen in der Entwicklungsphase so große Datenmengen an,

dass diese nicht lokal auf dem Roboter gespeichert werden können, sondern separat hinterlegt werden müssen. Sowohl die Speicherung der Personendaten auf dem Roboter als auch im separaten Speicher muss sicher sein und sollte nach Möglichkeit nur die Patientendaten enthalten, welche bei den Übungssitzungen vom Roboter erfasst werden (zum Beispiel Laufmuster, Haltungsprobleme und so weiter). Weiterhin handelt es sich um ein Forschungsprojekt, wodurch zur Entwicklung der notwendigen Algorithmen und Methoden auch Trainingsdaten gewonnen werden müssen. Obwohl noch nicht alle Fragen des Projektes geklärt wurden, ist durch den TLfDI Wert darauf gelegt worden, dass die Anwendungen auf dem Roboter möglichst datensparsam gemäß Art. 5 Abs. 1 Buchstabe c) Datenschutz-Grundverordnung arbeiten und sich darauf fokussieren, nur die erforderlichen Daten langfristig zu speichern. Dabei wurde auch auf die technischen Möglichkeiten des Roboters Rücksicht genommen, um rechenintensive Anonymisierungsmethoden dann auszuführen, wenn der Roboter dies von der Rechenlast ermöglicht. Um den Roboter datenschutzfreundlich (das heißt datensparsam) zu betreiben, wurde zum Beispiel vereinbart, Gesichter von Passanten/Personal direkt auf dem Roboter zu verpixeln, sobald die Rechenkapazität dazu verfügbar ist (das heißt regelmäßig in der Nacht). Da Patienten-IDs in jedweder Form personenbezogene Daten (Pseudonyme) sind, müssen diese auch durch technische Maßnahmen wie Verschlüsselung, sehr enge Zugriffsrechte und möglichst kurze Speicherdauern auf dem Roboter entsprechend geschützt werden. Aufgenommene Bewegungsmuster sind ebenfalls personenbezogene Daten. Die daraus entstehenden diagnostischen Daten sind ebenfalls personentypisch und damit entsprechend zu schützen. Da es sich um Gesundheitsdaten handelt, sind diese nach Art. 9 Abs. 1 DS-GVO „besondere Kategorien“ von personenbezogenen Daten und dadurch besonders schützenswert. Die technischen und organisatorischen Maßnahmen müssen daher in allen Bereichen der Datenverarbeitung entsprechend hoch ausfallen. Auch der dauerhafte externe Speicherort der Daten sollte daher im Krankenhaus liegen und keine öffentliche Cloud gewählt werden (auch wenn diese Verschlüsselung anbietet), da die Verarbeitungen lokal vollständig kontrolliert werden können müssen und auch die IT-Sicherheitsstruktur des Krankenhauses vollständig bekannt ist. Dadurch kann eine sehr kontrollierte und kontrollierbare Verarbeitungsumgebung genutzt werden. Hier muss sich der TLfDI noch über die genauen Speichermodalitäten

und die Einbettung des Speichersystems in der Krankenhauslandschaft mit der Entwicklerfirma abstimmen.
Neben diesen eher klassischen Datenschutzbetrachtungen gibt es aber auch interessante neue Datenkategorien, bei welchen der Personenbezug bisher unklar beziehungsweise unbewiesen ist. Hierbei handelt es sich primär um die Tiefendaten, welche ähnlich einer Digitalkamera pro Bildpunkt keinen Farbwert liefern, sondern wie weit das nächste Hindernis vom Sensor entfernt ist. Ein „Gesicht“ besteht in den vorliegenden Aufnahmesituationen dabei nur aus wenigen Tiefenpunkten (der gesamte Patient muss für die medizinische Diagnostik von Kopf bis Fuß sichtbar sein und entsprechend klein ist dadurch das Gesicht aufgelöst), sodass hier keine biometrischen Merkmale aus den Gesichtsdaten ableitbar sind. Liegen außergewöhnliche Features im Körperbau vor, ist dagegen ein Personenbezug herstellbar. Daher wurde vereinbart, sicherheitshalber die Tiefenbilddaten, welche nicht den Patienten betreffen, ebenfalls so zu verrauschen, dass kein Personenbezug herstellbar ist. Da noch keine Algorithmen dafür bekannt sind, wie dies umsetzbar ist, muss diesbezüglich ein geeignetes Verfahren in diesem Projekt experimentell gefunden werden.
Sollte dies gelingen, könnte es aus datenschutzrechtlicher Sicht auch für andere Projekte interessant sein. Diese Daten sollen dann ebenfalls in der Nacht anonymisiert werden.
Der TLfDI wird das Projekt daher mit Interesse weiterverfolgen und für Datenschutzkonformität sorgen.

2. Fälle öffentlicher Bereich



© DOC RABE Media - Rathaus - fotolia.com

2.1 Der Angemessenheitsbeschluss vom 28.06.2021 für GB als Folge des Brexits

Reisende soll man nicht aufhalten, sagt der Volksmund: Auch, wenn die Mehrheit der Briten im Vereinigten Königreich im Jahr 2016 dessen Austritt aus der Europäischen Union gefordert hatte, gilt nach dem Angemessenheitsbeschluss der Europäischen Kommission vom 28. Juni 2021 in „Good Old Britain“ immer noch ein Datenschutzniveau, das der Sache nach jenem gleichwertig ist, was die DS-GVO garantiert. Und die EU-Kommission hat sogar versprochen, dies in den nächsten drei Jahren weiter zu überprüfen – frei nach dem Motto einer englischen Sketch-Episode, in der es alljährlich zu Silvester im Fernsehen heißt: „I’ll do my very best!“

Als Einstieg ein Blick zurück auf den 24. Dezember 2020: Während sich in ganz Europa die Menschen auf das Weihnachtsfest, den Weihnachtsbraten und das Geschenkeauspacken freuten, war in Arbeitszimmern der EU-Kommission in Brüssel und in den Büros der britischen Regierung noch längst kein Weihnachtsfrieden eingezogen. Der Grund dafür war der vom Vereinigten Königreich bereits mehrfach angestrebte, aber immer noch nicht rechtlich geregelte Austritt aus der Europäischen Union (EU), der seinen Auslöser im Referendum vom 23. Juni 2016 hatte, als knapp 52 Prozent der Britischen Wählerinnen und Wähler für „Leave“ (= verlassen) also den Austritt aus der EU

gestimmt hatten. Nun also, am 24. Dezember 2020 konnten die Unterhändler der britischen Regierung und der EU-Kommission sich auf ein umfassendes Freiheitshandels- und Kooperationsabkommen einigen, dass in letzter Minute auch ein drohendes Datenchaos verhinderte: In diesem Abkommen-Paket bestimmten die EU-Kommission und die britische Regierung auch eine sechsmonatige Übergangsfrist für einen freien Datenaustausch. Dies war auch bitternötig, denn anderenfalls wäre das Vereinigte Königreich plötzlich zu einem sogenannten Drittland geworden. Angesichts der erheblichen Vernetzung zwischen der europäischen und der britischen Wirtschaft wäre ein Chaos bei der Übermittlung personenbezogener Daten entstanden, das sicher schnell wirtschaftliche Nachteile und Schäden auf beiden Seiten zur Folge gehabt hätte. Dass es aber nicht so weit kam, dafür sorgte in dem oben genannten Abkommen zunächst eine vereinbarte, mehrmonatige Übergangsfrist, während der der gemeinsame Datenverkehr zwischen den Mitgliedstaaten der Europäischen Union und dem Vereinigten Königreich wie bisher weiter fließen konnte. Gleichwohl mussten sich beide Seiten sputen, um die Verarbeitung personenbezogener Daten künftig auf eine neue Rechtsgrundlage zu stellen. Die dafür vorgesehene Frist bis Ende April 2021 wurde aus Zeitgründen bis Ende Juni 2021 verlängert.

Am 28. Juni 2021 war es dann endlich so weit: Die EU-Kommission legte einen „Durchführungsbeschluss gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates zur Angemessenheit des Schutzes personenbezogener Daten durch das Vereinigte Königreich“ vor (https://ec.europa.eu/info/sites/default/files/decision_on_the_adequate_protection_of_personal_data_by_the_united_kingdom_-_general_data_protection_regulation_de.pdf).

Rechtsgrundlage für die Erarbeitung und den Erlass eines solchen Beschlusses ist Artikel 45 Abs. 3 der Europäischen Datenschutz-Grundverordnung (DS-GVO), der da lautet: *„Nach der Beurteilung der Angemessenheit des Schutzniveaus kann die Kommission im Wege eines Durchführungsrechtsaktes beschließen, dass ein Drittland, ein Gebiet oder ein oder mehrere spezifische Sektoren in einem Drittland oder eine internationale Organisation ein angemessenes Datenschutzniveau im Sinne des Absatzes 2 des vorliegenden Artikels bieten.“*

Die drei Hauptkriterien für die Existenz eines angemessenen Datenschutzniveaus benennt Artikel 45 Abs. 2 Buchstaben a bis c) DS-GVO wie folgt: Zu berücksichtigen sind:

- *„a) Die Rechtstaatlichkeit, die Achtung der Menschenrechte und Grundfreiheiten, die in dem betreffenden Land bzw. bei der betreffenden internationalen Organisation geltenden einschlägigen Rechtsvorschriften sowohl allgemeiner als auch sektoraler Art [...] sowie die Anwendung dieser Rechtsvorschriften, Datenschutzvorschriften, Berufsregeln und Sicherheitsvorschriften einschließlich der Vorschriften für die Weiterübermittlung personenbezogener Daten an ein anderes Drittland [...] die Rechtsprechung sowie wirksame und durchsetzbare Rechte der betroffenen Person und wirksame verwaltungsrechtliche und gerichtliche Rechtsbehelfe für betroffene Personen, deren personenbezogene Daten übermittelt werden,*
- *b) die Existenz und die wirksame Funktionsweise einer oder mehrerer unabhängiger Aufsichtsbehörden in dem betreffenden Drittland oder denen eine internationale Organisation untersteht und die für die Einhaltung und Durchsetzung der Datenschutzvorschriften, einschließlich angemessener Durchsetzungsbefugnisse, für die Unterstützung und Beratung betroffener Personen bei der Ausübung ihrer Rechte und für die Zusammenarbeit mit den Aufsichtsbehörden der Mitgliedstaaten zuständig sind,*
- *c) die von dem betreffenden Drittland bzw. der betreffenden internationalen Organisation eingegangenen internationalen Verpflichtungen oder andere Verpflichtungen, die sich aus rechtsverbindlichen Übereinkünften oder Instrumenten sowie aus der Teilnahme des Drittlands oder der internationalen Organisation an multilateralen oder regionalen Systemen insbesondere in Bezug auf den Schutz personenbezogener Daten ergeben.“*

Auf insgesamt 109 Seiten (in der deutschen Übersetzung) legte die EU-Kommission diese gerade genannten Vorgaben als Maßstab ihrer Prüfung an und kam zu folgenden Ergebnissen in ihrem Durchführungsbeschluss:

- Bereits vor dem Austritt und während des Übergangszeitraums bis zum 31. Dezember 2020 habe der Rechtsrahmen für den Schutz personenbezogener Daten im Vereinigten Königreich aus den einschlägigen EU-Vorschriften, insbesondere aus der Verordnung (EU) 2016/679 (= DS-GVO) und der Richtlinie (EU) 2016/680 (= die JI-Richtlinie) des Europäischen Parlaments und des Rates sowie nationalen Rechtsvorschriften, insbesondere dem Gesetz über den Datenschutz von 2018 (Data Protection Act 2018 – **nachfolgend DPA 2018**) bestanden.

- Zur Vorbereitung auf den Austritt aus der Europäischen Union habe die Regierung des Vereinigten Königreiches das Gesetz über den Austritt aus der Europäischen Union von 2018 **(European Union (Withdrawal) Act 2018)** erlassen, mit dem unmittelbar geltende Rechtsvorschriften der Union in das Recht des Vereinigten Königreiches übernommen wurden. Dieses beibehaltene EU-Recht umfasse die Verordnung (EU) 2016/679 (also die DS-GVO) in all ihren Teilen, einschließlich ihrer Erwägungsgründe. Laut diesem Gesetz müsse das unverändert beibehaltene EU-Recht von den Gerichten des Vereinigten Königreichs gemäß der einschlägigen Rechtsprechung des Europäischen Gerichtshofs und den allgemeinen Grundsätzen des Unionsrechts ausgelegt werden, so wie sie unmittelbar vor dem Ende des Übergangszeitraumes gelten.
- Aufgrund dessen besteht – so die EU-Kommission – der rechtliche Rahmen für den Schutz personenbezogener Daten im Vereinigten Königreich nach dem Ende der Übergangszeit aus **dem UK GDPR, wie sie durch den European Union (Withdrawal Act 2018)** in das Recht des Vereinigten Königreichs übernommen wurde, und aus der **DPA 2018.** Deshalb gelangt die UK-Kommission zu folgendem Fazit: *„Da die UK GDPR auf einem EU-Rechtsakt basiert, geben die Datenschutzvorschriften im Vereinigten Königreich in vielen Aspekten weitgehend die entsprechenden innerhalb der Europäischen Union geltenden Vorschriften wieder.“*
- Hinsichtlich der Unabhängigkeit der Britischen Datenschutzaufsichtsbehörde und ihrer Befugnisse gelangte die EU-Kommission zu folgenden Ergebnissen: Im Vereinigten Königreich sei der Information Commissioner für die Überwachung und Durchsetzung der Einhaltung des UK GDPR und des DPA 2018 zuständig. Der Information Commissioner sei ein eigenständiges Rechtssubjekt, das aus einer einzigen Person bestehe, in seiner Arbeit aber mit Stand vom 31. März 2020 von 768 Festangestellten unterstützt werde. Die Befugnisse des Information Commissioners seien in Artikel 58 UK GDPR festgelegt, der keine wesentlichen Änderungen gegenüber dem entsprechenden Artikel in der DS-GVO umfasse.
- Schließlich kam die EU-Kommission auf der Grundlage ihrer verfügbaren Informationen über die Rechtsordnung des Vereinigten Königreichs zu der Auffassung, dass jeder Eingriff britischer

Behörden in die Grundrechte der Personen, deren personenbezogene Daten aus der Europäischen Union in das Vereinigte Königreich zu Zwecken des öffentlichen Interesses, insbesondere zu Zwecken der Strafverfolgung und der nationalen Sicherheit, übermittelt werden, auf das zur Erreichung des betreffenden rechtmäßigen Ziels unbedingt erforderliche Maß beschränkt ist und dass ein wirksamer Rechtsschutz gegen derartige Eingriffe bestehe.

Kritik an dem Angemessenheitsbeschluss wurde insbesondere dahingehend geübt, dass die Regulierungen im Datenschutzrecht des Vereinigten Königreichs möglicherweise keinen hinreichenden Schutz beim Datentransfer in andere Drittstaaten gewährleisten. Weiterhin rügten Datenschützerinnen und Datenschützer, dass es datenschutzrechtliche Ausnahmeregelungen für die Zwecke der Einwanderungskontrolle gebe.

Der skizzierte Angemessenheitsbeschluss gilt aber nicht zeitlich unbeschränkt, sondern hat zunächst eine Laufzeit von vier Jahren, bis zum 27. Juni 2025. Bis dahin will die EU-Kommission mittels festgelegter Verfahren prüfen, ob das Datenschutzniveau in Großbritannien sich auch weiterhin auf dem geforderten Niveau bewegt.

2.2 „The Never Ending Story“ – Der „Jungbrunnen“ für Prüffristen bei der Thüringer Polizei

§ 5 Thüringer Verordnung über Prüffristen bei vollzugspolizeilicher Datenspeicherung (ThürPolPrüffristVO) gilt als „Jungbrunnen“ bei Prüf- und Löschfristen personenbezogener Daten, die die Polizei speichert. Soweit innerhalb der Speicherfrist eines Ereignisses (Straftat) ein neues Ereignis (Straftat) hinzukommt, beginnt die Prüffrist neu zu laufen. Dies hat zur Folge, dass auch die vergangenen Ereignisse nunmehr der neuen Speicherungsfrist unterliegen.

Die datenschutzrechtliche Überprüfung der Erfassung personenbezogener Daten in polizeilichen Informationssystemen gehört unter anderem zum Tagesgeschäft des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Nicht selten kommt es vor, dass die Polizeivertrauensstelle bei der Landespolizeidirektion Erfurt Anliegen dieser Art zuständigkeitshalber an den TLfDI abgibt. Insbesondere war der betroffene Bürger in einem Fall aus dem Berichtszeitraum verwundert darüber, dass Verfahren über

ihn weiterhin im polizeilichen Informationssystem gespeichert wurden, obwohl diese bereits mehrere Jahre zurücklagen.
Zur Erfüllung der Aufgaben der Polizei werden rechtmäßig erlangte personenbezogene Daten befristet gespeichert. Dennoch dürfen personenbezogene Daten nicht unendlich lange gespeichert werden. Daher wird sowohl im Einzelfall als auch nach festgelegten Fristen (Aussonderungsprüffristen) seitens der Polizei geprüft, ob die Voraussetzungen für eine Aufrechterhaltung der Speicherung noch vorliegen. Wie in den meisten ähnlich gelagerten Fällen richtete sich die Fristenberechnung im konkreten Fall nach § 40 Abs. 6 Polizeiaufgabengesetz (PAG) in Verbindung mit § 5 Thüringer Verordnung über Prüffristen bei vollzugspolizeilicher Datenspeicherung (ThürPolPrüffristVO). Die Prüffrist beginnt danach grundsätzlich mit dem Tag zu laufen, an dem das letzte Ereignis eingetreten ist, das zur Speicherung der Daten geführt hat. Dabei handelt es sich nicht um eine Verlängerung im Sinne des § 2 Abs. 4 ThürPolPrüffristVO, sondern die Prüffrist beginnt erneut zu laufen. Im Kommentar zum PAG (Ebert, Seel, 8. Auflage) zu § 40 Abs. 6, Satz 428, Randnummer 39 wird dies damit begründet, „dass sich eine Einzelfalllöschung in der Praxis als nicht umsetzbar erweist, weil sich das Erkenntnisdatum in einem Gesamtvolumen befindet und gerade bei Wiederholungstätern zu einer polizeilichen Erkenntnislücke führen würde“. Weiterhin heißt es: „Datenschutzrechtlich ist eine derartige Einzelfallprüfung nicht geboten, weil der Grundschutz durch Verfahren lediglich eine angemessene, nicht aber eine optimale Verfahrensgestaltung fordert.“
In der Praxis bedeutet dies, dass, soweit innerhalb der Speicherfrist eines Ereignisses (Straftat) ein neues Ereignis (Straftat) hinzukommt, die Prüffrist neu zu laufen beginnt. So war es auch im konkreten Fall. Dies hatte zur Folge, dass auch die vergangenen polizeilichen Verfahren nunmehr dieser neuen Speicherungsfrist unterlagen. Aufgrund der Art der Straftaten (Verstoß gegen das Betäubungsmittel- und Waffengesetz und Widerstand gegen Vollstreckungsbeamte) wurde für die Vorgänge des Betroffenen gemäß § 2 Abs. 1 ThürPolPrüffristVO eine Prüffrist von fünf Jahren festgelegt. Für den Betroffenen hatte dies zur Folge, dass das Aussonderungsprüfdatum auf den August 2022 datiert wurde. Fallen bis zu diesem Datum keine weiteren Straftaten an, erfolgt sodann die Löschung seiner Datensätze.
Aus datenschutzrechtlicher Sicht hält der TLfDI diesen „Jungbrunnen“ für Prüf-/ Löschfristen für nicht akzeptabel. Vielmehr sollte für jedes einzelne Ereignis auch eine separate Prüffrist gelten. Dabei ist

entscheidend, dass die Akten anlässlich der Einzelfallbearbeitung oder nach Ablauf der jeweiligen Prüffrist „in die Hand genommen“ beziehungsweise elektronisch gesichtet werden, eine Erforderlichkeitsprüfung durchgeführt und in diesem Zusammenhang entweder eine weitere Prüffrist (nur für das jeweilige Ereignis) festgelegt wird oder die Daten gelöscht beziehungsweise vor Aktenvernichtung dem Archiv angeboten werden. Der TLfDI verfolgt nach wie vor das Ziel einer normativen Klärung in dieser Rechtsfrage.

2.3 Auskunftsverlangen der Thüringer Polizei – am Ende unrechtmäßig

Neben einer Rechtsgrundlage für ein Auskunftsverlangen der Polizei oder Staatsanwaltschaft ist immer schon im Vorfeld auch die Rechtsgrundlage für die Antwort durch das Unternehmen oder die öffentliche Stelle, die Auskunft erteilen soll, im Blick zu behalten. Dies gilt allerdings nicht für den Bereich der ermittlungsrichterlichen Beschlüsse in strafrechtlichen Ermittlungsverfahren; diese sind selbst zunächst ausreichende Grundlage für die Rechtspflichten des Auskunftsgebenden, können aber im strafgerichtlichen Beschwerdeverfahren überprüft und – wie der nachfolgende Fall zeigt – aufgehoben werden.

Ein Unternehmen, welches unter anderem in Thüringen als Carsharing-Anbieter Fahrzeuge zur Anmietung bereitstellt, informierte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) im Berichtszeitraum darüber, dass dort regelmäßig Anfragen von verschiedenen Polizeidienststellen sowie auch vom Landeskriminalamt (LKA) in Thüringen zu einzelnen Fahrten der Nutzer des Carsharing-Angebots eingehen würden. Das Unternehmen führte dazu weiter aus, dass diese Auskunftsersuchen aus dortiger Sicht als (datenschutzrechtlich) problematisch bewertet werden, da gewisse Formalitäten nicht eingehalten würden. Beispielhaft für die behauptete regelmäßige Anfragepraxis verwies der Carsharing-Anbieter auf einen konkreten Sachverhalt, bei dem das Unternehmen im Rahmen eines Verfahrens wegen gefährlicher Körperverletzung durch das LKA Thüringen via E-Mail zur Herausgabe umfangreicher Datensätze für einen Zeitraum von zwei Tagen bezüglich aller von Kunden genutzten PKW des Unternehmens in Erfurt und Leipzig im Rahmen eines Verfahrens wegen gefährlicher Körperverletzung

aufgefordert worden war. Nach Angaben des Carsharing-Anbieters seien damit über 3.700 Fahrdatensätze inklusive Personenstammdaten (Name, Geburtsdatum, Adresse) angefordert worden. Durch das Unternehmen wurde in Bezug auf die konkrete Anfrage moniert, dass weder eine Rechtsgrundlage benannt, noch der konkrete Zweck der Maßnahme näher konkretisiert worden sei. Zudem wandte sich das Unternehmen auch gegen die formale Gestaltung der Anfrage, da diese per unverschlüsselter E-Mail an eine zentrale E-Mail-Adresse erfolgt sei. Die Anfrage habe zudem keine Vorgangsnummer, Tatvorwürfe oder Ermittlungsgrundlagen enthalten. Als problematisch wurde auch erachtet, dass keinerlei Eingrenzung der Daten erfolgt und keinerlei Begründung für den Umfang der Abfrage gegeben worden sei. Im Rahmen der datenschutzrechtlichen Prüfung konsultierte der TLfDI zunächst das LKA Thüringen, um zum einen bezogen auf den vom Carsharing-Anbieter beispielhaft vorgebrachten Sachverhalt eine Bewertung vornehmen zu können, und zum anderen auch, um Informationen zur allgemeinen Praxis des LKA Thüringen bei Auskunftsersuchen gegenüber Carsharing-Anbietern zu erlangen. Das LKA Thüringen bestätige daraufhin die tatsächlichen Gegebenheiten hinsichtlich der beschwerdegegenständlichen Anfrage, wobei solche Anfragen allerdings kein standardisierter, regelmäßiger Prozess seien. Umfang und Form der Anfrage würden sich aus dem konkreten Einzelfall ergeben. Im Ergebnis der datenschutzrechtlichen Prüfung stellte der TLfDI schließlich fest, dass ein Verstoß gegen datenschutzrechtliche Vorschriften im durch das Unternehmen speziell gerügten Fall nicht vorlag, weil es nicht zu einer Verarbeitung der personenbezogenen Daten aufgrund der Anfrage des LKA Thüringen gekommen ist. Diese Feststeng begründete sich wie folgt: Aufgrund des „Doppeltürprinzips“ stellt sich das Problem, dass die Übermittlung auf eine möglicherweise ungenügende Anfrage hin im Zweifel keinen Verstoß des LKA Thüringen darstellen muss. Das „Doppeltürprinzip“ besagt, dass einerseits der Inhaber des Datenbestandes rechtlich berechtigt und verpflichtet sein muss, Daten zu übermitteln, und andererseits die für die Aufgabe zuständige Behörde berechtigt sein muss, die Daten für den Zweck abzurufen. Die Abfrage und die Übermittlung sind dabei zwei verschiedene, aufeinander aufbauende, aber rechtlich zu trennende Vorgänge. Die fehlende Berücksichtigung der „zweiten Tür“ im Rahmen des Doppeltürprinzips schon bei der Gestaltung der Auskunftsanfrage durch das LKA stellt hierbei keinen Verstoß dar, wobei

anzumerken ist, dass sich diese Rechtslage für das Unternehmen gegebenenfalls als problematisch darstellt, da die Übermittlung auf Grundlage einer ungenügenden Anfrage wiederum einen Verstoß des Übermittlers – sprich vorliegend des Carsharing-Anbieters – darstellen kann. Ein Verstoß durch Verarbeitungen personenbezogener Daten ohne Rechtsgrundlage wurde im vom Carsharing-Anbieter vorgetragenen Fall zunächst durch die Verweigerung der Auskunft seitens des Unternehmens verhindert. Für die danach doch erfolgte Herausgabe der personenbezogenen Daten durch das Unternehmen bestand durch einen ermittlungsrichterlichen Beschluss (dieser Gerichtsbeschluss liegt außerhalb der Prüfungskompetenz des TLfDI, siehe § 2 Abs. 1 Satz 1, Abs. 9 Satz 1 und Satz 2 Thüringer Datenschutzgesetz) zunächst eine Rechtsgrundlage, die aber im dafür vorgesehen und vorrangigen Rechtsbehelf, einem strafgerichtlichen Beschwerdeverfahren vor dem Landgericht Erfurt, beseitigt wurde. Mit dem Rechtsmittel der Beschwerde gemäß § 304 ff. Strafprozessordnung (StPO) kann grundsätzlich jede richterliche Maßnahme angefochten werden, die im ersten Rechtszug oder im Berufungsverfahren von einem Gericht erlassen wurde (§ 304 Abs. 1 Hs. 1). Statthaft ist eine Beschwerde gemäß § 304 StPO gegen richterliche Beschlüsse und Verfügungen, die etwa Hausdurchsuchungen und Beschlagnahmen betreffen können. Von der Möglichkeit einer solchen Rechtsbeschwerde gegen den gegenüber dem Carsharing-Anbieter im betreffenden Fall erlassenen amtsrichterlichen Durchsuchungs- und Beschlagnahmebeschluss sowie die bei dem Unternehmen erfolgte Beschlagnahme von Daten in Form eines Datensatzes auf einem USB-Stick wurde im betreffenden Fall erfolgreich Gebrauch gemacht. Nach Prüfung des angefochtenen Beschlusses in rechtlicher und tatsächlicher Hinsicht stellte das Landgericht Erfurt im weiteren Verlauf fest, dass dem verfassungsrechtlichen Erfordernis des tatsachenbasierten Gefahrenverdachts als Voraussetzung für die Datenübermittlung im betreffenden Fall nicht Genüge getan war, da zur Einleitung eines Ermittlungsverfahrens ein Anfangsverdacht vorausgesetzt ist, §§ 152 Abs. 2, § 160 Abs. 1 StPO. Dieser verlangt zureichende, objektive Anhaltspunkte für das Vorliegen einer verfolgbaren Straftat, die jedoch hier nicht vorlagen, woraus sich auch die Unverhältnismäßigkeit des Umfangs der angefragten Daten bei dem Carsharing-Anbieter ergab. Der amtsrichterliche Beschluss zur Datenbeschlagnahme wurde damit im Ergebnis vollumfänglich aufgehoben und die beschlagnahmten Daten mussten an das Unternehmen herausgegeben werden. Im Hinblick auf das Vorbringen

des Unternehmens, dass die Anfrage im konkreten Fall keine Vorgangsnummer und keinen Tatvorwurf beinhaltete, war dies für den TLfDI anhand der vorgelegten E-Mail nicht nachvollziehbar. Auch wenn damit ein Datenschutzverstoß vom TLfDI aufgrund seiner begrenzten Befugnisse im konkreten Fall nicht festgestellt werden konnte, so wurde die grundsätzliche Anfragepraxis des LKA Thüringern durch den TLfDI als verbesserungswürdig eingestuft. Denn ein Verstoß im konkreten Fall konnte nur durch das umsichtige Prüfverhalten des Carsharing-Anbieters abgewendet werden.
Der TLfDI übermittelte dem LKA Thüringen daher nach Abschluss der datenschutzrechtlichen Prüfung des Sachverhalts rechtliche Hinweise zur sachgerechten Gestaltung der Anfragepraxis im Hinblick auf datenschutzrechtliche Belange mit der Bitte um zukünftige Beachtung, weil bei dem Anfrageverhalten, wie es dem TLfDI im konkreten Fall bekannt wurde, zumindest datenschutzrechtliche Verstöße auf Seiten der übermittelnden Unternehmen nicht ausgeschlossen sind. Eine zukünftige Berücksichtigung der „zweiten Tür“ im Rahmen des Doppeltürprinzips schon bei der Gestaltung der Auskunftsanfrage liegt hier in beiderseitigem Interesse, da dies nicht nur der Rechtssicherheit für den Auskunftsgebenden dient, sondern letztendlich auch dem Eigeninteresse von LKA/Staatsanwaltschaft. Es versetzt die Unternehmen nämlich in die Lage, diese Anfragen schnell zu prüfen und im Regelfall dann auch eine Auskunft zu erteilen. Die Etablierung eines Auskunftsprozesses mit notwendigen Mindestangaben ist also für beide Seiten derartiger Auskunftsersuchen dienlich. Nebenbei stärkt es – und dies ist das Hauptinteresse des TLfDI im Rahmen dieser Sache – den Datenschutz bei den angefragten Unternehmen.

2.4 Ihr Auskunftsrecht beim Amt für Verfassungsschutz – ABER richtig!

Voraussetzung für einen korrekten Auskunftsantrag beim Amt für Verfassungsschutz ist eine Darstellung des Grundes des Auskunftsverlangens sowie der Art der personenbezogenen Daten, über die Auskunft erteilt werden soll. Auch eine einfache Kopie des Personalausweises für eine eindeutige Identifizierung ist unter Einschränkungen zulässig.

Immer wieder erreichen den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) Beschwerden über

verweigerte oder auch unzureichende Auskünfte zu personenbezogenen Daten durch das Amt für Verfassungsschutz (AfV). Daher erhalten Sie an dieser Stelle einen kurzen Überblick, welche Voraussetzungen für eine Auskunftserteilung durch das AfV erfüllt sein müssen:
Der Auskunftsanspruch gegenüber dem AfV, welches beim Thüringer Ministerium für Inneres und Kommunales angegliedert ist, ist abschließend spezialgesetzlich in § 17 Thüringer Verfassungsschutzgesetz (ThürVerfSchG) in Verbindung mit § 36 ThürVerfSchG und § 42 Abs. 1 Satz 2 und 3 Thüringer Datenschutzgesetz geregelt. Gemäß § 17 Abs. 1 ThürVerfSchG erteilt das AfV der beziehungsweise dem Betroffenen auf Antrag unentgeltlich Auskunft über die zu ihrer/seiner Person gespeicherten Daten. Die Auskunftsverpflichtung erstreckt sich kraft ausdrücklicher gesetzlicher Regelung (§ 17 Abs. 3 ThürVerfSchG) nicht auf die Herkunft der Daten und die Empfänger von Übermittlungen. Sie unterbleibt danach, wenn die betroffene Person keine Angaben macht, die das Auffinden der Daten ermöglichen und deshalb der für die Erteilung der Auskunft erforderliche Aufwand außer Verhältnis zu dem von der betroffenen Person geltend gemachten Informationsinteresse steht. In dem Antrag müssen somit zwingend die Art der personenbezogenen Daten, über die Auskunft erteilt werden soll, und der Grund des Auskunftsverlangens näher bezeichnet werden. Insoweit soll bei der Antragstellung eine Darstellung erfolgen, welche personenbezogenen Daten beim AfV durch den Betroffenen vermutet werden. Dies können beispielsweise allgemeine Personendaten, Kennnummern, Bankdaten, Patientendaten, physische Merkmale, Besitzmerkmale oder auch besonders schutzwürdige personenbezogene Daten, die in Art. 9 Nr. 1 Datenschutz-Grundverordnung definiert sind, sein.
Außerdem wird oftmals für die eindeutige Identifizierung des Antragstellers eine einfache Ausweiskopie verlangt. Dies ist grundsätzlich zulässig, einzelne Datenfelder auf der Personalausweiskopie kann der Betroffene dabei aber schwärzen, da sie für die Identifizierung nicht erforderlich sind (zum Beispiel Ausweisnummer, Größe, Augenfarbe).
Sind diese Voraussetzungen erfüllt, steht Ihrem Auskunftsantrag beim AfV nichts mehr entgegen. Sollten sie doch einmal Probleme bei Ihrer Antragsstellung haben, scheuen Sie sich nicht, sich an den TLfDI zu wenden.

2.5 Darf der Rechnungshof denn alles wissen?

Dem Thüringer Rechnungshof als unabhängiger Kontrollbehörde stehen im Rahmen seiner Prüfkompetenz weitgehende Erhebungsbefugnisse auch personenbezogener Daten zu, soweit dies für dessen Aufgabenerfüllung erforderlich ist. Das kann auch die Gehälter der Geschäftsführer oder Vergütungen der Aufsichtsorgane kommunaler Unternehmen umfassen, auch wenn diese ansonsten als „vertraulich" vereinbart wurden oder so eingestuft werden.

Im Rahmen einer überörtlichen Querschnittsprüfung der Betätigung der Thüringer Kommunen bei Unternehmen des privaten Rechts und bei kommunalen Anstalten des öffentlichen Rechts wandte sich eine Kommune an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und wollte sich rückversichern, ob sie dem Thüringer Rechnungshof (TRH) die geforderten Angaben zur Vergütungsstruktur der Geschäftsführungen und Aufsichtsorgane kommunaler Unternehmen übermitteln könne oder ob dem datenschutzrechtliche Gründe entgegenstünden. Immerhin handelt es sich bei den Gehältern und Vergütungen der namentlich zu benennenden Personen um vertraulich zu behandelnde Angaben, es sei denn, sie wären zur Veröffentlichung vorgesehen.
Das Prüfungsrecht des TRH ist in Art. 103 Abs. 3 der Verfassung des Freistaates Thüringen verankert. Nach §§ 88 und 92 Thüringer Landeshaushaltsordnung unterliegt „die gesamte Haushalts- und Wirtschaftsprüfung des Landes einschließlich seiner Sondervermögen und Betriebe" sowie auch staatliche Beteiligungen bei privatrechtlichen Unternehmen der Prüfung durch den THR. Näheres zum Prüfverfahren beim TRH findet sich in dem Thüringer Gesetz zur überörtlichen Prüfung der Haushalts- und Wirtschaftsprüfung und zur Beratung der Gemeinden und Landkreise (ThürPrBG). Gemäß § 1 Abs. 1 Satz 1 ThürPrBG obliegt die überörtliche Rechnungs- und Kassenprüfung nach § 83 Thüringer Kommunalordnung (ThürKO) und den §§ 3 und 4 des ThürPrBG dem Rechnungshof. Gemäß § 1 Abs. 1 Satz 2 ThürPrBG unterliegen alle kommunalen Körperschaften, auf die die Bestimmungen des Vierten Abschnitts des Ersten Teils der Thüringer Kommunalordnung Anwendung finden, der überörtlichen Rechnungs- und Kassenprüfung. Hierzu zählen auch Gemeindliche Unternehmen in der Rechtsform des privaten Rechts (§§ 73 ff. ThürKO) und Kommunale Anstalten des öffentlichen Rechts (§ 76a ThürKO).

Darüber hinaus hat sich der TRH eine Prüfungs- und Beratungsordnung (PBO-TRH) gegeben. Danach zieht der TRH personenbezogene und andere schutzwürdige oder geheim zu haltende Daten nur insoweit heran, als er sie zur Erfüllung seiner Aufgaben für erforderlich hält. Mit den gewonnenen Erkenntnissen aus den Prüfungen geht der TRH vertraulich um (§ 8 Abs. 1 Satz 1 PBO-TRH). Seine Prüfungsmitteilungen und Prüfberichte fasst der TRH grundsätzlich so ab, dass Rückschlüsse auf Drittbetroffene weder durch Namensnennung noch durch Angaben sonstiger Erkennungsmerkmale möglich sind (§ 9 Abs. 2 Satz 1 PBO-TRH).
Die (datenschutzrechtliche) Rechtmäßigkeit der im Rahmen der Prüftätigkeiten durch den TRH vorgenommenen Datenverarbeitungsvorgänge richtet sich nach §§ 16 und 17 Thüringer Datenschutzgesetz (ThürDSG). Gemäß § 16 Abs. 1 ThürDSG ist die Verarbeitung personenbezogener Daten durch eine öffentliche Stelle (Anmerkung: hier des TRH) dann zulässig, wenn sie zur Erfüllung der in der Zuständigkeit des Verantwortlichen im öffentlichen Interesse liegenden Aufgabe erforderlich ist oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Dies ist bei dem TRH der Fall.
Grundsätzlich sind personenbezogene Daten von der verantwortlichen Stelle nur „zweckgebunden“ zu verarbeiten, das heißt, Daten dürfen nur für den ursprünglich erhobenen Zweck verarbeitet werden (so auch Art. 5 Abs. 1 Buchstabe b) Datenschutz-Grundverordnung (DS-GVO)). Die hier abgefragten Daten und Gehälter der Geschäftsführer und Aufsichtsorgane von kommunalen Unternehmen in privater Rechtsform und kommunalen Anstalten der Jahre 2017 bis 2019 wurden von den verantwortlichen Stellen ursprünglich erhoben, um das Rechtsverhältnis zwischen der betroffenen Person und dem kommunalen Unternehmen/der kommunalen Anstalt (Bestellung als Geschäftsführer/Aufsichtsorgan) durchführen zu können, nicht jedoch um damit Prüfpflichten des TRH zu dienen. Datenschutzrechtlich bedarf jede Datenverarbeitung zu einem anderen Zweck als dem ursprünglichen und – wie hier – eine damit verbundene Weiterleitung an Dritte – einer Rechtsgrundlage. Jedoch sieht § 17 Abs. 1 Nr. 3 ThürDSG vor, dass die Verarbeitung „zur Rechnungsprüfung“ keinen über den ursprünglichen Zweck der Datenerhebung hinausgehenden Zweck darstellt. Mit anderen Worten: Übermittelt das kommunale Unternehmen/die kommunale Anstalt die Daten zur Rechnungsprü-

fung gegenüber dem TRH weiter, so ist dies vom ursprünglichen Erhebungszweck umfasst und bedarf keiner erneuten Rechtfertigung. Auch bedarf es in einem solchen Fall keiner Information nach Art. 13 Abs. 3 DS-GVO an die Betroffenen über die Weiterverarbeitung (siehe auch Gesetzesbegründung zu § 17 ThürDSG in Drucksache 6/4943 des Thüringer Landtags).
Was sich die Prüfer des TRH im Rahmen ihrer Prüfpflichten vorlegen lassen dürfen, richtet sich nach § 2 Abs. 1 und 2 ThürPrBG. Danach sind den Prüfern die *erforderlichen* Auskünfte zu erteilen (Abs. 1) und „die zur Prüfung *erforderlichen* Unterlagen auszuhändigen“ (Abs. 2 Satz 1). Damit kommt zum Ausdruck, dass der TRH in seiner umfassenden und weitgehenden Prüfungskompetenz auch nur diejenigen Auskünfte und Unterlagen verlangen darf, die er zur Prüfung seiner Aufgaben auch benötigt. Zu beachten ist dabei, dass die Prüfungen des TRH in der Regel stellen- und nicht personenbezogen erfolgen. Dies bedeutet nicht, dass dabei keine personenbezogenen Daten gemäß Art. 4 Nr. 1 DS-GVO an den TRH offengelegt werden dürften. Vielmehr betrachtet der TRH dabei die Ordnungsgemäßheit des Mitteleinsatzes öffentlicher Gelder, was nicht zwangsläufig mit bestimmten Personen verbunden ist. Zudem ist in § 19 Abs. 4 PBO-TRH geregelt, dass sich die Auskunfts- und Vorlageverpflichtungen auch auf vertraulich zu behandelnde oder geheim zu haltende Daten erstreckt. Gehaltsangaben zu Geschäftsführern oder Aufsichtsorganen kommunaler Unternehmen oder Anstalten wird man sicherlich als „vertraulich zu behandelnde Daten“ bezeichnen können. Jedoch wird man diese Angaben ebenso als *erforderlich* zur oben ausgeführten Aufgabenerfüllung des TRH als zuständige Prüfungsinstanz ansehen können.

2.6 Einmal Gerichtspost für ALLE?

Nach den Grundsätzen der DS-GVO sind personenbezogene Daten vor der unbefugten Offenlegung an Dritte zu schützen. Dies ergibt sich aus dem Grundsatz der Integrität und Vertraulichkeit gemäß Art. 5 Abs. 1 Buchstabe f) DS-GVO und gilt auch für Briefumschläge, mit denen Thüringer Gerichte personenbezogene Daten an Bürgerinnen und Bürger versenden.

Im Berichtszeitraum hat der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) Kenntnis davon erlangt, dass bei einem Thüringer Amtsgericht Briefumschläge mit

mangelhafter Klebeeigenschaft verwendet werden. Konkret wurde einem Bürger ein nicht verschlossener Brief in einer privaten Angelegenheit durch das Gericht zugestellt. So bestand zumindest die Möglichkeit der Preisgabe personenbezogener Daten an nicht berechtigte Dritte.
Im Rahmen seiner datenschutzrechtlichen Ermittlungen konnte durch den TLfDI tatsächlich festgestellt werden, dass die Briefumschläge bei dem betroffenen Gericht teilweise nicht zuverlässig schließen. Insbesondere bei stärkerer Füllung konnten sich die Klebestellen der Briefumschläge wieder lösen. Ein vom Gericht durchgeführter Test mit mehreren Briefumschlägen und unterschiedlicher Befüllung ergab, dass sich auch bei anfangs verschlossenen Umschlägen nach einigen Stunden die Klebestellen wieder lösen konnten. Der Direktor des Amtsgerichts hatte deshalb bereits in der Vergangenheit veranlasst, dass betreffende Umschläge immer mit einem zusätzlichen Klebestreifen verschlossen werden sollten.
Gemäß § 7 Abs. 1 Satz 5 Thüringer Datenschutzgesetz in Verbindung mit Artikel 58 und 83 der Datenschutz-Grundverordnung (DS-GVO) kann der TLfDI von einer weitergehenden Stellungnahme, mit welcher er Abhilfebefugnisse gegenüber der verantwortlichen Stelle geltend macht, absehen, wenn es sich um unerhebliche oder inzwischen beseitigte Mängel handelt. Der betroffene Bürger selbst hatte dem TLfDI im konkreten Fall mitgeteilt, dass er nicht von einer Öffnung der Briefe durch Dritte ausgehe und lediglich auf den Missstand aufmerksam machen wollte. Außerdem wurde durch den Direktor des Amtsgerichts der Vorfall zum Anlass genommen, zuständige Mitarbeiter nochmals darauf hinzuweisen, dass bei den derzeit verwendeten Umschlägen immer ein zusätzlicher Klebestreifen aufgebracht werden muss. Zudem wurde die zentrale Beschaffungsstelle über die mangelhafte Klebeeigenschaft der letzten Umschlaglieferung in Kenntnis gesetzt, sodass künftig andere, besser klebende Briefumschläge beschafft werden sollen. Damit wird dann dem Grundsatz der Integrität und Vertraulichkeit personenbezogener Daten gemäß Art. 5 Abs. 1 Buchstabe f) DS-GVO in dem gebotenen Umfang Rechnung getragen. Der Vorgang konnte daher beim TLfDI abgeschlossen werden.

2.7 Ein Jäger bläst zu laut zum Halali

Viel hilft nicht immer viel und ist erst recht nicht immer datenschutzkonform: Sofern eine Behörde für ein Verwaltungsverfahren die Akte mit personenbezogenen Daten von einer anderen Behörde anfordert und heranzieht, ist sie nicht zuletzt wegen des Prinzips der Datenminimierung aus Art. 5 Abs. 1 Buchstabe c) DS-GVO verpflichtet, nur jene Bestandteile mit personenbezogenen Daten aus der Akte zu verarbeiten, die für das Verwaltungsverfahren erforderlich sind. Dies gilt erst recht, wenn es sich um besondere Kategorien von personenbezogenen Daten gemäß Art. 9 Abs. 1 DS-GVO, im konkreten Fall um Gesundheitsdaten, handelt.

Durch die Beschwerde eines Betroffenen wurde der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) im Berichtszeitraum darauf aufmerksam, dass die Untere Jagdbehörde eines Landkreises im Rahmen der gesetzlich geforderten Überprüfung eines Jagdscheins eine vollständige Ermittlungsakte der Staatsanwaltschaft angefordert hatte. Grund für die Anforderung waren Einträge des Jagdschein-Inhabers im Bundeszentralregister. Diese Ermittlungsakte hatte die Untere Jagdbehörde erhalten und legte davon eine vollständige Kopie an.
In der Akte der Staatsanwaltschaft befand sich unter anderem ein Bescheid der Versorgungsverwaltung, den der Beschwerdeführer als Beschuldigter im Ermittlungsverfahren selbst zu den Akten gegeben hatte. Das Schreiben betraf verschiedene körperliche Behinderungen des Beschwerdeführers und erwähnte unter anderem auch eine „posttraumatische Angststörung“. Für die Untere Jagdbehörde ergaben sich hieraus Anhaltspunkte für Eignungszweifel im Hinblick auf den Beschwerdeführer aus Sicht des Bundesjagd- und Bundeswaffengesetzes. Die Untere Jagdbehörde ging daher davon aus, dass nach § 24 Thüringer Verwaltungsverfahrensgesetz im Rahmen der Untersuchung nach pflichtgemäßem Ermessen der Amtsarzt mit einzubeziehen sei, um die Bedeutung einer „posttraumatischen Angststörung“ für die Eignung und Zuverlässigkeit beurteilen zu können.
Zudem befanden sich in der staatsanwaltlichen Ermittlungsakte mehrere Seiten mit Bankkonto-Informationen sowie ein Vermögensverzeichnis des Beschwerdeführers, die ebenfalls durch die Untere Jagdbehörde kopiert wurden.

Kopiert wurde die gesamte Akte zunächst deshalb, weil die Untere Jagdbehörde keine Gesamtsichtung und -bewertung der Akte dahingehend vorgenommen hatte, welche erforderlichen Informationen sie daraus für die Überprüfung des Jagdscheins benötigte.
Im Laufe des Beschwerdeverfahrens beim TLfDI räumte die Untere Jagdbehörde ein, dass ein Großteil der Aktenbestandteile zur Verarbeitung nicht erforderlich war. Diese Teile wurden sodann aus der Akte entfernt und datenschutzkonform vernichtet. Der zuständige Mitarbeiter wurde hinsichtlich der Anforderungen an Kopien sensibilisiert und die Untere Jagdbehörde kündigte datenschutzrechtliche Schulungen durch den behördlichen Datenschutzbeauftragten an.
Gemäß Art. 6 Abs. 1 Satz 1 Buchstabe e), Abs. 3 Datenschutz-Grundverordnung (DS-GVO) in Verbindung mit § 16 Thüringer Datenschutzgesetz (ThürDSG) ist die Verarbeitung personenbezogener Daten durch eine öffentliche Stelle zulässig, wenn sie zur Erfüllung der in der Zuständigkeit des Verantwortlichen im öffentlichen Interesse liegenden Aufgabe erforderlich ist.
Die Prüfung der Zuverlässigkeit und Eignung ist eine Aufgabe, die von der Unteren Jagdbehörde wahrgenommen wird. Bei der Ausübung der Aufgabe ist aber gleichwohl Art. 5 Abs. 1 Buchstabe c) DS-GVO zu beachten. Danach müssen personenbezogene Daten dem Zweck angemessen und erheblich sowie auf das für den Zweck der Verarbeitung notwendige Maß beschränkt sein (Datenminimierung).
Zweck der hier gegenständlichen Datenverarbeitung war die Prüfung der Zuverlässigkeit und Eignung des Beschwerdeführers im Rahmen seiner Jagdscheinverlängerung. Hierfür war es nach Würdigung des Sachverhaltes durch den TLfDI allerdings nicht erforderlich, die gesamte staatsanwaltschaftliche Akte zu der eigenen Akte der Unteren Jagdbehörde zu nehmen. Im Sinne des Datenminimierungsgrundsatzes nach Art. 5 Abs. 1 Buchstabe c) DS-GVO hätten zudem nur solche Bestandteile zur Akte der Unteren Jagdbehörde genommen werden dürfen, die für die Aufgabenerfüllung erforderlich gewesen sind. Die Aufnahme der nicht erforderlichen Unterlagen zur eigenen Akte war gerade nicht gemäß § 16 ThürDSG zur Aufgabenerfüllung notwendig. Es war insbesondere nicht erforderlich, das Vermögensverzeichnis des Beschwerdeführers und mehrere Seiten mit Kontoinformationen zur Akte der Unteren Jagdbehörde zu nehmen.
Auch die Angaben des Beschwerdeführers in dem Bescheid der Versorgungsverwaltung stellen, bezogen auf seinen Namen, personenbezogene Daten gemäß Art. 4 Nr. 1 DS-GVO dar, da sie sich auf eine

identifizierte beziehungsweise identifizierbare natürliche Person beziehen. Die Angaben des Beschwerdeführers zu seinen gesundheitlichen Einschränkungen stellen zudem eine besondere Kategorie personenbezogener Daten gemäß Art. 9 Abs. 1 DS-GVO dar.
Für Gesundheitsdaten, als besondere Kategorie personenbezogener Daten, gilt, dass eine Verarbeitung nach Art. 9 Abs. 1 DS-GVO grundsätzlich verboten ist. Dieses grundsätzliche Verarbeitungsverbot gilt nur dann nicht, wenn die Verarbeitung einen Ausnahmetatbestand des Art. 9 Abs. 2 DS-GVO erfüllt.
Vorliegend wurde der Amtsarzt zum Zweck der Abklärung des Begriffs „posttraumatische Angststörung“ konsultiert. Hierfür war es nach datenschutzrechtlicher Würdigung des Sachverhaltes durch den TLfDI nicht erforderlich, den kompletten Bescheid der Versorgungsverwaltung mitsamt den (besonders geschützten) personenbezogenen Daten (Name des Beschwerdeführers, Aufzählung der organischen Erkrankungen und der psychischen Erkrankung) des Beschwerdeführers an den Amtsarzt zu übermitteln. Zur Abklärung der generellen Bedeutung einer posttraumatischen Angststörung hätte eine Anfrage ohne personenbezogene Daten ausgereicht. Zur Beurteilung der Bedeutung einer solcher Störung im konkreten Fall wäre zudem ohnehin ein fachmedizinisches Gutachten notwendig gewesen. Gemäß § 18 ThürDSG trägt die Verantwortung für die Zulässigkeit der Übermittlung personenbezogener Daten die übermittelnde Stelle. Die Übermittlung, als Form der Verarbeitung personenbezogener Daten gemäß Art. 4 Nr. 2 DS-GVO, war in diesem Fall nicht rechtmäßig, da sie zur Aufgabenerfüllung der Unteren Jagdbehörde nicht erforderlich war.
Die Untere Jagdbehörde wurde deshalb vom TLfDI wegen der Kopie von Aktenbestandteilen, die keinen Bezug zum Prüfungsgegenstand erkennen ließen sowie wegen der Übermittlung der personenbezogenen Daten an den Amtsarzt ohne Rechtsgrundlage gemäß Art. 58 Abs. 2 Buchstabe b) DS-GVO verwarnt.
Soweit sich die Beschwerde auch gegen die Einsicht in die staatsanwaltliche Ermittlungsakte selbst und eine behauptete Verarbeitung durch den Amtsarzt richtete – dieser hatte die Unterlagen ungesichtet zurückgeleitet – wies der TLfDI die Beschwerde zurück. Ein diesbezüglich vom Beschwerdeführer eingeleitetes verwaltungsgerichtliches Streitverfahren endete durch Einstellungsbeschluss wegen Klagerücknahme des Beschwerdeführers. Insoweit hatte der Beschwerdeführer und Jäger zu laut zum Halali geblasen.

2.8 Die neuen Fangbücher beim Fischen – am Ende datenschutzkonform

Angler müssen bei der durch § 9 Abs. 1 Satz 4 ThürFischAVO vorgeschriebenen Vorlage einer Fangkarte bei dem jeweiligen Fischerei(ausübungs)berechtigten keine personenbezogenen Daten angeben, da sich eine Verpflichtung dazu aus den Bestimmungen der ThürFischAVO nicht ergibt. Lediglich die in § 9 Abs. 1 ThürFischAVO genannten Daten müssen in einer Fangkarte enthalten sein.

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichten im Berichtszeitraum mehrere Eingaben von Anglern, die im Hinblick auf die Umsetzung gesetzlicher Regelungen aus der Ausführungsverordnung zum Thüringer Fischereigesetz (ThürFischAVO) datenschutzrechtliche Bedenken äußerten. Konkret betrafen die Vorbringen der Angler die Umsetzung des § 9 ThürFischAVO, der in Absatz 1 vorsieht, dass die Fänge der Angelfischerei vom Fischereiausübungsberechtigten in eine Fangkarte einzutragen sind, die dem Fischereiberechtigten oder, im Fall der Verpachtung, dem Fischereiausübungsberechtigten spätestens mit Ablauf der Geltungsdauer des Erlaubnisscheins zum Fischfang nach § 14 Abs. 1 Thüringer Fischereigesetz (ThürFischG) zu übergeben ist. Die Fangkarte hat dabei Angaben über Art, Anzahl und Länge der entnommenen und wieder zurückgesetzten Fische sowie über die Dauer der Fangzeiten pro Tag zu enthalten beziehungsweise ist im Falle nicht getätigter Fänge eine Fehlmeldung zu erteilen.
Die Angler monierten gegenüber dem TLfDI unabhängig voneinander, dass nach § 9 ThürFischAVO die Dauer der Fangzeit pro Tag in die Fangkarte eingetragen werden müsse. Zum Teil wurde der Nutzen dieser Daten für die Fischhege hinterfragt, problematisch war aus Sicht der Angler aber vielmehr, dass diese ihre Fangkarten unter Angabe von Namen, Adresse und weiterer personenbezogener Daten abgeben müssten. In Verbindung mit der Angabe der Fangzeiten befürchteten die Angler hier eine Profilbildung.
Um die Angelegenheit aus datenschutzrechtlicher Sicht prüfen zu können, setzte sich der TLfDI zunächst mit dem Thüringer Ministerium für Infrastruktur und Landwirtschaft (TMIL) in Verbindung und erbat eine Stellungnahme zum Sachverhalt. Im Ergebnis teilte das TMIL mit, dass grundsätzlich keine personenbezogenen Daten über

die Fangkarte erhoben würden, da diese nach § 9 Abs. 1 Satz 3 ThürFischAVO lediglich Angaben über Art, Anzahl und Länge der entnommenen und wieder zurückgesetzten Fische sowie über die Dauer der Fangzeiten pro Tag zu enthalten habe. Wie das TMIL weiter ausführte, sei damit insbesondere nicht vorgeschrieben, dass Name und Anschrift in der Fangkarte eingetragen werden müssten. Nach Aussage des Ministeriums gab es kein vorgeschriebenes Muster der Fangkarte, sodass über die Ausgestaltung der jeweilige Fischereiberechtigte beziehungsweise der Fischereiausübungsberechtigte selbst entscheide. Diese wären für den Fall, dass personenbezogene Angaben mit der Fangkarte erhoben würden, auch Verantwortlicher im Sinne des Art. 4 Nr. 7 Datenschutz-Grundverordnung (DS-GVO).
Da der TLfDI die kommunizierte Auffassung des TMIL teilte, informierte er die Angler anschließend darüber, dass nach den Bestimmungen der ThürFischAVO nicht vorgesehen ist, dass mit der Fangkarte personenbezogene Daten erhoben werden, und bat gleichzeitig um Mitteilung, sofern den Anglern bekannte Fischereiberechtigte beziehungsweise Fischereiausübungsberechtigte dennoch personenbezogene Daten erheben würden. Der TLfDI erhielt daraufhin von einem Angler die Information, dass der Landesanglerverband Thüringen e. V. (LAVT) mit der Fangkarte personenbezogene Daten erhebe. Dazu legte der Angler Auszüge aus einem Fischereierlaubnisschein des LAVT für das Jahr 2021 vor. Bei der Sichtung des Dokuments stellte der TLfDI fest, dass in den Erlaubnisschein, der unter anderem Name und Anschrift des Erlaubnisinhabers enthielt, die Fangkarte (als Fangbuch bezeichnet) integriert war, sodass zur Vorlage der Fangkarte beim LAVT als Fischereiausübungsberechtigtem mit Ablauf der Geltungsdauer des Erlaubnisscheins zum Fischfang nach § 14 Abs. 1 ThürFischG offensichtlich entsprechend den Angaben des Anglers der Erlaubnisschein mit der darin enthaltenen Fangkarte übergeben werden musste.
In diesem Fall wären zwar nicht direkt personenbezogene Daten im Fangbuch vermerkt gewesen, da diese jedoch im Erlaubnisschein enthalten waren, wurden im Ergebnis bei dieser Vorgehensweise – Vorlage des Fischereierlaubnisscheins inklusive des ausgefüllten Fangbuches – personenbezogene Daten im Zusammenhang mit dem Fangbuch an den LAVT übermittelt. Dies bewertete der TLfDI in datenschutzrechtlicher Hinsicht als problematisch, da Einzelinformationen aus dem Fischereierlaubnisschein (unter anderem vollständiger Name

des Erlaubnisinhabers), verknüpft mit dem darin enthaltenen Fangbuch (unter anderem Angelverhalten) durchaus eine Profilbildung ermöglichten.
Der TLfDI nahm vor diesem Hintergrund Kontakt mit dem LAVT auf und legte dar, dass – auch nach Auffassung des TMIL – nach § 9 Abs. 1 ThürFischAVO nicht vorgesehen ist, dass personenbezogene Daten auf der Fangkarte eingetragen beziehungsweise im Zusammenhang mit dieser erhoben werden. Zudem wurde angeführt, dass § 36 ThürFischAVO keine Vorgabe dahingehend macht, dass der Erlaubnisschein zum Fischfang die Dokumentation der Fangerträge in Form einer Fangkarte enthalten muss. Der TLfDI machte somit deutlich, dass es gesetzlich nicht vorgeschrieben ist, dass Angler dem LAVT ihre Fangkarte unter Angabe personenbezogener Daten übermitteln beziehungsweise die Fangkarte im Zusammenhang mit dem Fischereierlaubnisschein vorlegen müssen, der personenbezogene Daten enthält.
Der LAVT teilte dem TLfDI daraufhin zum Sachverhalt unter anderem mit, dass zwar im Zusammenhang mit dem Fischereierlaubnisschein eine Erhebung personenbezogener Daten erfolge, dies jedoch nicht über das Fangbuch, das allein der Auswertung der Fänge im Rahmen der gesetzlichen Hegeverpflichtung des Fischereiberechtigten/Fischereipächters diene. Der LAVT erläuterte weiter, dass in der Regel der komplette Fischereierlaubnisschein nach seiner Gültigkeit zurückgegeben werde, da die Fangbücher in den Fischereierlaubnisscheinen integriert sind. Nach Angaben des LAVT habe jedoch immer die Möglichkeit bestanden, das Fangbuch herauszunehmen und gesondert an den LAVT zurückzusenden.
Vor dem Hintergrund, dass seitens des LAVT entsprechend der gesetzlichen Bestimmungen aus der ThürFischAVO nicht auf einer Vorlage des Fangbuchs unter Angabe personenbezogener Daten (auf der Karte selbst oder über den Erlaubnisschein) bestanden und die Möglichkeit der gesonderten Übersendung der Fangkarte ohne Angabe von personenbezogenen Daten eingeräumt wurde, konnte der TLfDI hier keinen Verstoß gegen datenschutzrechtliche Bestimmungen feststellen. Da jedoch aus dem durch den betreffenden Angler auszugsweise vorgelegten Fischereierlaubnisschein des LAVT aus Sicht des TLfDI nicht eindeutig hervorging, dass die Möglichkeit der gesonderten Übersendung des Fangbuchs ohne Angabe personenbezogener Daten besteht, hat der TLfDI gegenüber dem LAVT angeregt, dass in die Fischereierlaubnisscheine zukünftig der Hinweis aufgenommen wird,

dass die enthaltenen Fangbücher herausgetrennt und dem LAVT gesondert ohne Angabe personenbezogener Daten zurückgesandt werden können. Zudem kommunizierte der TLfDI aufgrund der mehrfach eingegangenen Anfragen und Beschwerden zur Umsetzung des § 9 ThürFischAVO, dass es hilfreich wäre, wenn der LAVT auch seine Mitgliedsvereine darauf hinweisen würde, dass von den Fischereiausübungsberechtigten in die zu führenden Fangkarten keine personenbezogenen Daten eingetragen werden müssen, da dies die ThürFischAVO nicht vorsieht.
Diese Hinweise des TLfDI hat der LAVT aufgenommen. In den neuen Fischereierlaubnisschein (Jahreskarte 2022) hat der LAVT nach Rücksprache mit dem TLfDI unter anderem den Zusatz aufgenommen, dass das Fangbuch aus dem Fischereierlaubnisschein herausgetrennt und ohne Angabe personenbezogener Daten dort vorgelegt werden kann. Damit ist zukünftig für die Erlaubnisinhaber eindeutig ersichtlich, dass der Fischereierlaubnisschein dem LAVT nicht mit dem darin enthaltenen Fangbuch vorgelegt werden muss.

2.9 Vom Fischer und seiner Ausführungsverordnung: Angaben in Fangkarten datenschutzrechtlich zulässig

Nach § 9 Abs. 1 ThürFischAVO sind Fischereiausübungsberechtigte verpflichtet, zu statistischen Zwecken bestimmte Angaben zu ihren Fangerträgen in einer Fangkarte zu dokumentieren. Hierunter fällt, neben der Angabe des Fangkarteninhabers, über die Dauer der täglichen Fangzeit Auskunft zu geben. Diese Datenverarbeitung ist nach Art. 6 Abs. 1 Satz 1 Buchstabe c) DS-GVO zulässig.

Ein Fischereiverein wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) mit der Frage, ob die Regelungen der seit dem 25. September 2020 geltenden Ausführungsverordnung zum Thüringer Fischereigesetz (ThürFischAVO) den datenschutzrechtlichen Vorgaben entsprechen würden. Die Mitglieder des Vereins sahen insbesondere § 9 Abs. 1 Satz 3 ThürFischAVO kritisch, da Fischereiausübungsberechtigte beziehungsweise Angler danach verpflichtet seien, die Dauer ihrer Fangzeit pro Tag in eine sogenannte Fangkarte einzutragen. Hierdurch werde ein erheblicher Bereich ihrer Privatsphäre abgebildet.

Nach § 9 Abs. 1 Satz 3 ThürFischAVO sind Fischereiausübungsberechtigte verpflichtet, Angaben über Art, Anzahl und Länge der entnommenen und wieder zurückgesetzten Fische sowie über die Dauer der Fangzeit pro Tag in eine Fangkarte einzutragen. Die Angaben auf der Fangkarte hinsichtlich der Dauer der Fangzeit ließen in der Tat Rückschlüsse auf das Freizeitverhalten der jeweiligen Fischereiausübungsberechtigten zu und könnten damit in deren Recht auf informationelle Selbstbestimmung nach Art. 6 Abs. 2 Thüringer Verfassung eingreifen.
Datenschutzrechtlich gilt, dass die Angabe der täglichen Fangdauer in Verbindung mit der namentlich geführten Fangkarte eine Verarbeitung personenbezogener Daten nach Art. 2 Abs. 1 in Verbindung mit Art. 4 Nr. 1 und 2 Datenschutz-Grundverordnung (DS-GVO) darstellt. Eine solche Verarbeitung muss nach Art. 5 Abs. 1 Buchstabe a) DS-GVO auf rechtmäßige Weise erfolgen.
In diesem Fall ist die Verarbeitung nach Art. 6 Abs. 1 Satz 1 Buchstabe c) DS-GVO rechtmäßig, da sie zur Erfüllung der rechtlichen Verpflichtung, nämlich aus § 9 Abs. 1 Satz 3 ThürFischAVO erforderlich ist. Die Erlaubnis zur Datenverarbeitung ist zulässig, da nach Art. 6 Abs. 3 Buchstabe b) DS-GVO der Zweck der Verarbeitung im Rechtfertigungsgesetz festgelegt ist. In § 9 Abs. 2 ThürFischAVO heißt es dazu, dass die Angaben aus der Fangkarte zur Erhebung einer Statistik über die jährlichen Fangerträge des jeweiligen Gewässers entsprechend § 25 Abs. 2 Satz 1 Nr. 8 Thüringer Fischereigesetz dienen. Diese Statistik wird in Thüringen von den Fischereiverbänden erhoben, wobei hierdurch grundsätzlich keine personenbezogenen Daten der Angler verarbeitet werden sollen. Für den Fall, dass dennoch personenbezogene Daten durch die Vorlage der Fangkarte erhoben werden, obliegt es den Verbänden, die datenschutzrechtlichen Bestimmungen einzuhalten.
Ob es sich bei den Angaben zur Dauer der Fangzeit um eine erforderliche Angabe im Interesse des Artenschutzes von Fischen und Fischereigebieten handelt, war datenschutzrechtlich hingegen nicht zu prüfen. Entscheidend für die Zulässigkeit der Datenverarbeitung nach der DS-GVO war lediglich das Vorliegen einer gesetzlichen Rechtsgrundlage.

2.10 Formulare bei der Erlegung von Schwarzwild – Ein Fall für den TLfDI

Das Freiwilligkeitsmerkmal ist eine zentrale datenschutzrechtliche Voraussetzung für eine wirksame Einwilligung. Aus Erwägungsgrund (ErwGr) 43 der DS-GVO ergibt sich, dass es einer Einwilligung dann an der Freiwilligkeit fehlt, wenn zwischen der betroffenen Person und dem für die Datenverarbeitung Verantwortlichen ein klares Ungleichgewicht besteht. Im ErwGr 43 wird gleichsam darauf hingewiesen, dass ein solches Ungleichgewicht insbesondere dann vorliegen kann, wenn es sich bei dem Verantwortlichen um eine Behörde handelt.

In Thüringen können Jagdausübungsberechtigte und Jagdhundeführer für die Erlegung von Schwarzwild oder den Einsatz von Jagdhunden anlässlich jagdbezirksübergreifender Treib- oder Drückjagden auf Schwarzwild einen Zuschuss in Höhe von 25 Euro beantragen. Das sieht die „Förderrichtlinie des Thüringer Ministeriums für Infrastruktur und Landwirtschaft zur Unterstützung der Jagdausübungsberechtigten und Jagdhundeführer bei der Durchführung vorbeugender Jagdmaßnahmen gegen den Eintrag der Afrikanischen Schweinepest nach Thüringen (FR-ASP-Jagd)“ als Ausgleich für den entstandenen Aufwand und als Anreiz für die Bejagung des Schwarzwildes vor. Die Förderungen können jeweils mit den Formularen „Antrag auf Auszahlung eines pauschalen Festbetrags für die Erlegung von Schwarzwild“ und „Antrag auf Auszahlung eines pauschalen Festbetrags für den Einsatz von Jagdhunden“, die der FR-ASP-Jagd als Anlagen beigefügt sind, beantragt werden.
Im Berichtszeitraum erreichte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) eine Beschwerde, die sich auf das Antragsformular bezüglich der Erlegung von Schwarzwild bezog. Der Beschwerdeführer teilte konkret mit, dass er gerne eine Abschussprämie erhalten wollte, jedoch mit der Übermittlung seiner personenbezogenen Daten an die im Antragsformular genannten Stellen nicht einverstanden war. Denn in dem Antragsformular fand sich unter Nr. 6 folgende Formulierung: „Ich bestätige mit meiner Unterschrift, dass ich in die elektronische Erhebung, Verarbeitung, Speicherung und Übermittlung meiner persönlichen Daten einschließlich meiner Kontodaten (IBAN) zum Zwecke der Prüfung und Auszahlung der Förderung sowie zum Datenabgleich

mit dem Veterinär- und Lebensmittelüberwachungsamt sowie der unteren Jagdbehörden einwillige. Ich wurde darauf hingewiesen, dass ich ein Recht auf Verweigerung der Einwilligung habe mit der Folge, dass keine Förderung an mich ausgezahlt werden kann. Ich erkläre diese Einwilligung freiwillig; sie gilt für diesen Antrag und kann jederzeit gegenüber dem Forstamt Sondershausen schriftlich oder per E-Mail mit Wirkung für die Zukunft widerrufen werden."

Der Beschwerdeführer bat daher den TLfDI, die Datenschutzkonformität des beschwerdegegenständlichen Formulars zu prüfen. Dazu konsultierte der TLfDI zunächst das Thüringer Forstamt Sondershausen, das für die Bearbeitung der Anträge nach der FR-ASP-Jagd zuständig ist, und bat um Mitteilung, aus welchen Gründen eine Übermittlung der personenbezogenen Daten erforderlich ist und ob von einer Übermittlung abgesehen werden kann, ohne zugleich die Abschussprämie zu versagen. Ferner erfragte der TLfDI, wieso die Einwilligung dennoch freiwillig abgegeben werden kann, wenn bei ihrer Verweigerung die Abschussprämie nicht gezahlt wird.

Zu diesen Fragen erhielt der TLfDI eine Antwort aus dem Thüringer Ministerium für Infrastruktur und Landwirtschaft (TMIL). Von dort wurde mitgeteilt, dass von der Übermittlung nicht abgesehen werden könne, ohne zugleich die Abschussprämie zu versagen, weil sonst die Prüfrechte gemäß der FR-ASP-Jagd nicht wahrgenommen werden könnten. Im Hinblick auf die Freiwilligkeit der abzugebenden Einwilligung führte das TMIL zunächst aus, dass nach dortiger Auffassung die Einwilligung freiwillig abgegeben werden kann, auch wenn bei ihrer Verweigerung die Abschussprämie nicht gezahlt wird, weil die Übermittlung der personenbezogenen Daten insbesondere für die Durchführung der Prüfrechte nach FR-ASP-Jagd und daher auch für die Auszahlung der Zuwendung erforderlich sei.

Nach weiterem Schriftwechsel und eingehender Prüfung des Sachverhalts gelangte der TLfDI zu dem Ergebnis, dass die Datenverarbeitungen, die im Zusammenhang mit einem „Antrag auf Auszahlung eines pauschalen Festbetrags für die Erlegung von Schwarzwild" sowie auch mit einem „Antrag auf Auszahlung eines pauschalen Festbetrags für den Einsatz von Jagdhunden" gemäß der FR-ASP-Jagd durchgeführt werden, aufgrund fehlender Freiwilligkeit nicht auf eine Einwilligung als Rechtfertigungsinstrument gestützt werden können. Denn bei einer Betrachtung der konkreten Umstände der abverlangten Einwilligungserteilung bei einem „Antrag auf Auszahlung eines pauscha-

len Festbetrags für die Erlegung von Schwarzwild“ / „Antrag auf Auszahlung eines pauschalen Festbetrags für den Einsatz von Jagdhunden“ war zum einen ein Ungleichgewicht nach den Maßstäben des Erwägungsgrundes 43 der DS-GVO zwischen Antragsteller und Verantwortlichem festzustellen, zum anderen war von einer nicht gegebenen Wahlfreiheit für den Antragsteller auszugehen, da eine Verweigerung der abverlangten Einwilligung nachteilige Auswirkungen (keine Förderung) für die Antragstellenden zur Folge hatte.
Der TLfDI wies daher das TMIL darauf hin, dass die Datenverarbeitungen, die im Zusammenhang mit den beiden Antragsformlaren nach der FR-ASP-Jagd durchgeführt werden, auf eine andere Rechtsgrundlage zu stützen sind. Der TLfDI erläuterte dazu gegenüber dem TMIL, dass die Vorgaben der FR-ASP-Jagd aufgrund der Rechtsnatur der Förderrichtlinie als Verwaltungsvorschrift zwar selbst als Rechtsgrundlage für eine Datenverarbeitung nicht in Betracht kommen, jedoch die Verarbeitungsvorgänge, die aufgrund der Bestimmungen der FR-ASP-Jagd bei Anträgen nach dieser Förderrichtlinie erforderlich sind, nach Auffassung des TLfDI auf § 16 Thüringer Datenschutzgesetz (ThürDSG) in Verbindung mit § 1 Thüringer Haushaltsgesetz 2021 (ThürHhG 2021) in Verbindung mit dem Einzelplan 10, Kapitel 1011, Titelgruppe 73 (Vorbeugung von Schäden infolge der Tierseuche Afrikanische Schweinepest), Titel 681 73 des Landeshaushaltsplan 2021 gestützt werden können. Denn § 16 ThürDSG stellt eine Rechtsgrundlage für die Datenverarbeitung durch öffentliche Stellen auf der Grundlage von Art. 6 Abs. 1 Satz 1 Buchstabe e) DS-GVO dar. Nach dieser Vorschrift ist eine Verarbeitung personenbezogener Daten durch eine öffentliche Stelle zulässig, wenn sie für die Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe erforderlich ist oder wenn sie in Ausübung öffentlicher Gewalt erfolgt, die ihr übertragen wurde. Die dem TMIL übertragene Aufgabe, die im öffentlichen Interesse liegt, ergibt sich in vorstehend angeführter Weise aus dem Landehaushaltsplan 2021, der mit dem ThürHhG 2021 beschlossen wurde.
Im Folgenden teilte das TMIL dem TLfDI mit, dass nunmehr dessen Auffassung, dass die Datenverarbeitung bei den Anträgen der FR-ASP-Jagd auf eine andere Rechtsgrundlage gestützt werden muss, geteilt wird. Auch wurde dargelegt, dass das TMIL die Ansicht des TLfDI teilt, dass die Verarbeitungsvorgänge, die aufgrund der Bestimmungen der FR-ASP-Jagd bei Anträgen nach dieser Förderrichtlinie erforderlich sind, auf die vom TLfDI benannte Rechtsgrundlage

gestützt werden können. Daraus folgend änderte das TMIL das Formular „Antrag auf Auszahlung eines pauschalen Festbetrags für die Erlegung von Schwarzwild“ sowie das Formular „Antrag auf Auszahlung eines pauschalen Festbetrags für den Einsatz von Jagdhunden“, mit denen eine Einwilligung von den Antragsstellenden verlangt wurde, sodass nunmehr für die Antragsteller die korrekte Rechtsgrundlage der Verarbeitung ihrer personenbezogenen Daten ersichtlich ist.
Dem Beschwerdeführer konnte der TLfDI somit im Ergebnis mitteilen, dass die mit einem „Antrag auf Auszahlung eines pauschalen Festbetrags für die Erlegung von Schwarzwild“ vom Antragstellenden abverlangte Einwilligung aufgrund der fehlenden Freiwilligkeit der Einwilligungserteilung zwar als unwirksam zu bewerten war, es jedoch aufgrund der bereits existierenden Rechtsgrundlage keiner wirksamen Einwilligung bedurft hätte. Auch wenn bis zu der erfolgten Korrektur der Formulare eine Einwilligung von den Antragstellern eingeholt wurde, die als solche die durchgeführten Datenverarbeitungen im Rahmen der Antragsbearbeitung nach der FR-ASP-Jagd aus genannten Gründen nicht legitimierte, war daher ein datenschutzrechtlicher Verstoß im Ergebnis nicht festzustellen.

2.11 Ein unbeugsames Dorf – unterfällt auch dem ThürDSG

Auch für die Thüringer Städte und Gemeinden gilt das ThürDSG. Der TLfDI ist für sie die zuständige datenschutzrechtliche Aufsichtsbehörde.

Als der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) im Rahmen eines Beschwerdeverfahrens aus dem Berichtszeitraum bei dem Bürgermeister einer kleinen Thüringer Gemeinde Auskünfte zur Aufklärung des Sachverhalts forderte, erlebte er eine Überraschung. Die Gemeinde verweigerte die Auskunft!
Sie begründete dies unter anderem recht kämpferisch damit, dass sich die Gemeinde bereits in einem Rechtsstreit mit dem Beschwerdeführer befände. In einem beim Verwaltungsgericht gegen den Beschwerdeführer geführten Verfahren lägen entsprechende Unterlagen vor. Auch sei ihr die Beschwerdeschrift nicht übersandt worden. Außerdem beantwortete sie so manche Frage nur mit einer Gegenfrage.

Trotz entsprechender Erläuterungen durch den TLfDI erteilte die besagte Gemeinde die Auskunft nicht vollständig. Deshalb erließ der TLfDI einen Bescheid und wies die Gemeinde gemäß § 7 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) in Verbindung mit Art. 58 Abs. 1 Buchstabe a) Datenschutz-Grundverordnung (DS-GVO) an, ihm die benötigten Auskünfte und Informationen zu erteilen. Der TLfDI teilte der Gemeinde mit, dass er den Gegenstand der Beschwerde in angemessenem Umfang entsprechend § 6 Abs. 6 ThürDSG zu untersuchen hat und er und seine Mitarbeiter der allgemeinen Verschwiegenheitspflicht gemäß § 4 Abs. 3 ThürDSG unterliegen. Deshalb werde der Gemeinde nur der Inhalt der Beschwerde mitgeteilt, die Beschwerdeschrift jedoch nicht übersandt. Zudem begründete der TLfDI der Gemeinde, warum seine Fragen nicht vollständig beantwortet waren.
Gegen diesen Bescheid des TLfDI erhob die Gemeinde im Anschluss Klage beim zuständigen Verwaltungsgericht. Es war die erste Klage gegen einen Auskunftsbescheid des TLfDI nach Art. 58 Abs. 1 Buchstabe a) DS-GVO.
Die Klage begründete die Gemeinde unter anderem damit, dass der TLfDI sachlich nicht für sie zuständig sei. Dies ergebe sich aus dem Gesetzestext. Gemäß § 6 Abs. 1 ThürDSG habe der TLfDI nur gegenüber den öffentlichen Stellen des Landes die Aufgaben nach Art. 57 der Verordnung (EU) 2016/679 wahrzunehmen. In § 2 Abs. 1 ThürDSG werde ausdrücklich unterschieden zwischen den Behörden, den Gerichten und sonstigen öffentlichen Stellen des Landes auf der einen Seite, den Gemeinden und Gemeindeverbänden und den sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts auf der anderen Seite. Im folgenden Klammerzusatz sei lediglich die Formulierung „öffentliche Stellen“ und nicht etwa „öffentliche Stellen des Landes“ enthalten, sodass davon auszugehen sei, dass auch in § 6 Abs. 1 ThürDSG die Formulierung „öffentliche Stellen des Landes" nur eben genau diese meint und nicht auch die sonstigen öffentlichen Stellen im Sinne des § 2 Abs. 1 ThürDSG. Damit sei der TLfDI nicht für die Gemeinden in Thüringen zuständig.
Das Verwaltungsgericht sah dies natürlich anders. Im Rahmen der mündlichen Verhandlung wies das Gericht darauf hin, dass der TLfDI die Aufgaben und Befugnisse nach §§ 6 und 7 ThürDSG auch gegenüber den Thüringer Gemeinden wahrnehmen kann und zuständige Aufsichtsbehörde ist. Zwar sei der Gesetzestext in § 6 Abs. 1

ThürDSG nicht eindeutig gefasst. Eine Auslegung dahingehend, dass § 6 Abs. 1 Satz 1 ThürDSG nur die vom Freistaat Thüringen unmittelbar verwalteten öffentlichen Stellen umfasse, würde aber dazu führen, dass die DS-GVO nicht vollständig umgesetzt sei. Nach Art. 51 und 55 DS-GVO sei jeder Mitgliedsstaat verpflichtet, eine Aufsichtsbehörde zu bestellen. Aufgrund der föderalen Struktur der Bundesrepublik habe dies sowohl auf Bundes- als auch auf Landesebene zu erfolgen.
Für den Freistaat Thüringen sei der TLfDI die einzige Aufsichtsbehörde. Würden die Gemeinden nicht § 6 Abs. 1 ThürDSG unterfallen, unterlägen sie keinerlei datenschutzrechtlicher Aufsicht. Damit hätte die Bundesrepublik Deutschland als Mitgliedsstaat ihrer Umsetzungsverpflichtung nicht ausreichend Rechnung getragen. Außerdem verwies das Verwaltungsgericht noch auf § 2 Bundesdatenschutzgesetz (BDSG), wonach die „öffentlichen Stellen der Länder“ auch die Gemeinden umfassten. Zwar fände das BDSG keine unmittelbare Anwendung, aber die Regelung mache deutlich, dass auch Gemeinden öffentliche Stellen der Länder seien.
Ferner wies das Gericht darauf hin, dass der TLfDI im Rahmen seiner Amtsermittlung, die Art. 58 Abs. 1 Buchstabe a) DS-GVO verlangt, einen weiten Ermessenspielraum hinsichtlich der geforderten Auskünfte hat und die im Bescheid begehrten Auskünfte verlangen darf.
Auch folgte das Verwaltungsgericht der Auffassung des TLfDI, dass dieser kein Recht auf Einsicht in Gerichtsakten hat, wenn er an dem Verfahren nicht beteiligt ist. Der TLfDI hätte also die von ihm begehrten Auskünfte nicht aus der Akte des weiteren Gerichtsverfahrens, welches der Beschwerdeführer und die Gemeinde führten, erlangen können.
Die Gemeinde nahm aufgrund der Hinweise des Gerichts die Klage zurück. Sie musste die Kosten des Verfahrens, zu denen auch die Kosten der von ihr beauftragten Rechtsanwaltskanzlei zählten, tragen.
Um die Auskunft der Gemeinde wird weiterhin gerungen. Das Beschwerdeverfahren ist leider noch längst nicht entscheidungsreif. Gegebenenfalls muss der TLfDI von weiteren seiner Durchsetzungsrechte Gebrauch machen.

2.12 Feuerwehrleute im Interesse eines Zweckverbandes

Die namentliche Erfassung von über den Umgang mit Hydranten belehrten Feuerwehrkameraden durch einen Zweckverband der Trinkwasserversorgung wäre nur nach entsprechender Einwilligung der betroffenen Personen datenschutzrechtlich zulässig. Dies war im folgenden Fall aber nicht erforderlich, weil sich der Zweckverband mit dem TLfDI auf eine bessere, datenschutzkonforme Vorgehensweise einigte.

Darf ein für die Wasserversorgung zuständiger Zweckverband von den im Verbandsgebiet ansässigen Feuerwehren verlangen, dass sich deren Kameraden nach erfolgter Belehrung über den Umgang mit verbandseigenen Trinkwasserhydranten namentlich in eine Liste eintragen und gegenüber dem Verband ihre Teilnahme an der Belehrung per Unterschrift bestätigen? Mit dieser Frage wandte sich im Berichtszeitraum ein Bürger an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Hintergrund der Anfrage war, dass der Bürger als Wehrführer einer freiwilligen Feuerwehr von einem Zweckverband die Aufforderung erhalten hatte, die Kameraden seiner Feuerwehr über den ordnungsgemäßen Umgang mit den im Eigentum des Verbandes stehenden Hydranten zu belehren. Nach erfolgter Belehrung der Kameraden zur Entnahme von Löschwasser aus dem Netz des Zweckverbandes sollte sodann eine von den Kameraden unterschriebene Belehrungsliste an den Zweckverband übermittelt werden. Da es nach Auffassung des Wehrführers jedoch keine rechtliche Grundlage für eine solche Erhebung der Daten der Feuerwehrleute durch den Zweckverband gab und zudem für ihn nicht nachvollziehbar war, wozu der Zweckverband die mit betreffendem Formular erfragten personenbezogenen Daten benötigte, wurde der TLfDI um datenschutzrechtliche Prüfung der Angelegenheit gebeten.
Zunächst ersuchte der TLfDI den betreffenden Zweckverband um eine Stellungnahme zum Sachverhalt. Dieser teilte dem TLfDI daraufhin mit, dass den Feuerwehren des Verbandsgebietes zum Einsatz für Brandnotfälle die Trinkwasserhydranten zur Benutzung zur Verfügung gestellt werden. Die namentliche Erfassung der vom Feuerwehrführer belehrten Kameraden werde dabei vom Verband als erforderlich erachtet, um im Haftungsfall nachprüfen zu können, ob und welche Feuerwehrkameraden eine Belehrung zum Umgang mit den ver-

bandseigenen Hydranten erfahren haben. Im Hinblick auf die Rechtmäßigkeit dieser Datenverarbeitung legte der Zweckverband dar, dass die Erfassung der Daten (Namen und Unterschriften) der belehrten Feuerwehrkameraden gemäß Art. 6 Abs. 1 Satz 1 Buchstaben e) und f) Datenschutz-Grundverordnung (DS-GVO) nur im Rahmen der Wahrnehmung einer Aufgabe im öffentlichen Interesse aufgrund satzungsgemäßer Aufgaben oder anderer gesetzlicher Verordnungen (Trinkwasserversorgung) sowie zur Wahrung berechtigter Interessen des Verbandes (Schutz des Eigentums) erfolge.
Für den TLfDI war zwar nach Prüfung der Rückäußerung des Verbandes nachvollziehbar, dass der Zweckverband die Feuerwehrkameraden als mögliche Benutzer der verbandseigenen Hydranten über den Umgang mit diesen belehren wollte, um sicherzustellen, dass eine Benutzung der Hydranten durch Fremde sorgsam und unter Beachtung von technischen Besonderheiten zum Schutz des Trinkwassers vor Verunreinigungen und unter Gewährleistung einer ständigen Versorgung der Bevölkerung mit Trinkwasser erfolge. Jedoch gelangte der TLfDI zu der Auffassung, dass die namentliche Erfassung belehrter Feuerwehrkameraden nicht auf die vom Zweckverband angeführten Zulässigkeitstatbestände (Art. 6 Abs. 1 Satz 1 Buchstabe e) und f) DS-GVO) gestützt werden konnte. Dies ergab sich aus den folgenden Gründen:
Zum einen ist gemäß Art. 6 Abs. 1 Satz 1 Buchstabe e) DS-GVO eine Verarbeitung nur rechtmäßig, wenn diese für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Eine einschlägige Rechtsgrundlage im Sinne des Art. 6 Abs. 1 Satz 1 Buchstabe e) DS-GVO, der es zwingend für die Legitimation der Datenverarbeitung bedarf, war für den TLfDI jedoch nicht ersichtlich. Bei der Versorgung der Bevölkerung mit Trink- und Betriebswasser handelt es sich zwar um eine Pflichtaufgabe der Gemeinden (§ 42 Abs. 1 Thüringer Wassergesetz) im Rahmen der Daseinsvorsorge, die vorliegend dem Zweckverband übertragen wurde. Die Daseinsvorsorge stellt eine Aufgabe im öffentlichen Interesse dar, sodass auch bei der Wasserversorgung durch den Zweckverband von einer „im öffentlichen Interesse liegenden Aufgabe“ auszugehen ist, dennoch ist die namentliche Kenntnis von über den Umgang mit Trinkwasserhydranten belehrten Feuerwehrkameraden nach Auffas-

sung des TLfDI im Einzelnen nicht notwendig, damit ein Zweckverband die im öffentliche Interesse liegende Aufgabe der Versorgung der Einwohner im Verbandsgebiet mit Trinkwasser erfüllen kann.
Zum anderen konnte die Verarbeitung der personenbezogenen Daten der belehrten Feuerwehrkameraden durch den Verband im konkreten Fall auch nicht auf Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO (Wahrung berechtigter Interessen der Daten verarbeitenden Stelle) gestützt werden, da diese Vorschrift nach Art. 6 Abs. 1 Satz 2 DS-GVO nicht für die Aufgabenerfüllung öffentlicher Stellen gilt. Adressat dieser Vorschrift sind ausschließlich private Verantwortliche, sodass sich ein Zweckverband als Körperschaft des öffentlichen Rechts grundsätzlich nicht auf Art. 6 Abs. 1 Buchstabe f) DS-GVO berufen kann.
Der TLfDI teilte dem Zweckverband vor diesem Hintergrund mit, dass er nach vorläufiger Prüfung im Ergebnis davon ausging, dass die personenbezogenen Daten der Feuerwehrkameraden auf unrechtmäßige Weise verarbeitet werden. Zwar wäre eine Verarbeitung der Daten auf Grundlage einer Einwilligung der belehrten Kameraden möglich (Art. 6 Abs. 1 Satz 1 Buchstabe a) DS-GVO), der TLfDI wies jedoch gleichsam darauf hin, dass es im Sinne der Datensparsamkeit (Art. 5 Abs. 1 Buchstabe c) DS-GVO) Möglichkeiten gibt, eine zielführende Belehrung der Feuerwehrkameraden über den Umgang mit den Trinkwasserhydranten dergestalt vorzunehmen, dass eine Kenntnis des Zweckverbandes über alle belehrten Personen entbehrlich ist. So erläuterte der TLfDI gegenüber dem Verband, dass ein Wehrführer nach durchgeführter Belehrung dem Verband zum Beispiel die Mitteilung machen könnte, dass die Feuerwehrkameraden der betreffenden Wehr entsprechend den Vorgaben des Verbandes belehrt wurden. Diese Bestätigung durch die Wehrführer, dass die Belehrung ordnungsgemäß erfolgt ist, wäre nach Ansicht des TLfDI in jedem Fall ausreichend, damit der Zweckverband seine im öffentlichen Interesse liegende Aufgabe der Wasserversorgung satzungsgemäß wahrnehmen kann. Soweit im Schadensfall an einem Hydranten des Verbandes nachgeprüft werden soll, ob der Verursacher über den ordnungsgemäßen Umgang mit den Trinkwasserhydranten belehrt wurde, könnte entsprechend der zuständige Wehrführer konsultiert werden, der dazu im Bedarfsfall sodann Auskunft erteilen kann.
Nachdem der TLfDI vor dem Hintergrund des vorläufigen Prüfungsergebnisses den Zweckverband um eine erneute Stellungnahme ersucht hatte, wurde von dort mitgeteilt, dass nunmehr auf die Forderung der Vorlage einer Belehrungsliste verzichtet wird. Der Verband

griff den Vorschlag des TLfDI auf: Eine ausdrückliche Versicherung der zuständigen Wehrführer über die erfolgte Belehrung der Kameraden im Umgang mit verbandseigenen Hydranten sah der Zweckverband nunmehr als ausreichend an.
Ergänzend wies der Zweckverband darauf hin, dass noch keine Feuerwehren des Verbandsgebietes die ausgegebenen Belehrungslisten ausgefüllt zurückgesandt hatten, sodass durch den Verband keine Datenerfassung oder Datenverarbeitung in der durch den TLfDI als nicht rechtmäßig klassifizierten Art und Weise erfolgt war. Im Ergebnis konnte der TLfDI daher keine unrechtmäßige Datenverarbeitung und daraus folgend auch keinen Verstoß gegen datenschutzrechtliche Bestimmungen seitens des Zweckverbandes feststellen. Aufgrund der nunmehr vom Verband umgesetzten Praxis konnte der Vorgang abgeschlossen werden.

2.13 Unterschriftenlisten aus Einwohneranträgen – was dürfen Gemeinderäte sehen?

Die Weitergabe von zu Einwohneranträgen gehörenden Unterschriftenlisten durch den Bürgermeister oder die Gemeindeverwaltung an den Gemeinderat ist unzulässig, sofern dafür nicht von den unterschriftsleistenden Bürgern eine wirksame Einwilligung erteilt wurde. Grundsätzlich gilt: Eine Datenübermittlung durch den Bürgermeister oder die Gemeindeverwaltung an den Gemeinderat, die auf Art. 6 Abs. 1 Satz 1 Buchstabe e) DS-GVO in Verbindung mit der jeweiligen fachgesetzlichen Regelung oder auf § 16 Abs. 1 ThürDSG gestützt wird, ist nur dann zulässig, wenn sich diese zur Aufgabenerfüllung des Gemeinderats erforderlich zeigt.

Nach § 16 Thüringer Kommunalordnung können Einwohner beantragen, dass der Gemeinderat über eine gemeindliche Angelegenheit, für deren Entscheidung er zuständig ist, berät und entscheidet. Näheres zu diesen sogenannten Einwohneranträgen regelt das Thüringer Gesetz über das Verfahren bei Einwohnerantrag, Bürgerbegehren und Bürgerentscheid (ThürEBBG). So sieht § 3 Abs. 1 ThürEBBG etwa vor, dass in einem Einwohnerantrag als Vertreter der Antragsteller eine Vertrauensperson und eine stellvertretende Vertrauensperson benannt werden.

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichte im Berichtszeitraum die Beschwerde eines Bürgers, der als Vertrauensperson mehrere Einwohneranträge nebst notwendiger Unterschriftenlisten an den Bürgermeister einer Thüringer Gemeinde übergeben hatte. Dabei kam es nach Auffassung des Bürgers zu einem Datenschutzverstoß, da die eingereichten Einwohneranträge nach Mitteilung der Vertrauensperson durch den Bürgermeister inklusive der Unterschriftenlisten, die personenbezogene Daten – hier der Vor- und Familienname, das Geburtsdatum und die Anschrift der Hauptwohnung – der Unterzeichnenden enthielten, an die Gemeinderatsmitglieder weitergegeben wurden. Der TLfDI wurde um Prüfung der Angelegenheit ersucht.
Wie in einem solchen Fall üblich, wurde der Gemeinde zunächst vom TLfDI Gelegenheit gegeben, sich zu dem Sachverhalt zu äußern. Seitens der Gemeinde wurde dabei bestätigt, dass der Bürgermeister die kompletten Einwohneranträge inklusive der Unterschriftenlisten per E-Mail an die Gemeinderatsmitglieder weitergeleitet hatte.
Im Rahmen der datenschutzrechtlichen Prüfung stellte der TLfDI fest, dass durch die Weitergabe der zu den Einwohneranträgen gehörenden Unterschriftenlisten ein Verstoß gegen datenschutzrechtliche Bestimmungen begangen wurden. Dies ergab sich aus den folgenden Gründen:
Die Versendung von zu Einwohneranträgen gehörenden Unterschriftenlisten an Gemeinderäte stellte eine Verarbeitung personenbezogener Daten dar. Gemäß § 6 Abs. 4 Satz 2 Thüringer Gesetz über das Verfahren bei Einwohnerantrag, Bürgerbegehren und Bürgerentscheid müssen auf einer solchen Unterschriftenliste unter anderem Vor- und Familienname, Geburtsdatum und bei mehreren Wohnungen die Anschrift der Hauptwohnung von den Unterzeichnern eingetragen werden. Hierbei handelt es sich um personenbezogene Daten im Sinne des Art. 4 Nr. 1 Datenschutz-Grundverordnung (DS-GVO). Art. 4 Nr. 2 DS-GVO definiert den Begriff der „Verarbeitung“ als „jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten (…)“. Konkret stellte der Vorgang eine „Offenlegung“ dar, die in Art. 4 Nr. 2 DS-GVO auch beispielhaft als Erscheinungsform der Datenverarbeitung benannt wird. Darunter fallen alle Vorgänge, durch die ein Verantwortlicher im Sinne des Art. 4 Nr. 7 DS-GVO (hier die Gemeinde, vertreten durch den Bürgermeister) personenbezogene Daten anderen Stellen in der Weise zugänglich macht, dass

diese Kenntnis vom Informationsgehalt der betreffenden Daten erlangen können (vergleich dazu Herbst in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl., Art. 4 Nr. 2 DS-GVO Rn. 29). Aus dem in Art. 5 Abs. 1 Buchstabe a) DS-GVO normierten Grundsatz der Rechtmäßigkeit folgt, dass personenbezogene Daten nur auf rechtmäßige Weise verarbeitet werden dürfen. Art. 6 Abs. 1 Satz 1 DS-GVO enthält sechs verschiedene Tatbestände, bei deren Vorliegen eine Verarbeitung personenbezogener Daten erlaubt ist. Jegliche Datenverarbeitung unterliegt damit grundsätzlich einem Verbot mit Erlaubnisvorbehalt.

Bei der per E-Mail durch den Bürgermeister erfolgten Versendung der zu den Einwohneranträgen gehörenden Unterschriftenlisten an die Gemeinderäte war keiner der normierten Zulässigkeitstatbestände erfüllt. Insbesondere konnte die Datenverarbeitung nicht auf Art. 6 Abs. 1 Satz 1 Buchstabe e) DS-GVO gestützt werden, wonach eine Verarbeitung nur rechtmäßig ist, wenn sie für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Denn im ThürEBBG ist zwar Näheres zu Einwohneranträgen im Sinn von § 16 Thüringer Kommunalordnung geregelt, eine Befugnis zur Übermittlung von zu Einwohneranträgen gehörenden Unterschriftenlisten an Gemeinderatsmitglieder findet sich in diesem Gesetz indes nicht. Für die Erfüllung der im Zusammenhang mit den Einwohneranträgen stehenden Aufgaben der Gemeinräte war es auch nicht erforderlich, neben den Einwohneranträgen auch die zugehörigen Unterschriftenlisten an sie zu übermitteln. Die stattgefundene Datenverarbeitung in Form einer Offenlegung durch Übermittlung war auch durch keine andere Rechtsgrundlage gedeckt, die Art. 6 Abs. 1 Satz 1 Buchstabe e) DS-GVO fordert.

Da es somit nach Ansicht des TLfDI keine Rechtsgrundlage für die stattgefundene Datenübermittlung an die Gemeinderäte gab, wurden die personenbezogenen Daten der unterschriftsleistenden Bürger auf unrechtmäßige Weise verarbeitet. Im Ergebnis war daher ein Verstoß gegen Art. 5 Abs. 1 Buchstabe a) DS-GVO festzustellen, für den die Gemeinde nach Art. 58 Abs. 2 Buchstabe b) DS-GVO durch den TLfDI verwarnt wurde.

Bei der Prüfung des Sachverhalts stellte der TLfDI zudem fest, dass es durch die Versendung der Unterschriftenlisten an die Gemeinderäte zu einer Verletzung des Schutzes personenbezogener Daten im Sinne des Art. 4 Nr. 12 DS-GVO kam. Dies deshalb, weil die per E-Mail

durch den Bürgermeister vorgenommene Übersendung der Unterschriftenlisten an die Gemeinderäte zu einer unbefugten Offenlegung der personenbezogenen Daten der unterschriftsleistenden Bürger gegenüber den Gemeinderäten geführt hat.
Dem Bürgermeister war die begangene Rechtsverletzung bereits vor Prüfung des Vorgangs durch den TLfDI bekannt, wie anhand einer E-Mail festgestellt werden konnte, die der Bürgermeister nach Übermittlung der Einwohneranträge nebst Unterschriftenlisten an die Gemeinderäte an selbige versandt hatte. In der E-Mail werden die Gemeinderäte zur Löschung der Unterschriftenlisten aufgefordert. Damit hätte die Rechtsverletzung gemäß Art. 33 Abs. 1 DS-GVO durch die Gemeinde (Verantwortlicher) unverzüglich und nicht länger als 72 Stunden nach Bekanntwerden der Verletzung dem TLfDI gemeldet werden müssen. Da der Meldepflicht durch die Gemeinde jedoch nicht innerhalb der gesetzlichen Frist nachgekommen wurde, war auch ein Verstoß gegen Art. 33 Abs. 1 DS-GVO festzustellen. Weil die Gemeinde die Meldung der Verletzung des Schutzes personenbezogener Daten nach Aufforderung des TLfDI jedoch nachträglich vorgenommen hatte, hat der TLfDI unter Anwendung seines Ermessens in diesem Fall von einer Ausübung seiner Befugnisse abgesehen.

2.14 Videoüberwachung im Kindergarten

Vor der Einrichtung einer Videoüberwachung ist genauestens zu prüfen, welchen Zweck die Videoüberwachung erreichen soll und ob für die Erreichung dieses Zweckes wirklich die Installation von Kameras erforderlich ist. In einem Kindergarten kann eine Videobeobachtung die geeignetere Form der Videoüberwachung sein als eine Videoaufzeichnung. Die Umsetzung einer Videoüberwachung kann nur dann in Betracht gezogen werden, wenn alle milderen Mittel ausgeschöpft sind.

Ein Kindergarten als eine öffentliche Stelle in Thüringen fragte im Berichtszeitraum beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) nach, ob eine geplante Videoüberwachung im öffentlichen Raum stattfinden dürfe. Der Kindergarten sah Handlungsbedarf, um die Sicherheit der Kinder zu gewährleisten. Im Kindergarten komme es immer wieder vor, dass Fremde diesen betreten würden, die kein Kind bringen oder abholen wollen (Postbote, Vertreter und andere). Auch habe es bereits Vorfälle

gegeben, bei denen Kinder das Grundstück des Kindergartens verlassen hätten, ohne dass die Erzieher dies gesehen hätten. Regelmäßige Belehrungen der Eltern, keine fremden Personen mit auf das Grundstück zu bringen oder Kinder ohne Abmeldung mit hinauszunehmen, hätten bisher nicht dazu geführt, dass diese Vorfälle seltener eintreten. Im Zuge einer größer angelegten Maßnahme zur Erhöhung der Sicherheit sollten an ein neues Tor Kameras angebracht werden, welche eine Videoüberwachung ermöglichen.
Nach Prüfung der Rechtslage und des Sachverhalts kam der TLfDI zu folgendem Ergebnis:
1. Zweck und Form der Videoüberwachung:
Die Auswahl einer möglichen Form der Videoüberwachung hängt davon ab, welche Zwecke der Verantwortliche erreichen will. Der Kindergarten wollte die Videoüberwachung in Form einer reinen Videoaufzeichnung einrichten. Bei einer Videoaufzeichnung erfolgt nur die Speicherung der aufgenommenen Bilder, die nachträglich von einer oder einem Beschäftigten der öffentlichen Stelle angesehen werden können, nachdem es bereits zu einem Vorfall gekommen ist. Im Gegensatz zu einer Videoaufzeichnung werden bei einer Videobeobachtung die Bilder aufgenommen und live auf einen Monitor übertragen; dort werden sie von einer oder einem Beschäftigten der öffentlichen Stelle oder einer sonst damit beauftragten Person angesehen, die unmittelbar auf wahrgenommene Ereignisse reagieren kann, etwa durch eigenes Agieren, durch Verständigen von Polizei oder Rettungsdienst (sogenannte technikgestützte Kontrolle des Verhaltens von Personen). Der TLfDI sah die Videoüberwachung in Form der Videoaufzeichnung im vorliegenden Fall als kritisch an, da die Videoaufzeichnung nicht bewirkt beziehungsweise ermöglicht hätte, dass unmittelbar und zeitnah auf Vorfälle am Eingangsbereich des Kindergartens reagiert werden kann, das heißt, sie war nicht wirklich geeignet, den mit ihr verfolgten Zweck zu erreichen, nämlich die Verhinderung der Tatsache, dass Kinder ohne Kenntnisnahme des Personals das Gelände verlassen.
2. Erforderlichkeit der Videoüberwachung:
Ferner muss die Videoüberwachung erforderlich sein. Hierbei ist zu prüfen, ob sie das mildeste Mittel ist, um den festgelegten Zweck zu erreichen. Mildere Mittel sind alle anderen Maßnahmen, die weniger in das Grundrecht auf informationelle Selbstbestimmung eingreifen als die Videoüberwachung. Nur wenn alle anderen milderen Mittel

ausgeschöpft sind, kann die Umsetzung der Videoüberwachung in Betracht gezogen werden. Im vorliegenden Fall waren zu diesem Zweck etliche andere Mittel denkbar. Der TLfDI hat somit dem Kindergarten angeraten, unter anderem die folgenden Alternativen (milderen Mittel) zu einer Videoüberwachung in Betracht zu ziehen:
1) Das Postfach/den Postkasten außerhalb des Zaunes vom Kindergarten aufstellen zu lassen, damit die Zusteller die Briefe und die Postsendungen ins Postfach legen können, ohne dabei das Kindergartengelände betreten zu müssen, und/oder
2) ein neues Tor mit verbessertem Schließsystem und Klingelanlage mit Gegensprechfunktion einbauen zu lassen.
Aufgrund der Beratung des TLfDI hat der Kindergarten zunächst Abstand von dem Vorhaben der Videoüberwachung genommen und wird stattdessen die oben genannten milderen Mittel prüfen und umsetzen.

2.15 Thüringer Gesetz zur Förderung der Teilnahme an Früherkennungsuntersuchungen für Kinder

Beim Datenschutz gilt das so genannte Verbot mit Erlaubnisvorbehalt. Es bedeutet, dass jede Verarbeitung von personenbezogenen Daten grundsätzlich verboten ist, es sei denn, es gibt für sie eine Rechtsgrundlage. Eine solche kann sich aus einem Gesetz, wie beispielsweise dem ThürFKG ergeben.

Ein Bürger beschwerte sich beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), weil er sich durch die nach dem Thüringer Gesetz zur Förderung der Teilnahme an Früherkennungsuntersuchungen für Kinder (ThürFKG) in seinen Grundrechten, insbesondere dem Recht auf informationelle Selbstbestimmung eingeschränkt sah. Nach seiner Auffassung handelte es sich bei dem Gesetz um einen europarechtswidrigen Verstoß gegen Art. 23 Abs. 2 Buchstabe c Datenschutz-Grundverordnung (DS-GVO).
Zweifellos wird durch das Gesetz, wie dies auch in dessen § 12 ausgeführt wird, das Recht auf Schutz der personenbezogenen Daten (Art. 6 Abs. 2 der Verfassung des Freistaats Thüringen) eingeschränkt (Art. 6 Abs. 3 der Verfassung des Freistaats Thüringen). Das ThürFKG sieht etliche Datenverarbeitungen vor. Nach § 3 ThürFKG erfolgen Meldungen vom Landesrechenzentrum an das Vorsorgezentrum. Wird eine Früherkennungsuntersuchung von der U 4 an oder eine vergleichbare Früherkennungsuntersuchung trotz Einladung und

Erinnerung nicht innerhalb des für diese vorgesehenen Zeitraums unter Berücksichtigung der Toleranzgrenze nachgeholt, übermittelt das Vorsorgezentrum dem zuständigen Jugendamt bestimmte Daten nach § 7 ThürFKG. All dem steht Art. 23 Abs. 2 Buchstabe c) DS-GVO allerdings nicht grundsätzlich entgegen. Diese Bestimmung betrifft nur Gesetzgebungsmaßnahmen, die die Pflichten und Rechte gemäß den Art. 12 bis 22 und 34 sowie Art. 5 DS-GVO beschränken, sofern dessen Bestimmungen den in Art. 12 bis 22 DS-GVO vorgesehenen Rechten entsprechen.
Nach dem ThürFKG ist die verantwortliche Stelle, das Vorsorgezentrum für Kinder, befugt, für seine Aufgabenerfüllung die dort genannten personenbezogenen Daten von Personensorgeberechtigten und deren Kindern zu verarbeiten. Die Rechte der betroffenen Personen nach der DS-GVO werden dabei nicht eingeschränkt, vielmehr bilden die Vorschriften des ThürFKG die erforderliche Rechtsgrundlage für die Datenverarbeitung nach Art. 6 Abs. 1 Satz 1 Buchstabe c) und e) DS-GVO. Einer Einwilligung der betroffenen Personen in die Datenverarbeitung nach Art. 6 Abs. 1 Buchstabe a) DS-GVO bedarf es daher nicht.
Dem TLfDI als Datenschutzaufsichtsbehörde im Freistaat Thüringen kommt weder Gesetzgebungskompetenz noch die Möglichkeit der Gesetzesinitiative zu. Er wird tätig, wenn es Anhaltspunkte für einen datenschutzrechtlichen Verstoß bei der Verarbeitung personenbezogener Daten durch die verantwortliche Stelle gibt. Hierfür gab es aber im vorliegenden Fall keine Anhaltpunkte.

2.16 Datenschutz bei der Vorlage von Kontoauszügen beim Jobcenter

Die Vorlage von Kontoauszügen der letzten drei Monate vor Antragstellung beim Jobcenter stellt eine nach Art. 6 Abs. 1 Satz 1 Buchstabe e) DS-GVO und §§ 67a und 67b SGB X zulässige Datenverarbeitung dar. Die Antragsteller sollten über die Möglichkeit von Schwärzungen einzelner Buchungen nach § 67a Abs. 1 Satz 2 SGB X in Verbindung mit Art. 9 Abs. 1 DS-GVO vorab informiert werden.

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichte eine Anfrage eines Bürgers hinsichtlich der Leistungen der Grundsicherungen im Alter und bei Erwerbsminderung nach Sozialgesetzbuch (SGB) Zwölftes Buch (XII).

Dabei erkundigte sich der Betroffene, für wie viele Monate rückwirkend das Jobcenter die Vorlage von Kontoauszügen bei der Antragstellung verlangen darf. Auch wurde erfragt, inwiefern dabei eine Schwärzung der Kontoauszüge erfolgen könnte, und welche Regelungen für Kontoauszüge des (Ehe- oder Lebens-) Partners der antragstellenden Person gelten würden.
Aus datenschutzrechtlicher Sicht ist die Einsicht oder das Anfertigen von Kopien von Kontoauszügen durch den Sozialleistungsträger eine Verarbeitung von personenbezogenen Daten gemäß Art. 4 Nr. 1 und 2 Datenschutz-Grundverordnung (DS-GVO). Die Datenverarbeitung ist in der Regel gemäß Art. 6 Abs. 1 Buchstabe e) in Verbindung mit Abs. 3 Buchstabe b) DS-GVO und §§ 67a und 67b SGB X rechtmäßig.
Das Jobcenter als zuständiger Sozialleistungsträger ist bei der Bearbeitung von Anträgen auf Sozialleistungen nach dem Vierten Kapitel des SGB XII verpflichtet, das Vorliegen der Anspruchsvoraussetzungen im konkreten Leistungsfall zu prüfen. Eine Voraussetzung ist dabei, dass der Hilfebedürftige nicht in der Lage ist, aus eigenem Einkommen und/oder Vermögen seinen notwendigen Lebensunterhalt gemäß § 43 SGB XII zu sichern. Hierfür wird die Einkommens- und Vermögenssituation des Hilfebedürftigen festgestellt. Kontoauszüge sind dabei ein zulässiges und notwendiges Beweismittel gemäß § 60 Abs. 1 Nr. 3 SGB I.
Das Bundessozialgericht hat zur Vorlagepflicht von Kontoauszügen im Rahmen von Ansprüchen nach dem SGB II am 19. Februar 2009 (Az.: B 4 AS 10/08) in einer Grundsatzentscheidung festgestellt, dass Leistungsempfänger im Rahmen der Mitwirkungspflichten gemäß §§ 60 ff. SGB I verpflichtet sind, bei jeder Leistungsbeantragung ihre Kontoauszüge der letzten drei Monate vorzulegen. Im Einzelfall kann beim Verdacht auf Missbrauch von Sozialleistungen die Vorlage der Kontoauszüge über den Zeitraum von drei Monaten hinaus erforderlich sein.
Das Schwärzen von einzelnen Buchungen kann dem Antragsteller dabei nicht grundsätzlich verwehrt werden. Eine Mitwirkung des Antragstellers kann lediglich im Rahmen des Verhältnismäßigkeitsgrundsatzes verlangt werden und muss erforderlich und angemessen sein. Die Betroffenen müssen auf die Möglichkeit des Schwärzens bereits bei der Anforderung der Kontoauszüge hingewiesen werden. Schwärzungen können unabhängig vom Betrag grundsätzlich dann

vorgenommen werden, wenn die Buchungstexte Angaben über besonders geschützte Daten im Sinne des § 67a Abs. 1 Satz 2 SGB X in Verbindung mit Art. 9 Abs. 1 DS-GVO 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 oder bei Zahlungen an eine Religionsgemeinschaft die Bezeichnung der Organisation geschwärzt werden. Der Text „Mitgliedsbeitrag" oder „Spende" sollte lesbar bleiben, um Missverständnisse zu vermeiden. Diese Grundsätze sind auch für Ansprüche nach dem SGB XII anwendbar.
Im Hinblick auf die Kontoauszüge der (Ehe- oder Lebens-) Partner eines Antragstellers heißt es in § 117 Abs. 1 SGB XII, dass diese ebenfalls gegenüber dem Träger der Sozialhilfe zur Auskunft verpflichtet sind. Hierfür müssen sie auf Verlangen Beweisurkunden vorlegen. Auch hierbei muss es den Betroffenen in gewissen Fällen möglich sein, Schwärzungen der Kontoauszüge vorzunehmen, wenn es sich beispielsweise um besonders geschützte Daten handelt.

2.17 Umgang mit Sozialhilfeakten – Verantwortlich aufbewahren – gilt auch für „geerbte" Altakten

Die Aufbewahrung von Sozialhilfeakten ist eine Form der Verarbeitung personenbezogener Daten, die nur solange zulässig ist, wie die Akten zur Erfüllung einer gesetzlichen Aufgabe in der Behörde benötigt werden. Geht die Aufgabe im Zuge einer gesetzlichen Neugliederung auf eine andere Gebietskörperschaft über, ist diese auch für die datenschutzkonforme Aufbewahrung und Sicherung der übernommenen Altakten verantwortlich.

Der Datenschutzbeauftragte einer Kommunalverwaltung wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) mit der Frage, ob und gegebenenfalls wie lange die Altakten des Sozialamtes im Archiv seiner Behörde verbleiben können. Hintergrund war der durch ein Neugliederungsgesetz angeordnete Übergang der Aufgabe auf eine andere Gebietskörperschaft.
Zur Beantwortung dieser Frage stellte der TLfDI zunächst fest, dass es sich bei der vorrübergehenden Aufbewahrung von Akten nicht um

einen Fall der Archivierung handelt. Zwar wird im normalen Sprachgebrauch unter den Begriffen Archivierung und Aufbewahrung oft dasselbe verstanden. Nach der Datenschutz-Grundverordnung (DS-GVO) ist aber zu differenzieren. Werden personenbezogene Daten ausschließlich für Archivzwecke verarbeitet, dürfen diese „länger“ als für die ursprüngliche Verarbeitung nötig aufbewahrt und gespeichert werden (Art. 5 Abs. 1 Buchstabe b) DS-GVO), um Unterlagen von bleibendem Wert für die Allgemeinheit zu erhalten (vergleiche § 2 Thüringer Archivgesetz – ThürArchivG). Werden hingegen Akten mit Dokumenten zu abgeschlossenen Vorgängen aufbewahrt, um im Rahmen der Sachbearbeitung gegebenenfalls auf sie zurückgreifen zu können, handelt es sich nicht um eine Archivierung im Rechtssinne. Diese Aufbewahrung von Akten gehört zu den „klassischen“ Verarbeitungspflichten (Art. 6 Abs. 1 Satz 1 Buchstabe c) DS-GVO), die dem Grundsatz der Erforderlichkeit unterliegt (Art. 6 Abs. 3 DS-GVO) und auf das notwendige Maß beschränkt sein muss (Art. 5 Abs. 1 Buchstabe c) DS-GVO). Wie das Sozialgesetzbuch (SGB) in Konkretisierung dieser vorrangigen Bestimmungen der DS-GVO im Zehnten Buch zum Ausdruck bringt (§ 67a Abs. 1 SGB X), ist die Verarbeitung der Sozialdaten somit nur solange zulässig, wie ihre Kenntnis zur Erfüllung der gesetzlichen Aufgaben erforderlich ist (so auch: Bundessozialgereicht – BSG – Urteil vom 14. Mai 2020, Aktenzeichen: B 14 AS 7/19 R). Andernfalls haben die Betroffenen einen Anspruch auf Löschung ihrer personenbezogenen Daten, die mit einer antragsunabhängigen Löschpflicht der zuständigen Behörde korrespondiert (Art. 17 Abs. 1 Buchstabe e) DS-GVO).

Mit Blick auf die Aufgabenübertragung im Zuge einer Gebiets- und/oder Funktionalreform betonte der TLfDI im konkreten Fall, dass der neue Aufgabenträger mit der gesetzlich angeordneten Funktions- und Einzelrechtsnachfolge auch für die datenschutzkonforme Aufbewahrung und Sicherung der Altakten verantwortlich ist. Die Verantwortlichkeit nach der DS-GVO knüpft an die gesetzliche Zuweisung an, ist also gerade nicht davon abhängig, welche Stelle (Behörde) die Daten ursprünglich erhoben und verarbeitet hat (Art. 4 Nr. 7 DS-GVO). Der neue Aufgabenträger muss deshalb nicht nur die Aufbewahrungsfristen festlegen, sondern grundsätzlich auch die Aufbewahrung der Altakten selbst übernehmen.

Da im einschlägigen Fachgesetz, dem Zwölften Buch des Sozialgesetzbuchs (SGB XII), anders als etwa im Sozialgesetzbuch Viertes und Fünftes Buch keine speziellen Regelungen für die Aufbewahrung

der Sozialakten enthalten sind, muss die Aufbewahrungsfrist von der aktenführenden Behörde festgelegt werden. Die Aufbewahrungsrichtlinie für die Behörden des Freistaats Thüringen (ThürAufbewRL, Staatsanzeiger 31/2019), die von den Gemeinden und Gemeindeverbänden entsprechend angewandt werden soll (Ziffer 1.9), sieht zwar für Schriftgut, bei dem keine gesetzliche Aufbewahrungsfrist festgesetzt ist und das seiner Bedeutung nach einer längeren Aufbewahrung bedarf, eine Frist von fünf Jahren vor (Ziffer 4.1). Angesichts des großen Leistungsspektrums in der Sozialhilfe und der verschiedenen Teilleistungen innerhalb der Fallbearbeitung kommt aber für Sozialakten eine pauschale Aufbewahrungsfrist nicht in Betracht. Vielmehr muss diese aufgabenbezogen festgesetzt und damit sachnotwendig differenziert werden. Dabei ist auch eine längerfristige Aufbewahrung denkbar, wenn diese etwa zur Geltendmachung gesetzlicher Forderungen, Rücknahmen oder Aufhebungen erforderlich ist (vergleiche § 45 Abs. 3 Satz 3 SGB X). Werden Sozialdaten hingegen für die Sachbearbeitung nicht mehr benötigt, lässt sich eine Aufbewahrung allenfalls für ein Jahr rechtfertigen, damit das zuständige öffentliche Archiv über die Archivwürdigkeit der ihm angebotenen Unterlagen entscheiden kann (§ 11 Abs. 5 ThürArchivG). Ergänzend wies der TLfDI darauf hin, dass die verantwortliche Behörde die Aufbewahrungsfrist nicht nur am Grundsatz der Datenminimierung (Art. 5 Abs. 1 Buchstabe c) DS-GVO) ausrichten muss, sondern auch in einem entsprechenden Löschkonzept zu dokumentieren hat (Art. 5 Abs. 2 DS-GVO).

2.18 Ärger ums „Azubi-Ticket Thüringen“

Auch für die Antragstellung bei den Beförderungsunternehmen gilt, dass nur für den jeweiligen Zweck erforderliche Daten abgefragt werden dürfen. Umfassende Angaben zu Personalausweisdaten sowie die Preisgabe seiner Bankkarte oder gar des Kontoauszuges eines Betroffenen gehören nicht dazu!

Im vergangenen Jahr war dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) zur Kenntnis gelangt, dass ein Beförderungsunternehmen aus datenschutzrechtlicher Sicht nicht erforderliche personenbezogene Daten im Rahmen der Antragstellung zu einem „Azubi-Ticket“ abgefragt hat.

So wurden von dem Unternehmen bei Abgabe des Antrages, ein solches „Azubi-Ticket“ zu erhalten, ein gültiges Personalausweisdokument sowie ein aktueller IBAN- und BIC-Nachweis (konkret eine Kopie der Bankkarte oder des Kontoauszuges) verlangt. Als Grund für dieses Prozedere nannte das Beförderungsunternehmen, dass so die Prüfung der korrekten Personen- und Adressdaten sichergestellt werden könne, die zur Bearbeitung des Abo-Antrages notwendig seien. Eine Vorlage der Bankkarte oder des Kontoauszuges erfolge ebenfalls zum Abgleich der Daten. Hierzu wurde dem TLfDI mitgeteilt, dass es durch den händischen Übertrag der Bankkartendaten auf das Abo-Formular regelmäßig zu Übertragungsfehlern – verursacht durch den Antragsteller – kommen würde. Dies wiederrum könne bei dem betroffenen Beförderungsunternehmen zu Rücklastschriften und Neuausstellungen des Abo-Antrages und damit zu einem Mehraufwand führen.
In verschiedenen Bereichen des öffentlichen Lebens kommt es immer wieder dazu, dass die Vorlage des Personalausweisdokumentes zur Identitätsfeststellung verlangt wird. Soweit Anträge postalisch bei den Behörden eingehen, wird teilweise auch eine Kopie des Personalausweises verlangt (so zum Beispiel auch bei Auskunftsersuchen im Polizeibereich). Der TLfDI kann dieser Intention grundsätzlich folgen. Nach Auffassung des TLfDI sind jedoch nicht alle auf dem Ausweisdokument befindlichen personenbezogenen Daten für eine Identitätsfeststellung erforderlich. Soweit demnach die Vorlage einer Kopie des Ausweisdokumentes verlangt wird, weil ein Antrag postalisch gestellt wird, hat der TLfDI im konkreten Fall das Beförderungsunternehmen darauf hingewiesen, dass nicht relevante personenbezogene Daten durch die Antragsteller/innen unkenntlich gemacht beziehungsweise geschwärzt werden können. Für einen Abgleich der Personen- und Adressdaten maximal als erforderlich erachtet werden lediglich die Übermittlung des Namens, des Geburtsdatums und der Adresse.
Hingegen wurde die Vorlage oder die Kopie der Bankkarte oder gar eines Kontoauszuges im Rahmen der Antragstellung zum „Azubi-Ticket“ durch den TLfDI gänzlich abgelehnt. Die Antragsteller/innen müssen ihre Bankdaten im Rahmen des Lastschriftverfahrens bereits händisch in das Formular eintragen. Das dargestellte Risiko eines Mehraufwandes bei dem Beförderungsunternehmen, weil es gegebenenfalls zu (von den Antragsteller/innen verursachten) Übertragungsfehlern kommen könnte, steht hinter dem Schutz der personenbezogenen Bankdaten der Antragsteller/innen zurück. Eine Erforderlichkeit

der weiteren Vorlage oder gar einer Kopie der Bankkarte/des Kontoauszugs sah der TLfDI daher nicht und hat dem Beförderungsunternehmen dringend angeraten, diese Formulierung aus dem Formular „Azubi Ticket“ zu entfernen.
Der TLfDI hatte im Verfahren auch angedroht, von seinen Befugnissen nach § 7 Abs. 1 Satz 2 Thüringer Datenschutzgesetz (ThürDSG) in Verbindung mit Art. 58 Abs. 2 Datenschutz-Grundverordnung (DS-GVO) Gebrauch zu machen. Glücklicherweise musste es nicht soweit kommen. Das betreffende Beförderungsunternehmen war sehr kooperativ und zeigte sich einsichtig. Sowohl die Passagen zur Vorlage beziehungsweise Kopie des Personalausweises als auch jene zur Bankkarte oder eines Bankauszuges wurden ersatzlos und umgehend aus dem Antragsformular entfernt. Damit konnte der TLfDI das Verfahren aus datenschutzrechtlicher Sicht im Sinne des § 7 Abs. 1 Satz 5 ThürDSG in Verbindung mit Art. 58 und 83 DS-GVO abschließen.

2.19 Abfrage des 3G-Status zum Elternabend

Ob vor dem Elternabend der 3G-Status abgefragt werden darf, hängt davon ab, ob die Schule sich in der Basis-, Situations- oder Warnphase befindet. Die Einteilung in diese Phasen richtet sich danach, ob bestätigte Corona-Infektionen an der Schule vorliegen (Situationsphase) oder das zuständige Ministerium in Anlehnung an das Frühwarnsystem des Gesundheitswesens die Warnphase ausgerufen hat. Maskenpflicht und die Abgabe der notwendigen Informationen zur Kontaktnachverfolgung gelten in jeder Phase.

Maskenpflicht, Testregime, Impfnachweis – für die Schulen im Freistaat war die Lage in den vergangenen Monaten nicht immer übersichtlich. Beständig angepasste Rechtsverordnungen, kurzfristig erlassene Allgemeinverfügungen mit missverständlichen Formulierungen sowie der Wechsel zwischen Basis- und Situationsphasen führten so manches Mal dazu, dass tagesaktuell nicht ganz klar war, was derzeit überhaupt galt. Und so viele Gesundheitsdaten wie zu Corona-Zeiten mussten die Schulen ebenfalls noch nie verarbeiten. Dass Gesundheitsdaten unter die besonderen Kategorien der personenbezogenen Daten fallen, deren Verarbeitung gemäß Art. 9 Abs. 1 Datenschutz-Grundverordnung (DS-GVO) grundsätzlich unzulässig sind und die nur unter den strengen Vorgaben des Art 9 Abs. 2 DS-GVO

verarbeitet werden dürfen, war bei den meisten Schulen schnell in einen routinierten und datenschutzkonformen Umgang mit diesen Daten übergegangen.
Der Schutz von Lehrkräften, Schülerinnen und Schülern vor einer Infektion stand dabei stets im Vordergrund. Aus diesem Anlass wurden an einigen Thüringer Schulen die Einladungen zum Elternabend auch unter der Vorgabe 3G – also geimpft, genesen oder getestet – versendet. Der entsprechende Nachweis solle beim Einlass zum Schulgebäude von einer dafür abgestellten Lehrkraft kontrolliert werden.
Nicht wenige Eltern wandten sich daraufhin an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und baten um schnelle Auskunft, ob die geforderten Nachweise tatsächlich an der Einlasskontrolle vorgezeigt werden müssten. Entscheidend für die Beantwortung der Anfragen war die jeweilige Corona-Lage an der Schule, denn danach richtete sich die Frage, ob der Schulbetrieb in der Basis-, Situations- oder der Warnphase lief.
Während die Regelungen der Basisphase immer gelten, sehen die Situationsphase, die bei einer bestätigten Infektion mit dem Corona-Virus innerhalb der Schule eintritt, sowie die Warnphase, die vom Thüringer Ministerium für Bildung, Jugend und Sport (TMBJS) in Anlehnung an das landesweite Frühwarnsystem ausgerufen werden kann, schärfere Maßnahmen zum Schutz vor einer möglichen Übertragung des SARS-CoV-2-Virus vor (§ 1 Abs. 2 Thüringer Verordnung zur Eindämmung der Ausbreitung des CoronavirusSARS-CoV-2 in Kindertageseinrichtungen, der weiteren Jugendhilfe, Schulen und für den Sportbetrieb (ThürSARS-CoV-2-KiJuSSp-VO)).
Zum Zeitpunkt der Anfragen beim TLfDI befanden sich nach Medienberichten alle Thüringer Schulen in der Basisphase – also ohne eine bestätigte Infektion mit dem SARS-CoV-2 Virus in der Schule. In dieser Basis-Phase gilt gemäß § 12 ThürSARS-CoV-2-KiJuSSp-VO, dass Eltern beim Zutritt zur Schule verpflichtet sind, eine Mund-Nasen-Bedeckung zu tragen. Außerdem müssen sie sich bei der Leitung der Einrichtung namentlich anmelden und eine schriftliche Erklärung zur Erreichbarkeit und darüber, dass bei ihnen keine erkennbaren Symptome einer COVID-19-Erkrankung vorliegen, abgeben. Zusätzlich müssen die Eltern für die Kontaktnachverfolgung gemäß § 9 Abs. 5 ThürSARS-CoV-2-KiJuSSp-VO die personenbezogenen Daten (Name und Erreichbarkeit) angeben. Diese sind von der Schule für die Dauer von vier Wochen aufzubewahren, vor unberechtigter

Kenntnisnahme und dem Zugriff Dritter zu schützen, für die zuständige Behörde (das TMBJS) vorzuhalten und auf Anforderung an diese zu übermitteln sowie unverzüglich nach Ablauf der 4-wöchigen Aufbewahrungsfrist datenschutzgerecht zu löschen oder zu vernichten. Außerdem müssen die Schulen den Betroffenen, also den Eltern, bei der Erhebung dieser personenbezogenen Daten gemäß Art. 13 DS-GVO die Rechtsgrundlage, den Zweck der Verarbeitung, die Speicherdauer sowie sonstige in der Bestimmung genannte Informationen mitteilen. Es ist also auch in der Basisphase eine ganze Reihe von Dingen, die es vor einem Elternabend zu beachten gilt – für eine Abfrage des Status „geimpft/genesen/getestet" besteht jedoch in der Basisphase keine Rechtsgrundlage. Die Abfrage des 3G-Status ist gemäß § 27 Abs. 1 ThürSARS-CoV-2-KiJuSSp-VO erst für die Situationsphase vorgesehen.

2.20 Beschwerde über Corona-Testpflicht in der Schule

Bei der Corona-Testpflicht im Klassenzimmer dürfen die Testergebnisse nicht öffentlich gemacht werden – das Bekanntwerden eines positiven Testergebnisses durch anschließende Separierung der betroffenen Schülerinnen und Schüler und Ausschluss vom Unterricht muss dabei aber in Kauf genommen werden.

Die Durchführung des verbindlichen Testregimes auf das Vorliegen einer Infektion mit dem SARS-CoV-2 Virus hat die Thüringer Schulen einigen organisatorischen Aufwand gekostet – schließlich werden dabei besondere Kategorien personenbezogener Daten gemäß Art. 9 Abs. 1 Datenschutz-Grundverordnung (DS-GVO) – nämlich Gesundheitsdaten – erhoben, deren Verarbeitung grundsätzlich untersagt und nur unter strengen gesetzlichen Auflagen rechtmäßig ist. Mit § 41 der Thüringer Verordnung über die Infektionsschutzregeln zur Eindämmung der Ausbreitung des Coronavirus SARS-CoV-2 in Kindertageseinrichtungen, der weiteren Jugendhilfe, Schulen und für den Sportbetrieb (ThürSARS-CoV-2-KiJuSSp-VO) gibt es zwar eine Rechtsgrundlage, die den Eingriff legitimiert, eine genaue Durchführungsbestimmung oder einen Erlass, wie die Tests konkret ablaufen sollen, existiert jedoch nicht.
Aus rein praktischen Erwägungen heraus haben die meisten Schulen den Weg gewählt, zweimal wöchentlich in der ersten Stunde, beaufsichtigt vom jeweiligen Fachlehrer, im Klassenverband gemeinsam

die Tests durchzuführen. Die Ergebnisse werden dann bilateral zwischen den Schülerinnen beziehungsweise Schülern mit der Lehrkraft ausgewertet. Im Falle eines positiven Ergebnisses sieht § 44 Abs. 3 ThürSARS-CoV-2-KiJuSSp-VO vor, dass die beziehungsweise der Betroffene „durch das betreuende pädagogische Personal unverzüglich zu isolieren“ ist, „für minderjährige Schülerinnen und Schüler ist die Abholung durch berechtigte Personen unverzüglich zu veranlassen“ und es besteht für die „getestete Person die Verpflichtung, unverzüglich einen PCR-Test durchführen zu lassen“.
Dass bei einer unverzüglichen Isolierung und Abholung einer Klassenkameradin beziehungsweise eines Klassenkameraden im Anschluss an den Test den in der Schule verbleibenden Mitschülern klar sein dürfte, dass ein positiver Selbsttest die Ursache ist, liegt auf der Hand und wurde vom Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) auch umgehend moniert. Wegen fehlender personeller und finanzieller Ausstattung hielten die Schulen jedoch generell an diesem Verfahren fest.
Dies zog unter anderem die Beschwerde einer Mutter nach sich, die sich umfassend über die „Quasi-Offenlegung“ von Gesundheitsdaten und den aus ihrer Sicht damit verbundenen schweren Eingriff in die Persönlichkeitsrechte ihres Kindes beschwerte. Dem TLfDI trug sie vor, dass eine Testung zu Hause den gleichen Zweck erfüllen würde, zumal ein positives Ergebnis im Selbsttest nicht immer ein positives Testergebnis im anschließend durchzuführenden genaueren PCR-Test nach sich zöge. Bei einer Testung zuhause könne man sein Kind also so lange einfach krankmelden, bis ein PCR-Test Klarheit gebracht habe, ohne dass möglicherweise der „falsche“ Verdacht einer vorliegenden Infektion mit dem SARS-CoV-2-Virus die Runde in der Schule machen würde.
Für die Durchführung der Tests gab es zum Zeitpunkt der Beschwerde bereits (ober-)gerichtliche Entscheidungen, unter anderem vom Oberverwaltungsgericht Nordrhein-Westfalen (OVG NRW), Beschluss 13 B 559/21.NE vom 22. April 2021. Danach hegt das OVG NRW „(…) gegen die (…) Testpflicht keine offensichtlich durchgreifenden Bedenken“ und erachtet sie als „verhältnismäßige Schutzmaßnahme“. Zu einer Durchführung der Tests zuhause hat das Gericht Folgendes ausgeführt: „(…) eine Selbsttestung von Schülern zu Hause durch ihre Eltern wäre voraussichtlich nicht gleich wirksam. Unabhängig von etwaigen Manipulationsmöglichkeiten, die sich im häuslichen Bereich

ergeben könnten, bietet der in der Schule durchgeführte Test die bessere Gewähr dafür, dass er tatsächlich, regelmäßig und ordnungsgemäß durchgeführt wird.“ (OVG NRW, a.a.O, Rn. 79).
Der TLfDI konnte der Mutter jedoch den Hinweis geben, dass zur Vermeidung der Testsituation in der Schule bereits mit Einführung des verbindlichen Testregimes die Möglichkeit bestand, einen Nachweis eines PCR-Tests mit negativem Ergebnis, der nicht älter als 48 Stunden war oder eine Bescheinigung über ein negatives Testergebnis eines durgeführten Antigenschnelltest, der nicht länger als 24 Stunden zurücklag, vorzulegen (§ 34b Abs. 1 Satz 1 bis 3 der ThürSARS-CoV-2 – IfS-Maßn-VO in der Fassung vom 5. Mai 2021).

2.21 Abfrage nach Corona-Test-Ergebnis bei Mitschülern und Eltern

Lehrkräfte und Schulleitung dürfen bei Erkrankung eines Kindes nicht bei Eltern und Mitschülern nach einer Diagnose fragen. Dies stellt den Versuch einer unzulässigen Verarbeitung besonderer Kategorien von personenbezogenen Daten dar.

„Wie ist denn nun der Corona-Test Ihrer Tochter ausgefallen?“ Eine solche Nachfrage einer Lehrerin bei der Mutter einer Schülerin war Anlass für eine Beschwerde beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Mehr noch, die Lehrerin hatte auch eine Klassenkameradin gefragt, wie es dem Mädchen ginge, das wegen Krankheit nicht zur Schule gekommen war. Aus Fürsorge habe sie gefragt, so die Antwort der Lehrerin auf die Aufforderung des TLfDI zur Stellungnahme, das müsse doch wohl noch erlaubt sein. Außerdem habe die Mutter der Schule selbst mitgeteilt, dass bei ihrer Tochter ein Corona-Test durchgeführt werde und eine mögliche Infektion ja damit öffentlich gemacht.
Ist der Datenschutz wirklich so streng, dass er jegliche empathische Frage und wohlmeinende Besorgnis verbietet? Natürlich nicht. Aber es gibt datenschutzrechtliche Einschränkungen bei der Abfrage von personenbezogenen Daten, insbesondere wenn es sich um besondere Kategorien von personenbezogenen Daten im Sinne des Art. 9 Abs. 1 Datenschutz-Grundverordnung (DS-GVO), wie zum Beispiel Gesundheitsdaten, handelt. Deren Verarbeitung ist grundsätzlich unter-

sagt, es gibt aber Ausnahmen, zum Beispiel, wenn die betroffene Person diese Daten offensichtlich öffentlich gemacht hat (Art. 9 Abs. 2 Buchstabe e) DS-GVO).
Im konkreten Fall hatte die Mutter der Schülerin die Schule per E-Mail darüber informiert, dass ihre Tochter erkrankt sei, ein Corona-Test durchgeführt werden würde und angekündigt, die Schule über das Ergebnis des Tests zu unterrichten. Nach erfolgtem Test änderte die Mutter jedoch ihre Meinung und wollte das Test-Ergebnis der Schule doch nicht mehr mitteilen. Die Meldung einer Erkrankung und einer möglichen Diagnose gegenüber einer Lehrkraft beziehungsweise der Schule stellt keine offensichtliche Veröffentlichung im Sinne des Art. 9 Abs. 2 Buchstabe e) DS-GVO dar, vielmehr sind Sorgeberechtigte gemäß § 5 Abs. 1 Thüringer Schulordnung verpflichtet, den Grund (Erkrankung) für die Verhinderung ihrer Kinder für die Teilnahme am Unterricht an die Schule zu melden. Die E-Mail der Mutter an die Schule war also keinesfalls damit gleichzusetzen, dass sie die Erkrankung ihrer Tochter sowie eine mögliche Diagnose offensichtlich öffentlich gemacht hätte.
Eine weitere Ausnahme vom Verbot der Verarbeitung von Gesundheitsdaten regelt Art. 9 Abs. 2 Buchstabe g) DS-GVO; danach ist die Verarbeitung zulässig, sofern sie aus Gründen eines erheblichen öffentlichen Interesse erforderlich ist und auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedsstaats erfolgt, das in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht. Zu denken ist hier beispielsweise an die namentliche Meldung nach § 9 des Infektionsschutzgesetzes.
Hier hätte ein erhebliches öffentliches Interesse zwar darin liegen können, bei einer nachgewiesenen Infektion mit dem SARS-CoV-2 Virus der Schülerin eine Kontaktnachverfolgung zu ihren Klassenkameraden und unterrichtenden Lehrkräften zu gewährleisten, damit durch die Anordnung von Quarantänemaßnahmen für die Kontaktpersonen Infektionsketten unterbrochen hätten werden können. Hierauf konnte sich die Schule jedoch nicht berufen, da für die Anordnung von Quarantänemaßnahmen ausschließlich das zuständige Gesundheitsamt ermächtigt ist.
Wenngleich die Mutter angekündigt hatte, das Ergebnis des Corona-Tests ihrer Tochter der Schule mitzuteilen, stellt die Nachfrage der

Lehrerin nach dem Testergebnis den Versuch einer unzulässigen Verarbeitung personenbezogener Daten der besonderen Kategorie dar.
Die Verarbeitung in Form der Offenlegung durch die Lehrkräfte im Rahmen eines Gesprächs mit Schülerinnen und Schülern, stellt damit immer einen Verstoß gegen die DS-GVO dar. Dies ist selbst dann der Fall, wenn die betroffene Person diese Information einer Lehrkraft mitgeteilt hat, da eine solche Mitteilung keineswegs eine offensichtliche Öffentlichmachung im Sinne von Art. 9 Abs. 2 Buchstabe e) DS-GVO darstellt.
Der TLfDI warnte die Schulleitung als Verantwortliche für die Verarbeitung der personenbezogenen Daten besonderer Kategorie. Rechtsgrundlage für die Warnung ist Art. 58 Abs. 2 Buchstabe a) DS-GVO. Demnach verfügt die Aufsichtsbehörde über Abhilfebefugnisse, die es ihr gestatten, einen Verantwortlichen oder einen Auftragsverarbeiter zu warnen, dass beabsichtigte Verarbeitungsvorgänge voraussichtlich gegen die DS-GVO verstoßen. Hier war die Datenverarbeitung allenfalls „versucht“ und nicht tatsächlich erfolgt, sodass eine Verwarnung im Sinne von Art. 58 Abs. 2 Buchstabe b) DS-GVO ausschied.

2.22 Beschwerde über einen Schulleiter wegen Weiterleitung einer Mail

Eine Mutter beschwerte sich über ihren dienstlichen E-Mail-Account über schulische Vorgänge. Der Schulleiter, der gleichzeitig Mitglied im Beirat des Arbeitgebers der Mutter ist, informierte deren Vorgesetzte über die unerlaubte Nutzung des E-Mail-Accounts – und kassierte eine Verwarnung durch den TLfDI.

„Die Welt ist klein“ – so mag ein Schulleiter gedacht haben, als er den E-Mail-Absender einer Beschwerde las, die die Mutter eines Schülers geschrieben hatte. Obgleich das von ihr geschilderte Problem ein rein schulisches und damit ihr privates Anliegen war, hatte die Mutter ihren dienstlichen E-Mail-Account genutzt und mit ihrer dienstlichen Signatur unterschrieben. Und wie es der Zufall wollte, war der Schulleiter neben seiner beruflichen Funktion an der Schule auch Mitglied im Beirat der gemeinnützigen Gesellschaft, bei der die Mutter beschäftigt war.
Neben der Lösung des in der E-Mail geschilderten schulischen Problems widmete der Schulleiter sich einer weiteren Angelegenheit, die aus seiner Sicht einer dringenden Klärung bedurfte. Der Arbeitgeber

der Mutter hatte die private Nutzung der E-Mail Accounts verboten. Als Beiratsmitglied informierte der Schulleiter also die Vorgesetzte der Mutter über die unerlaubte Nutzung des dienstlichen E-Mail-Accounts – mit unangenehmen Folgen für die Mutter. Verärgert wandte sie sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und beschwerte sich über die Weitergabe ihrer E-Mail durch den Schulleiter an ihren Arbeitgeber.
Zur Stellungnahme durch den TLfDI aufgefordert, schilderte der Schulleiter, dass er die E-Mail und deren Inhalt zwar nicht an die Arbeitgeberin der Mutter weitergegeben habe, er habe jedoch über die unerlaubte Nutzung des dienstlichen E-Mail-Accounts für private Zwecke informiert. In seiner Eigenschaft als Mitglied im Beirat der gemeinnützigen GmbH, bei der die Mutter beschäftigt war, habe er schließlich vom Verbot zur privaten Nutzung der dienstlichen E-Mail-Accounts Kenntnis gehabt und sich offenbar verpflichtet gesehen, auch außerschulisch erzieherisch einzuwirken.
Namen und E-Mail-Adressen sind personenbezogene Daten im Sinne des Art. 4 Nr. 1 Datenschutz-Grundverordnung (DS-GVO). Die Verarbeitung – zum Beispiel Offenlegung durch Übermittlung – von personenbezogenen Daten ist nur rechtmäßig, wenn mindestens eine der Bedingungen des Art. 6 Abs. 1 Satz 1 Buchstabe a) bis f) DS-GVO vorliegt. Da die Mutter keine Einwilligung zur Weitergabe ihrer Daten gemäß Art. 6 Abs. 1 Satz 1 Buchstabe a) DS-GVO erteilt hatte, kam hier nur Art. 6 Abs. 1 Satz 1 Buchstabe e) DS-GVO in Betracht, und zwar nur, sofern die Verarbeitung in Ausübung öffentlicher Gewalt erfolgte, die dem Verantwortlichen übertragen wurde. Die Weitergabe des Namens und der verwendeten E-Mail-Adresse erfolgte jedoch weder in der Funktion als Schulleiter, noch bestand für die Schule eine Rechtsgrundlage, diese personenbezogenen Daten an Dritte weiterzugeben. Die Weitergabe des Namens und der verwendeten E-Mail-Adresse an die Arbeitgeberin der Mutter war damit unzulässig. Der TLfDI verwarnte daher den Schulleiter gemäß Art. 58 Abs. 2 Buchstabe b) DS-GVO.

2.23 Maske vergessen? Schulsekretariat darf Schüler bei der Ausgabe von Ersatzmasken nicht erfassen

Schülerinnen und Schüler, die ihre Mund-Nasen-Bedeckung vergessen haben, dürfen bei Ausgabe einer Ersatzmaske durch das Schulsekretariat nicht namentlich erfasst werden – für eine mögliche Kostenerstattung durch die Eltern fehlt die Rechtsgrundlage.

Die Hausaufgaben hat der Hamster gefressen, im Turnbeutel fehlen plötzlich die Sportschuhe, den Atlas wollte der Banknachbar mitbringen – bei Schülern sind kreative Ausreden gefragt, sonst droht eine Eltern-Information. Wer hingegen seine Mund-Nasen-Bedeckung vergessen hat, muss auch bei mehrfachen Erinnerungslücken dergleichen nicht befürchten.
Doch in einem Landkreis sah das zunächst anders aus. Das Landratsamt als zuständiger Schulträger hatte die Schulen aufgefordert, bei Ausgabe von Masken aus dem Notfallvorrat im Schulsekretariat die säumigen Schüler namentlich zu erfassen. Die Eltern wurden per Brief im Vorfeld über die geplante Vorgehensweise informiert. Mit der Frage, auf welcher Grundlage die Erfassung der Namen durch das Landratsamt zulässig sei, wandte sich daraufhin ein Beschwerdeführer an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI).
Auf Nachfrage des TLfDI antwortete das Landratsamt, Ziel der namentlichen Erfassung sei, den Eltern besonders „vergesslicher“ Kinder die Kosten für die Mund-Nasen-Bedeckungen in Rechnung zu stellen. Der Verbrauch an kostenlos im Schulsekretariat ausgegebenen Masken sei zwischenzeitlich so in die Höhe geschnellt, dass der für die Beschaffung der Masken-Vorräte an den Schulen verantwortliche Landkreis den sparsamen und wirtschaftlichen Umgang mit seinen finanziellen Ressourcen gefährdet sähe. Die kostenfreie Ausgabe der Masken sei ein falscher Anreiz. Bereits die Einführung der namentlichen Erfassung derer, die eine Maske von der Schule erhielten, hätte den gewünschten pädagogischen Effekt gehabt und der Verbrauch sei deutlich zurückgegangen.
Berufen wurde sich dabei auf ein Schreiben des Thüringer Ministeriums für Bildung, Jugend und Sport, wonach Schülerinnen und Schüler sowie alle Beschäftigten der Schule sich in eigener Verantwortung mit ausreichendem Mund-Nasen-Schutz auszustatten und die Schulen

eine Notfallreserve vorzuhalten hätten, falls jemand keine Maske mit sich führe.
Bei allem Verständnis des TLfDI für die abschreckende Wirkung der Maßnahme, handelte es sich bei der Erfassung der Namen von Schülerinnen und Schülern, die zu einem bestimmten Datum eine Maske erhalten hatten, um die Verarbeitung personenbezogener Daten. Und die ist an die rechtlichen Vorgaben der Datenschutz-Grundverordnung (DS-GVO) gebunden.
Einer der Grundsätze für die Verarbeitung personenbezogener Daten ist Rechtmäßigkeit und Transparenz, 5 Abs. 1 Buchstabe a) DS-GVO. Das Verfahren, bei dem weder festgelegt war, ab welcher ausgegebenen Stückzahl die Masken in Rechnung gestellt werden und wieviel diese kosten sollen und darüber hinaus keine Vorgabe bestand, ob die Abgabe kostenpflichtig oder kostenfrei zu gestalten sei, ließ keine rechtliche Verpflichtung erkennen, auf Grundlage derer die Namen erfasst und verarbeitet hätten werden dürfen. Die Rechtmäßigkeit auf Art. 6 Abs. 1 Satz 1 Buchstabe e) DS-GVO zu stützen, würde aber einer nationalen Vorschrift bedürfen (Art. 6 Abs. 3 DS-GVO), also zum Beispiel einer Rechtsverordnung oder kommunalen Satzung, die genau dieses Verfahren transparent und präzise regelt.
Und auch der – nicht bestreitbare – Hinweis des Landkreises, die unkontrollierte Ausgabe von Masken führe zu einer übermäßigen Belastung des Haushalts, konnte nicht als Rechtfertigung dafür dienen, dass nicht geregelt war, unter welchen konkreten rechtlichen Bedingungen die personenbezogenen Daten der betroffenen Schülerinnen und Schüler vom Schulveraltungsamt herangezogen werden dürften.
Nach dieser rechtlichen Prüfung teilte der TLfDI dem Landratsamt mit, dass die intransparente und unbestimmte Verarbeitung der personenbezogenen Daten bei der Maskenausgabe unzulässig sei. Das zuständige Schulverwaltungsamt informierte die Schulen entsprechend, dass die Mund-Nasen-Bedeckungen künftig ohne die Erfassung der Schülernamen ausgegeben werden müssen – mit dem Hinweis, die Schülerinnen und Schüler bei der Ausgabe der Masken aus der Notfallreserve zumindest mündlich an ihre Eigenverantwortung zu erinnern.

2.24 „Setzen, Sechs!“ hat ausgedient – Schulnoten dürfen vor der Klasse nicht verkündet werden.

Noten sind personenbezogene Daten von Schülerinnen und Schülern. Ihre Bekanntgabe vor der Klasse bedarf einer Rechtsgrundlage – und die ist nur für sehr wenige pädagogische Ausnahmefällen vorhanden.

„Setzen! Sechs!“ Der eine oder andere mag sich noch mit Grauen an solche hochnotpeinlichen Momente seiner Schulzeit erinnern, wenn der Lehrer vor der versammelten Klasse sein niederschmetterndes Urteil verkündete und man sich mit hochrotem Kopf auf den Stuhl sinken ließ. Die Sinnhaftigkeit solcher pädagogischen Maßnahme zu bewerten, ist nicht Aufgabe des Datenschutzbeauftragten – und doch meldete sich eine besorgte Mutter beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und schilderte folgenden Fall:
Ihr Sohn habe als Hausaufgabe in der vierten Klasse einer Grundschule ein Plakat anfertigen müssen. Dies sei nach ihrem Dafürhalten überaus gelungen und völlig zu Unrecht nur mit der Note drei bewertet worden. Sie habe die Note daher nicht unterschrieben, sondern ihre Gründe für die aus ihrer Sicht zu strenge Bewertung auf einem Zettel dargelegt, den ihr Sohn seiner Lehrerin übergab. Die Klassenlehrerin habe eben diesen Zettel der Schulleiterin gegeben, die das zum Anlass nahm, persönlich im Unterricht der vierten Klasse zu erscheinen und die an den Wänden hängenden Plakate der Schüler öffentlich zu bewerten – und ihrem Ärger Luft zu machen. Für eine vierte Klasse seien einige der Plakate deutlich zu schlecht. Gerade das besagte Werk des Jungen, der die Note drei erhalten habe, wäre nach ihrer Einschätzung viel zu gut bewertet und verdiene eigentlich eine fünf. Er solle froh sein, dass er überhaupt eine befriedigende Note erhalten habe, so das vor der Klassengemeinschaft verkündete Urteil der Schulleiterin.
Die Mutter des Schülers schilderte in ihrer Beschwerde an den TLfDI, dass ihr Sohn daraufhin von Klassenkameraden ausgegrenzt worden sei und wollte wissen, ob das öffentliche Verkünden von Noten und Leistungseinschätzungen einzelner Schüler aus Sicht des Datenschutzes überhaupt zulässig sei. Schulnoten werden in einem Dateisystem für die nichtautomatisierte Verarbeitung gespeichert, sie fallen damit unter den Anwendungsbereich der Datenschutz-Grundverordnung (Art. 2 Abs. 1 DS-GVO).

Benotungen schriftlicher Arbeiten sind personenbezogene Schülerdaten. Die Offenlegung durch mündliche Übermittlung stellt eine Verarbeitung gemäß Art. 4 Nr. 2 der Datenschutz-Grundverordnung dar. Diese Verarbeitung bedarf einer Rechtsgrundlage nach Art. 6 Abs. 1 DS-GVO in Verbindung mit Art. 5 Abs. 1 Buchstabe a) DS-GVO. Gemäß § 57 Abs. 1 Thüringer Schulgesetz ist eine Bekanntgabe personenbezogener Daten nur dann zulässig, wenn dies zur Wahrnehmung einer schulischen Aufgabe erforderlich ist. Zwar ist Wissensvermittlung und die entsprechende Bewertung vom Bildungsauftrag des Schulgesetzes gedeckt, die Bekanntgabe von Noten beziehungsweise eine individuelle Leistungseinschätzung kann jedoch auch in einem persönlichen Gespräch mit den Schülern stattfinden, ohne dass die öffentliche Verkündung aus pädagogischen Gründen erforderlich ist.

In der Praxis bedeutet das, dass die Noten einzelner Schüler vor der Klasse nur in sehr begrenzten, gut begründbaren pädagogischen Ausnahmefällen bekannt gemacht werden dürfen. Aus datenschutzrechtlicher Sicht ist neben der Nennung der Note auch das Vorführen möglicher Unzulänglichkeiten einzelner Kinder vor der Klasse nicht zulässig.

Vom TLfDI zur Stellungnahme aufgefordert, bekräftigte die Schulleiterin jedoch ihre Auffassung, dass Kritik an schlechten Leistungen sehr wohl vor der Klassenöffentlichkeit geäußert werden können müsse, damit alle Schülerinnen und Schüler dadurch die Möglichkeit erhielten, zu lernen, wo Verbesserungspotential sei.

Der TLfDI leitete daraufhin ein Verfahren gemäß § 7 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) in Verbindung mit Art. 58 DS-GVO ein, der Schulleiterin wurde erneut die Rechtslage erläutert und eine weitere Gelegenheit zur Stellungnahme gegeben. Im Zuge des Verfahrens wurden gemäß § 7 Abs. 1 Satz 3 ThürDSG auch das zuständige Schulamt und das Bildungsministerium informiert.

Der Schulamtsleiter setzte sich schließlich für die Schulleiterin ein. Nach einem Gespräch mit ihr, in dem er ihr ihre datenschutzrechtlichen Pflichten und mögliche dienstrechtliche Konsequenzen aufgezeigt hatte, versicherte sie überzeugend, ihren Fehler einzusehen und nicht zu wiederholen.

Auch in ihrer Stellungnahme gegenüber dem TLfDI zeigte die Schulleiterin nicht nur Einsicht, sondern auch glaubhaftes Bedauern, den Schüler dieser Situation ausgesetzt zu haben. Sie werde künftig darauf

achten, Noten nicht mehr in öffentlicher Form, sondern in der persönlichen Ansprache mit dem jeweiligen Schüler zu äußern und in Konfliktfällen direkt mit den betroffenen Eltern Kontakt aufzunehmen.
Aufgrund dieser positiven Einsicht konnte der TLfDI von einer Verwarnung Abstand nehmen. Den Schülerinnen und Schülern bleiben solche als pädagogische Maßnahme betitelte öffentliche Demütigungen hoffentlich künftig erspart.

2.25 Elternvertreter: Finger weg von WhatsApp!

Elternvertreter dürfen für die Erfüllung ihrer Aufgabe WhatsApp nicht verwenden – weder für „private“ noch für schulische Zwecke. Wenn sie dennoch Nachrichten über diesen Dienst versenden, droht ihnen schlimmstenfalls ein Bußgeld – das ist aber abhängig davon, ob die versendete Nachricht schulorganisatorischen Inhalt hat. Elternvertreter sollten daher unbedingt über datenschutzgerechte Messengerdienste kommunizieren.

Wenn beim Elternabend gefragt wird, wer das Amt der Elternvertreter übernehmen möchte, erinnern sich viele an ihre eigene Schulzeit: Den Blick nach unten, geschäftig etwas auf ein Blatt notieren, sich möglichst unauffällig verhalten und am besten unsichtbar sein. Diejenigen, die sich mit mehr oder weniger großer Begeisterung dennoch in dieses Amt wählen lassen, erwartet nicht nur eine Reihe von Aufgaben, sondern zum Teil auch Ungemach. So wandte sich ein Elternteil an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und beschwerte sich darüber, dass der Elternvertreter der Klasse ihres Kindes einen WhatsApp-Verteiler verwendete, um den Eltern schulorganisatorische Informationen im Auftrag des Klassenleiters mitzuteilen.
Zur Verwendung von WhatsApp im schulischen Kontext hatte sich der TLfDI bereits in einem Rundschreiben an alle Thüringer Schulen klar positioniert, ebenso wie das Thüringer Ministerium für Bildung, Jugend und Sport, dass auf seiner Internetseite ein Verbot der Nutzung von WhatsApp für Lehrkräfte beim Austausch von personenbezogenen Daten veröffentlichte. WhatsApp greift für einen vollen Funktionsumfang nicht nur auf die gespeicherten Kontaktdaten Dritter auf dem Endgerät des Nutzers zu – ohne dass die erforderliche Einwilligung all dieser Kontaktpersonen vorliegt –, es überträgt auch diese personenbezogenen Daten auf Server außerhalb der EU, etwa in die

USA, die nicht den hohen datenschutzrechtlichen Standard der Datenschutz-Grundverordnung (DS-GVO) gewährleisten. Damit ist eine Übertragung in diese Länder in der Regel nicht datenschutzkonform möglich.
Auch der Messengerdienst WhatsApp selbst schreibt in seinen Nutzungsbedingungen: „Du wirst unsere Dienste nicht auf eine Art und Weise nutzen (beziehungsweise anderen bei der Nutzung helfen), die […] (f) irgendeine nicht-private Nutzung unserer Dienste beinhaltet, es sei denn, dies wurde von uns genehmigt.“ Die Antwort an die Beschwerdeführerin war also eindeutig: WhatsApp ist für die Nutzung von Elternvertretern in dieser Funktion nicht zulässig.
Die Beschwerdeführerin ließ es bei dieser Antwort des TLfDI nicht bewenden und fragte nach, ob gegen Elternvertreter, die WhatsApp verwendeten, ein Bußgeld verhängt werden könne und wenn ja, in welcher Höhe. Außerdem forderte sie den TLfDI auf, das Nutzungsverbot von WhatsApp in diesem Zusammenhang öffentlich zu machen.
Die Frage, ob ein Bußgeld gegen eine Elternvertretung verhängt werden kann, hängt davon ab, ob die Elternvertretung als „öffentliche Stelle“ tätig wird, gegen die grundsätzlich kein Bußgeld verhängt werden kann, oder ob die Elternvertretung die ihr in dieser Funktion zur Verfügung stehenden Daten zu eigenen Zwecken privat verarbeitet.
Im Thüringer Schulgesetz und der Thüringer Schulordnung ist die Rechtsstellung der aus der Wahl der Klassenelternschaft gebildeten Elternvertretung nicht geregelt. Art. 23 der Thüringer Verfassung ist jedoch zu entnehmen, dass die Eltern an der Wahrnehmung der staatlichen Schulaufsicht von innen teilhaben. In diesem Sinn können Elternvertretungen als eine andere „öffentliche Stelle“ und als innerhalb der staatlichen Organisation angesiedelter Teil der Schulorganisation angesehen werden – und gegen öffentliche Stellen kann grundsätzlich kein Bußgeld verhängt werden.
Als gewählte Mitglieder nehmen die Elternvertreter mithin eine Art öffentlich-rechtliches Amt in Form eines unbezahlten Ehrenamts wahr. Dabei käme für die einzelnen Elternvertreter die Verhängung eines Bußgelds nur dann in Frage, wenn personenbezogene Daten durch sie auf rechtswidrige Weise zu anderen Zwecken als der Elternvertretung verarbeitet würden. Jeweils fallbezogen wäre dann zu klären, ob bei dieser Verarbeitung entgegen den Regelungen der Datenschutz-Grundverordnung beziehungsweise des Thüringer Datenschutzgesetztes die personenbezogenen Daten (der Kinder und Eltern)

erhoben, gespeichert, verändert, übermittelt oder genutzt werden oder weitere Tatbestandsmerkmale des die Ordnungswidrigkeiten und Strafbestimmungen regelnden § 61 Thüringer Datenschutzgesetz vorliegen.
Nutzt ein Elternvertreter die ihm in dieser Funktion zur Verfügung stehenden personenbezogenen Daten unzulässiger Weise für eigene – also private – Zwecke, dann befindet er sich im sogenannten Exzess und wird dadurch selbst zum Verantwortlichen für die Datenverarbeitung gem. Art. 4 Nr. 7 DS-GVO. In diesem Fall käme die Verhängung eines Bußgeldes nach Art. 83 DS-GVO in Betracht.
Um sowohl die Elternvertretungen als auch die Schulleitungen auf die bestehende Problematik aufmerksam zu machen, hat der TLfDI die Thüringer Landeselternvertretung auf die Problematik der Nutzung von WhatsApp zur Kommunikation mit den Eltern aufmerksam gemacht und darum gebeten, die Elternvertretungen darüber zu informieren. Ebenfalls wurde den Schulen vorgeschlagen, die Elternvertreter schriftlich zur Einhaltung der datenschutzrechtlichen Vorschriften zu verpflichten. Außerdem wurde dem Thüringer Ministerium für Bildung, Jugend und Sport empfohlen, in der Thüringer Schulordnung weitere Regelungen zum Umgang mit personenbezogenen Daten für die Elternvertretung aufzunehmen. Insbesondere sollten die Schulen verpflichtet werden, die Elternvertretung über die Einhaltung der datenschutzrechtlichen Vorschriften aufzuklären.
Mit dieser umfangreichen Antwort waren alle Fragen der Beschwerdeführerin geklärt.
Ergänzender Hinweis: Problematisch bei WhatsApp ist insbesondere, dass dieser Messengerdienst automatisch auf alle in dem Smartphone des Nutzers gespeicherten Kontaktdaten zugreift, auch wenn diese selbst kein WhatsApp nutzen und einer Verwendung ihrer Daten durch WhatsApp nicht zugestimmt haben. Das Amtsgericht Bad Hersfeld hat in einem Urteil aus dem Jahr 2017 (Urteil vom 15. Mai 2017 – F 120/17 EASO) die Mutter eines 11-jährigen Jungen dazu verpflichtet, alle Kontakte, die auf dem Smartphone des Kindes gespeichert waren, über die Nutzung von WhatsApp und die damit verbundene Verarbeitung ihrer personenbezogenen Daten zu informieren und von diesen eine schriftliche Zustimmungserklärung einzuholen, wonach sich diese mit der Speicherung ihres Namens im Adressbuch des Smartphones des Sohnes sowie einer Datenweiterleitung an den Betreiber des Dienstes WhatsApp mit Sitz in Kalifornien/USA einverstanden erklären. In der Begründung des Urteils argumentierte der

Amtsrichter, dass derjenige, der durch die Nutzung von WhatsApp "diese andauernde Datenweitergabe zulässt, ohne zuvor von seinen Kontaktpersonen aus dem eigenen Telefon-Adressbuch hierfür jeweils eine Erlaubnis eingeholt zu haben, gegenüber diesen Personen eine **deliktische Handlung** begeht und sich in die Gefahr begibt, von den betroffenen Personen kostenpflichtig abgemahnt zu werden". Dieses Urteil und seine bundesweite mediale Wirkung hatten dazu geführt, dass diese gemäß DS-GVO unzulässige Praxis von WhatsApp einer breiten Öffentlichkeit bekannt wurde – und sich damit auch die Sensibilität gegenüber möglichen Verstößen erhöht hat.

2.26 Abfrage bei Präsenzveranstaltung an Hochschulen – was darf der Sicherheitsdienst?

Der 3G-Nachweis darf bei Präsenzveranstaltungen an Hochschulen stichprobenartig durch einen beauftragten Sicherheitsdienst geprüft werden. Rückschlüsse auf das Studienfach des Überprüften sind zwar nicht auszuschließen, aus datenschutzrechtlicher Sicht jedoch hinnehmbar.

An Hochschulen sind häufig deutlich mehr Menschen unterwegs als an Schulen – umso größer die Herausforderungen, einen sicheren Präsenzbetrieb unter Einhaltung der Corona-Regeln zu organisieren. Eine Thüringer Hochschule hatte für die Überprüfung der 3G-Regel (geimpft/genesen/getestet) einen Sicherheitsdienst beauftragt, der stichprobenartig vor den Seminar- und Vorlesungsräumen die entsprechenden Nachweise überprüfen sollte. Bei der Vorlage des Nachweises waren sowohl Lehrende als auch Studierende und Gäste aufgefordert, einen Identitätsnachweis vorzulegen.
Eine Lehrperson war mit diesem Vorgehen nicht einverstanden und wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), schließlich könne der Sicherheitsdienstleister vertrauliche Gesundheitsdaten einsehen und das noch in Verbindung mit einem Ausweisdokument und nicht etwa anonym. Außerdem könnten aufgrund der Positionierung vor den Eingängen einer bestimmten Lehrveranstaltung Rückschlüsse gezogen werden, welches Fach die überprüfte Person studiere.
Für die datenschutzrechtliche Zulässigkeit des Vorgehens der Hochschule galt es zunächst grundsätzlich zu prüfen, ob, und falls ja unter

welchen Voraussetzungen, Präsenzveranstaltungen überhaupt durchgeführt werden dürfen. Gemäß der zum Beschwerdezeitpunkt geltenden Fassung des § 22 Abs. 1 der Thüringer Verordnung zur Regelung infektionsschutzrechtlicher Maßnahmen zur Eindämmung des Coronavirus SARS-CoV-2 (Thüringer SARS-CoV-2-Infektionsschutz-Maßnahmenverordnung-ThürSARS-CoV-2-IfS-MaßnVO-)
war die Durchführung sowohl von Hochschulprüfungen in Präsenz als auch weiteren Präsenzveranstaltungen zulässig. Allerdings war die Teilnahme daran nur Studierenden, Lehrenden und Gästen gestattet, die ein negatives Testergebnis auf das Vorliegen einer Infektion mit dem Coronavirus SARS-CoV-2 (§ 2 Abs. 2 Nr. 8 ThürSARS-CoV-2-IfS-MaßnVO) vorweisen konnten. Ergänzend zur ThürSARS-CoV-2-IfS-MaßnVO galt gemäß § 2 Abs. 1 der Verordnung die Thüringer Verordnung über die Infektionsschutzregeln zur Eindämmung der Ausbreitung des Coronavirus SARS-CoV-2 in Kindertageseinrichtungen, der weiteren Jugendhilfe, Schulen und für den Sportbetrieb (ThürSARSCoV-2-KiJuSSp-VO). Danach war in der damals geltenden Fassung eine Testung mit negativem Ergebnis einem vollständigen Impfschutz gegen eine beziehungsweise einer Genesung von einer Infektion mit dem SARS-CoV-2 Virus gleichgestellt. Die entsprechenden Nachweise mussten gemäß § 3 Satz 2 ThürSARSCoV-2-KiJuSSp-VO von den genesenen Personen geführt werden.
Gesundheitsdaten fallen gemäß Art. 9 Abs. 1 Datenschutz-Grundverordnung (DS-GVO) unter die besonderen Kategorien personenbezogener Daten, deren Verarbeitung grundsätzlich unzulässig ist. Sie dürfen aber gemäß Art. 9 Abs. 2 Buchstabe g) DS-GVO auf der Grundlage des Rechts eines Mitgliedstaats, das in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht, aus Gründen eines erheblichen öffentlichen Interesses verarbeitet werden. Die beiden genannten Verordnungen (ThürSARS-CoV-2-IfS-MaßnVO und ThürSARSCoV-2-KiJuSSp-VO) beinhalteten die entsprechenden Rechtsgrundlagen. Die Abfrage des 3G-Status war daher aus datenschutzrechtlicher Sicht zulässig.
Die Kontrollen ohne zusätzliches Ausweisdokument hätten dabei nicht die Anforderungen der Rechtsvorschriften erfüllt, da nicht nachvollziehbar gewesen wäre, ob der vorgelegte 3G-Nachweis tatsächlich für die betroffene Person ausgestellt wurde.

Die Durchführung von Stichproben war auf die hohe Zahl der Studierenden zurückzuführen, die eine Kontrolle aller Personen durch hochschuleigenes Personal unmöglich machte. Dass die Stichproben durch einen Sicherheitsdienst erhoben wurden, hatte die Beschwerdeführerin ebenfalls kritisiert. Ein Sicherheitsdienst wird typischerweise als Auftragsverarbeiter im Sinne des Art. 4 Nr. 8 DS-GVO tätig und prüft beziehungsweise erhebt die 3G-Daten im Auftrag des Verantwortlichen (hier also der Hochschule). Zu diesem Zweck muss die Hochschule einen Auftragsverarbeitungsvertrag nach Art. 28 DS-GVO mit dem Sicherheitsdienst abgeschlossen haben. In diesem Vertrag sind der Gegenstand und die Dauer sowie Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte der Hochschule zu regeln. Der Sicherheitsdienst als Auftragsverarbeiter muss unter anderem gewährleisten, dass die zur Verarbeitung der personenbezogenen Daten befugten Personen (also die Personen, die die 3G-Nachweise kontrollieren) zur Vertraulichkeit verpflichtet wurden.
Bei der Art der personenbezogenen Daten, die vom Sicherheitsdienst erhoben wurden, war nicht anzunehmen, dass der jeweilige Studiengang des Kontrollierten umfasst war. Es lagen keine Anhaltspunkte dafür vor, dass der Studiengang als zu erhebendes Datum Teil des Auftragsverarbeitungsvertrags war. Ein milderes Mittel, die per Verordnung vorgeschriebenen 3G-Kontrollen an den Hochschulen durchzuführen, war nicht ersichtlich. Dass möglicherweise das Personal des Sicherheitsdienstes im Moment der Kontrolle spekulierte, ob jemand ein bestimmtes Fach studiert, war daher aus datenschutzrechtlicher Sicht hinnehmbar.

2.27 Einem Datenschutzverstoß kann nur bei einem Nachweis nachgegangen werden

Die Meldung eines Verstoßes gegen das Hygiene-Schutz-Konzept in einer Sparkassen-Filiale erfordert auch eine Meldung einer Verletzung des Schutzes personenbezogener Daten aufgrund der Weitergabe der Beschwerde an Dritte beim TLfDI.

Ein Bürger wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und trug vor, dass er Zeuge eines groben Verstoßes gegen das Hygiene-Schutz-Konzept in einer Sparkassen-Filiale geworden war und daraufhin zwei Kunden

und die dort arbeitende Reinigungskraft bei der zuständigen Ordnungsbehörde und bei der Sparkassen-Filiale angezeigt hatte. Der Bürger schilderte weiterhin, dass es einige Tage später aufgrund des Vorfalls zu Differenzen zwischen ihm und seinem Stiefkind gekommen sei. Zur weiteren Sachverhaltsaufklärung legte der Beschwerdeführer offen, dass die oben genannte Reinigungskraft die Ex-Schwiegermutter seiner Partnerin und somit Großmutter seines Stiefkindes sei.
Er habe vom Kindsvater seines Stiefkinds über WhatsApp eine Nachricht erhalten. Darin teilte der Kindsvater mit, der Inhalt der Beschwerde sei der Reinigungskraft ausgedruckt und ihr mitgegeben worden. Als Beweis sei ein Foto des Textes der Beschwerde beigefügt gewesen. Die eigentliche Beschwerde des Bürgers bestand also darin, dass seine vorgetragene Beschwerde bei der Sparkasse über den beobachteten Verstoß gegen das Hygiene-Schutz-Konzept an die Reinigungskraft weitergegeben wurde.
Der TLfDI wandte sich mit einem Auskunftsersuchen nach Art. 58 Abs. 1 Buchstabe a) Datenschutz-Grundverordnung an die Sparkassen-Filiale und bat diese um eine Stellungnahme zu dem streitgegenständlichen Sachverhalt.
Der Datenschutzbeauftragte der Sparkassen-Filiale teilte dem TLfDI mit, dass der Bürger die Sparkasse über eine zentrale E-Mail-Adresse über den von ihm beobachteten Verstoß gegen das Infektionsschutzgesetz unterrichtet habe. Am nächstfolgenden Arbeitstag sei die Nachricht dem Leiter des Corona-Krisenstabes zur weiteren Prüfung weitergeleitet worden. Auf das zentrale Postfach der Sparkasse habe nur ein sehr eingeschränkter Mitarbeiterkreis Zugriff. Auch sei der Screenshot des Smartphones vom Beschwerdeführer als Beweis nachgereicht worden. Dieser Screenshot habe allein den Text der Beschwerde enthalten, nicht aber Kopf- und Fußzeile der eingegangenen E-Mail. Deswegen sei kein klarer Rückschluss möglich, dass das Schreiben in der Sparkassen-Filiale ausgedruckt wurde. Dem Mailpostfach der Sparkasse seien auch keine Hinweise auf eine Weiterleitung auf elektronischem Weg zu entnehmen gewesen. Damit sei fraglich, welches Dokument auf welche Weise an die Reinigungskraft gelangt war. Alle mit dem Vorgang befassten Mitarbeiter seien hinsichtlich des Sachverhalts befragt worden. Dabei konnten keine Hinweise bezüglich der Weitergabe der E-Mail an die Reinigungskraft gefunden werden.

Da keine weiteren Anhaltspunkte oder Hinweise vorlagen, dass ein Mitarbeiter der Sparkasse die Beschwerde an die Reinigungskraft weitergegeben hatte, konnte kein datenschutzrechtlicher Verstoß nachgewiesen werden. Diese konnten auch durch den Beschwerdeführer nicht beigebracht werden. Aus den genannten Gründen konnte der TLfDI die Angelegenheit leider nicht weiter aufklären, was dem Beschwerdeführer mitgeteilt wurde, der die Entscheidung akzeptierte.

2.28 Anzeige eines Datenschutzverstoßes führt nicht immer zum Betriebsfrieden

Eine Beschwerde bei der Aufsichtsbehörde nach Art. 77 DS-GVO kann nur die Person einlegen, um deren personenbezogene Daten es in dem jeweiligen Fall geht. Gleichwohl prüft der TLfDI angezeigtes Verhalten und berät bei Datenschutzverstößen.

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit erreichte die „Datenschutzbeschwerde“ einer Stadtverwaltung, die das Verhalten mehrerer ihrer Beschäftigten betraf. Diese hätten Details über Vertragsbestandteile sowie über Streitigkeiten innerhalb eines Arbeitsteams an Stadtratsmitglieder bekanntgegeben, was gegen den Datenschutz verstieße. Da nicht alle notwendigen Sachverhaltsinformationen vorlagen, wurde die Stadtverwaltung zunächst um Präzisierung ihrer Angaben gebeten und auf Folgendes hingewiesen:
Datenschutzrechtliche Bestimmungen haben den Schutz der personenbezogenen Daten der betroffenen Personen zum Gegenstand. „Betroffene Person“ ist dabei diejenige Person, deren personenbezogene Daten verarbeitet werden (Definition in Art. 4 Nr. 1 Datenschutz-Grundverordnung [DS-GVO]). Daneben ist immer zu fragen, wer die Daten verarbeitet, mithin „Verantwortlicher“ für die Datenverarbeitung ist. „Verantwortlicher“ ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet (Definition in Art. 4 Nr. 7 DS-GVO). Handeln Beschäftigte für die Behörde als Verantwortliche, wäre der Versand als Übermittlung personenbezogener Daten der verantwortlichen Stelle zuzuordnen. Tun sie dies in eigener Verantwortung und in eigenen Angelegenheiten, können sie selbst Verantwortli-

cher sein. Dies war zu prüfen. Ebenso war zu prüfen, ob die Stadtratsmitglieder als Empfänger der personenbezogenen Daten (Art. 4 Nr. 9 DS-GVO). als „Dritte“ (Art. 4 Nr. 10 DS-GVO) anzusehen waren. Hier lag die Besonderheit darin, dass die betroffenen Beschäftigten zum einen selbst ihre Daten offenlegten, weswegen eine Verletzung von datenschutzrechtlichen Bestimmungen fraglich erschien. Nach den vorliegenden Informationen hatten die Beschäftigten allerdings zum anderen auch personenbezogene Daten und Verhaltensweisen zweier weiterer Personen übermittelt.
Die Stadtverwaltung teilte erläuternd zum Sachverhalt mit, die Beschäftigten einer städtischen Einrichtung hätten sich an einen Stadtrat gewandt, um ihm die Missstände zum Personaleinsatz und zum Umgang mit dem Personal zur Kenntnis zu bringen, wobei sie die Leitung der Einrichtung namentlich benannten und deren Verhalten ihnen gegenüber beschrieben. Weiterhin beschrieben sie eine aus ihrer Sicht ungerechte Bevorzugung eines anderen Beschäftigten hinsichtlich des Einsatzes zu nur „angenehmen“ Dienstzeiten und legten zum Nachweis den Dienstplan bei, aus dem dies ersichtlich sei. Offenbar sahen sich die Beschäftigten veranlasst, sich wegen der Missstände an einen Stadtrat zu wenden, da sie innerhalb der Verwaltung keine Ansprechpartner oder Gehör fanden.
Die Übermittlung der personenbezogenen Daten der Leitung und des weiteren Beschäftigten sowie die Daten aus dem Dienstplan (Einsatzzeiten) bewertete die Stadtverwaltung beziehungsweise das Personalamt als Datenschutzverstoß. Die Stadtverwaltung ist jedoch mangels Beschwer nicht nach Art. 77 DS-GVO beschwerdeberechtigt. Daher wurde die Anzeige der Stadtverwaltung als Hinweis auf eine Datenschutzverletzung beziehungsweise als Beratungsgesuch bewertet, zumal die Stadtverwaltung sich bereits in einem arbeitsrechtlichen Verfahren mit den Beschäftigten befand.
Fest steht, dass es sich bei den Angaben im Dienstplan um Beschäftigtendaten handelt, die der Arbeitgeber/der Dienstherr ohne Rechtsgrundlage nicht Dritten zur Kenntnis geben darf. Für den Dienstherrn gilt die Rechtsgrundlage des § 27 Thüringer Datenschutzgesetz in Verbindung mit den dienstrechtlichen Vorschriften §§ 79 bis 87 des Thüringer Beamtengesetzes. Diese Rechtsgrundlage gilt jedoch nicht für die einzelnen Beschäftigten, die nicht mit den Aufgaben der Personalverwaltung und -bewirtschaftung beauftragt sind. Die Verarbeitung der Daten aus dem Dienstplan durch einzelne Beschäftigte erfolgte in Wahrnehmung der ihnen außerhalb der Personalverwaltung

obliegenden Aufgaben, nämlich um ihre eigenen Einsatzzeiten entnehmen zu können.
Die geschilderte Verhaltensweise der Leitung der Einrichtung gegenüber den betroffenen Beschäftigten war datenschutzrechtlich nicht bewertbar. Was Dritten über einen Dienstvorgesetzten geäußert werden kann und darf, ist dienstrechtlich zu bewerten.
Als Rechtsgrundlage für die Übermittlung des Dienstplans an einen dort nicht beschäftigten Stadtrat waren die allgemeinen Zulässigkeitsvoraussetzungen der Art. 5 und 6 DS-GVO zu prüfen. Der Dienstplan steht den Beschäftigten zur Verfügung, um ihre Beschäftigungszeiten zu entnehmen. Dass dieser nicht unbefugten Dritten zur Kenntnis gelangen darf, ist zunächst von der Dienststelle als Verantwortlicher für die Einhaltung der datenschutzrechtlichen Vorschriften gegenüber den Mitarbeitern sicherzustellen. Daher darf ein Dienstplan zum Beispiel auch nicht zur Kenntnis von Dritten/Besuchern ausgehangen werden.
Vorliegend wurde der Plan zum Beleg einer ungerechten oder ungleichen Behandlung dem Stadtratsmitglied, das in dieser Funktion keine personalverwaltenden Aufgaben wahrzunehmen befugt ist, übermittelt, was eine zweckwidrige Verwendung darstellt, die einen Verstoß nach Art 5 Abs. 1 Buchstabe b) DS-GVO darstellen kann. Dies wurde der Stadtverwaltung mitgeteilt. Ob und welche arbeitsrechtlichen Konsequenzen daraus abgeleitet wurden, ist nicht bekannt.
Beschwerden der von der Übermittlung an das Stadtratsmitglied betroffenen Personen und damit der Beschwerdeberechtigten im Sinne des Art. 77 DS-GVO waren beim TLfDI nicht eingegangen.

2.29 Wo der Datenschutz endet: Zulässigkeit eines digitalen Suchsystems für Grabstätten

Die Einrichtung eines digitalen Suchsystems für Grabstätten und die Bereitstellung von personenbezogenen Daten von Verstorbenen sind grundsätzlich datenschutzrechtlich zulässig. Es besteht kein grundsätzliches postumes Recht an den eigenen Daten nach der DS-GVO.

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) ging der Frage nach, ob die Erstellung eines digitalen Grabstätten-Auskunftssystems mit den datenschutzrechtlichen Bestimmungen vereinbar ist. Es war geplant, bundesweit eine

Internet-Plattform einzuführen, die es interessierten Friedhofsverwaltungen ermöglichen sollte, ihren Friedhofslageplan digital in einheitlicher Form zur Einsicht zur Verfügung zu stellen. Eine Suchmaschine mit Auswahlkriterien wie Name, Stadt, Friedhof, Jahr der Bestattung sollte es Nutzern ermöglichen, das Grab einer gesuchten Person ausfindig zu machen.
Da es sich um ein bundesweites Auskunftssystem handeln sollte, wären auch Verstorbene anderer Bundesländer betroffen gewesen. Darum arbeitete der TLfDI in dieser Sache mit dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zusammen.
Grundsätzlich werden durch eine Auskunftsdatei personenbezogene Daten nach Art. 2 Abs. 1 Datenschutz-Grundverordnung (DS-GVO) ganz oder teilweise automatisch verarbeitet und in einem Dateisystem gespeichert. Deshalb sind die Bestimmungen der Art. 5 Abs. 1 und Art: 6 Abs. 1 DS-GVO zur rechtmäßigen Datenverarbeitung anzuwenden.
Allerdings sind mit personenbezogenen Daten gemäß Art. 4 Nr. 1 DS-GVO Informationen gemeint, die sich auf natürliche, also lebende, Personen beziehen. Erwägungsgrund 27 zur DS-GVO schließt die Anwendung der Datenschutz-Grundverordnung auf Daten Verstorbener ausdrücklich aus. Die Mitgliedstaaten könnten demnach Vorschriften für die Verarbeitung der personenbezogenen Daten Verstorbener erlassen, wobei Deutschland bisher hiervon keinen Gebrauch gemacht hat. Somit findet die DS-GVO auf ein Auskunftssystem für Grabstätten keine Anwendung.
Unabhängig von dem Anwendungsbereich der DS-GVO könnte vorliegend allerdings das aus Art. 1 Abs. 1 Grundgesetz abgeleitete postmortale Persönlichkeitsrecht der Verstobenen zu Einschränkungen führen. Dieses Recht umfasst den Schutz des sittlichen, personalen und sozialen Geltungswertes, welcher von der Person über ihren Lebenszeitraum erlangt wurde, und schützt das Lebensbild des Verstorbenen gegen schwerwiegende Entstellungen. Allein die Angabe des Standorts des Grabes führt regelmäßig zu keiner Beeinträchtigung des Lebensbildes, selbst wenn die Ruhestätte im Internet einer breiten Öffentlichkeit zugänglich gemacht wird.
Insoweit ist es auch nicht erforderlich, dass der Nutzer der Plattform neben dem Namen des Verstorbenen weitere Angaben zum Jahr oder Ort der Bestattung machen muss, bevor ihm der Standort übermittelt werden darf. Das Auskunftssystem dürfte bedingungslos für alle Interessierten digital zugänglich sein, also für einen Personenkreis über

enge Verwandte der Verstorbenen hinaus. Gleichzeitig ist es zulässig, wenn die Plattform selbst das Jahr der Bestattung als Teil des Suchergebnisses angeben würde. Weiterhin ist hinsichtlich der Aufnahme von besonders alten Gräbern in das System zu beachten, dass der Schutz des postmortalen Persönlichkeitsrechtes gegenüber anderen Grundrechtspositionen mit zunehmendem zeitlichen Abstand zu dem Todesdatum an Geltung verliert.
Die Persönlichkeitsrechte der Angehörigen dürfen der Veröffentlichung des Standorts der Grabstätte ebenfalls in aller Regel nicht entgegenstehen. Das allgemeine Persönlichkeitsrecht schützt auch die freie Entscheidung über die Preisgabe und Verwendung persönlicher Daten. Dieser Schutz dürfte jedoch regelmäßig durch die Veröffentlichung nicht verletzt werden. Allenfalls könnten Betroffene Rechte aus der DS-GVO geltend machen, wenn Angehörige durch die Angabe des Standorts im Sinne des Art. 4 Nr. 1 DS-GVO identifizierbar gemacht werden. In diesen Einzelfällen ist jedoch von einer rechtmäßigen Datenverarbeitung nach Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO auszugehen. Schutzwürdige Interessen von Angehörigen wären nur in einem sehr begrenzten Umfang betroffen, sodass das berechtigte Interesse des Verantwortlichen überwiegt.
Allgemein ist aber immer der Grundsatz der Datenminimierung gemäß Art. 5 Abs. 1 Buchstabe c) DS-GVO zu beachten, sodass lediglich zwingend notwendige Daten veröffentlicht werden sollten.
Der Anbieter einer solchen Plattform hat damit grundsätzlich die Möglichkeit, die Standorte von Grabstätten öffentlich zu machen. Er muss jedoch kritisch hinterfragen, welche Daten der Verstorbenen dabei veröffentlicht werden sollen.

2.30 Was darf der Fragebogen zum Kauf von Wohnungseigentum erheben?

Die Thüringer Gutachterausschüsse für Grundstückswerte sind nach den §§ 193 Abs. 3 und 195 Abs. 1 BauGB gesetzlich dazu verpflichtet, Kaufverträge über Grundstücke zu erfassen, auszuwerten und darauf basierend eine Kaufpreissammlung zu führen. Nach § 197 Abs. 1 BauGB können die dafür benötigten Auskünfte von Grundstückseigentümern beziehungsweise -erwerbern eingeholt werden, etwa mithilfe eines teilmarktspezifischen Fragebogens, der auch personenbezogene Daten erfasst. Auch die Frage nach zwischen dem Käufer und

Verkäufer bestehenden persönlichen Verbindungen, die Einfluss auf den Kaufpreis hatten, ist dabei zulässig.

Im Berichtszeitraum wandte sich ein Bürger an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und teilte mit, dass er nach einem Grundstückserwerb durch das Thüringer Landesamt für Bodenmanagement und Geoinformation (TLBG) kontaktiert und um Beantwortung diverser Fragen im Zusammenhang mit seinem Erwerb von Wohnungseigentum aufgefordert worden sei. Der Bürger bat den TLfDI im Hinblick darauf um Prüfung, inwiefern er zur Auskunft gegenüber dem TLBG verpflichtet ist und den vollständig ausgefüllten Fragebogen zurücksenden müsse. Insbesondere äußerte der Bürger Unverständnis darüber, dass in dem Fragebogen auch nach persönlichen Verbindungen zum Verkäufer gefragt wurde, die den Kaufpreis beeinflusst haben. Für den Bürger war nicht nachvollziehbar, dass im Zusammenhang mit dem Kauf von Wohnungseigentum derartige Daten abgefragt werden, sodass er sich darüber entsprechend beim TLfDI beschwerte.
Für die datenschutzrechtliche Prüfung des Sachverhalts ließ sich der TLfDI zunächst den betreffenden Fragebogen vom Bürger übermitteln. Dabei wurde festgestellt, dass der Bürger von einem der neun Thüringer Gutachterausschüsse für Grundstückswerte, die jeweils für mehrere Landkreise zuständig und beim TLBG angesiedelt sind, ein als „Fragebogen über den Kauf von Wohnungseigentum“ bezeichnetes Formular erhalten hatte. Dieser Fragebogen sollte durch den Bürger ausgefüllt zurückgesandt werden. Enthalten war auch die vom beschwerdeführenden Bürger kritisierte Frage „Bestanden persönliche Verbindungen zum Verkäufer, die Einfluss auf den Kaufpreis hatten?“.
Nachdem sich der TLfDI im Rahmen der datenschutzrechtlichen Prüfung des Sachverhalts mit dem TLBG in Verbindung gesetzt hatte, konnte dem Bürger im Ergebnis Folgendes mitgeteilt werden:
Gutachterausschüsse sollen als unabhängige Kollegialgremien von Sachverständigen für Transparenz auf dem Grundstücksmarkt sorgen. Die Einrichtung der Gutachterausschüsse und die Beschreibung ihrer Aufgaben sind im Baugesetzbuch (BauGB) bundeseinheitlich geregelt. Ergänzende und konkretisierende Regelungen finden sich für Thüringen in der Thüringer Gutachterausschussverordnung (ThürGAVO).

Zu den Aufgaben eines Gutachterausschusses gehört gemäß § 193 Abs. 5 BauGB unter anderem die Führung und Auswertung einer Kaufpreissammlung. Grundlage für diese Kaufpreissammlung sind Abschriften entgeltlicher Übereignungsverträge, die von beurkundenden Stellen (vor allem Notare) gemäß § 195 Abs. 1 Satz 1 BauGB an den Gutachterausschuss zu übersenden sind. Da die den Gutachterausschüssen übersandten Kaufverträge im Regelfall aber nur sehr wenige Informationen zur Kaufpreisbildung enthalten, werden regelmäßig Nachfragen zu kaufpreisbildenden Merkmalen erforderlich, damit die Gutachterausschüsse ihre gesetzliche Aufgabe (Führung der Kaufpreissammlung) erfüllen können.
Der Gutachterausschuss nimmt eine öffentliche Aufgabe wahr, übt eine hoheitliche Tätigkeit aus und ist damit eine Behörde (Schrödter [Hrsg.]: Baugesetzbuch, 9. Auflage 2019, Nomos-Kommentar, § 192 Rn. 6). Als Behörde hat der Gutachterausschuss die Verpflichtung, den Sachverhalt von Amts wegen zu erforschen, wobei der Wahrnehmung dieser Aufgabe insbesondere die in § 197 BauGB genannten Rechte dienen (Schrödter, a.a.O.; § 197 Rn. 1). Zur Beschaffung der erforderlichen Daten stehen dem Gutachterausschuss zunächst sämtliche informellen Instrumente, wie zum Beispiel freiwillige Auskünfte zur Verfügung. Sofern die notwendigen Angaben und Auskünfte nicht auf diesem Wege zu erlangen sind, besteht gemäß § 197 Abs. 1 Satz 1 BauGB die Möglichkeit, mündliche oder schriftliche Auskünfte von Sachverständigen und Personen, die Angaben über das Grundstück machen können, auch gegen deren Willen einzuholen. Darüber hinaus hat der Gutachterausschuss gemäß § 197 Abs. 1 Satz 2 BauGB die Möglichkeit, die Vorlage von Unterlagen durch den Eigentümer oder sonstigen Rechtsinhaber zu verlangen, wenn die Unterlagen zur Führung der Kaufpreissammlung oder für die Begutachtung eines Grundstücks erforderlich sind (Federwisch in: BeckOK BauGB, hrsg. v. Spannowsky/Uechtritz, 53. Ed., Stand: 01.08.2021, zu § 197).
Aus den gesetzlichen Aufgaben und Befugnissen der Gutachterausschüsse ergibt sich damit, dass diese berechtigt sind, personenbezogene Daten – etwa mit Hilfe eines teilmarktspezifischen Fragebogens – zu verarbeiten. Denn nach Maßgabe des Art. 6 Abs. 1 Datenschutz-Grundverordnung (DS-GVO) ist eine Datenverarbeitung im Sinne des Art. 4 Nr. 2 DS-GVO unter anderem dann rechtmäßig, wenn die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, der der Verantwortliche unterliegt (Art. 6 Abs. 1 Satz 1 Buchstabe c) DS-GVO), oder die Verarbeitung für die Wahrnehmung einer

Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde (Art. 6 Abs. 1 Buchstabe e) DS-GVO). Art. 6 Abs. 1 Satz 1 Buchstabe c) und e) DS-GVO setzen eine konkrete Rechtsgrundlage im Unionsrecht oder im mitgliedstaatlichen Recht voraus.
Da Gutachterausschüsse nach den §§ 193 Abs. 3 und 195 Abs. 1 BauGB gesetzlich dazu verpflichtet sind, Kaufverträge zu erfassen, auszuwerten und darauf basierend eine Kaupreissammlung zu führen, wobei nach § 197 Abs. 1 BauGB die dafür benötigten Auskünfte von Grundstückseigentümern beziehungsweise -erwerbern eingeholt werden können, stellen diese Vorschriften die erforderliche Rechtsgrundlage dar. Eine Datenverarbeitung durch Thüringer Gutachterausschüsse im Rahmen der Führung einer Kaufpreissammlung ist somit auf Grundlage von Art. 6 Abs. 1 Satz 1 Buchstabe c) und e) in Verbindung mit den §§ 193 Abs. 3, 195 Abs. 1 und 197 Abs. 1 BauGB sowie § 9 Nr. 1 ThürGAVO als zulässig zu bewerten.
Im zugrundeliegenden Sachverhalt war der betreffende Gutachterausschuss somit befugt, sich mit dem „Fragebogen über den Kauf von Wohnungseigentum“ an den Beschwerdeführer zu wenden und darüber – im Falle einer Beantwortung durch diesen – Daten zu seinem Grundstückserwerb unter Beachtung der datenschutzrechtlichen Vorgaben aus § 12 Abs. 3 und § 16 ThürGAVO zu verarbeiten. Im Ergebnis konnte der TLfDI deshalb in Bezug auf den zur Prüfung vorgelegten Fragebogen eines Thüringer Gutachterausschusses für Grundstückswerte keinen Verstoß gegen datenschutzrechtliche Bestimmungen feststellen. Dies gilt auch im Hinblick auf die vom beschwerdeführenden Bürger monierte Frage nach persönlichen Verbindungen des Käufers zum Verkäufer, die Einfluss auf den Kaufpreis hatten. Denn diese Frage diente nach Angaben des TLBG zur Prüfung, ob der Kaufpreis dem gewöhnlichen Geschäftsverkehr (Verkehrswert) zugeordnet werden kann und er damit für weitere Auswertungen geeignet ist.
In der gegebenen Form entspricht die Datenverarbeitung mittels des Fragebogens über den Kauf von Wohnungseigentum auch dem verfassungsrechtlich gewährleisteten Grundsatz der Verhältnismäßigkeit, der verlangt, dass jede Maßnahme, die in Grundrechte eingreift, einen legitimen Zweck verfolgt und überdies geeignet, erforderlich und verhältnismäßig im engeren Sinn (angemessen) sein muss. Denn für die

Erreichung des angestrebten Ziels (Erfüllung der gesetzlichen Aufgaben der Gutachterausschüsse) ist der derzeitige Umfang der Datenverarbeitung mit dem betreffenden Fragebogen aus Sicht des TLfDI als geeignet, erforderlich und angemessen (der Grundrechtseingriff steht nicht außer Verhältnis zum verfolgten Zweck) anzusehen. Sofern allerdings zukünftig weitere personenbezogene Daten von den Gutachterausschüssen im Rahmen der Datenverarbeitung mittels des Fragebogens über den Kauf von Wohnungseigentum zur Aufgabenerfüllung für erforderlich gehalten werden, müsste nach Auffassung des TLfDI in jedem Fall überprüft werden, ob der sich aus dem im Grundgesetz verankerten Rechtsstaatsprinzip herleitende Verhältnismäßigkeitsgrundsatz dann noch gewahrt ist.

3. Fälle nicht-öffentlicher Bereich



© Praxis und Familie – Fotolia.

3.1 Steckbriefe der Ungeimpften im Unternehmen im Internet

Die Verarbeitung von Beschäftigtendaten und auch Gesundheitsdaten auf Wunsch von Beschäftigten ist auf der Grundlage deren Einwilligung grundsätzlich möglich (Art. 6 Abs. 1 Satz 1 Buchstabe a) DS-GVO, § 26 Abs. 2 und 3 BDSG in Verbindung mit Art. 9 DS-GVO). Allerdings ist die Einwilligung an konkrete Voraussetzungen und Formen gebunden. Stellt der TLfDI einen Verstoß gegen datenschutzrechtliche Vorschriften fest, hat er angemessene und verhältnismäßige Maßnahmen nach Art. 58 Abs. 2 DS-GVO zu treffen.

Die umzusetzenden und zu treffenden Maßnahmen im Rahmen der Bekämpfung der Corona-Pandemie hat auch Arbeitgeber als Verantwortliche im Sinne des Art. 4 Nr. 7 Datenschutz-Grundverordnung (DS-GVO) vor Herausforderungen gestellt. Neben sich schnell ändernden Rechtsvorschriften galt es, die Hygienemaßnahmen zum Schutz der Beschäftigten vor Ort umzusetzen und den Betrieb aufrecht zu erhalten. Der Thüringer Landesbeauftragte für den Datenschutz

und die Informationsfreiheit (TLfDI) hat in diesem Zusammenhang eine Fülle von Anfragen, Beratungs- und Unterstützungsersuchen, aber auch eine immense Anzahl von Fragen und Beschwerden von Betroffenen erhalten und bestmöglich beantwortet.
Folgender Fall hat im Berichtszeitraum großes Medieninteresse nach sich gezogen:
Im Oktober 2021 erreichte den TLfDI der Hinweis, in einem Unternehmen seien „Steckbriefe“ ausgehängt worden, auf denen die Mitarbeiter, die ungeimpft seien, mit Bild und Namen den anderen Mitarbeitern bekannt gemacht würden. Auf den zur Verfügung gestellten Aufnahmen von unter anderem in einem Pausenraum aufgehängten Papieren waren Fotos und Namen der Arbeitnehmer sowie der mit roter Farbe unterlegte Hinweis, dass bei diesen Mitarbeitern bisher kein vollständiger Impfschutz bestehe, zu erkennen.
Der TLfDI nahm dies zum Anlass, umgehend eine unangekündigte Prüfung vor Ort durchzuführen. Derartige Unterfangen waren für den TLfDI ebenfalls mit einigem Aufwand verbunden, denn auch der TLfDI musste Maßnahmen zum Schutz der Gesundheit seiner Beschäftigten treffen und gleichzeitig alle Eventualitäten vor Ort abschätzen, um auch die dort getroffenen Maßnahmen einhalten zu können. Bei einer unangekündigten Kontrolle muss man sich als Aufsichtsbehörde auch darauf vorbereiten, dass Verantwortliche nicht bereit sein könnten, freiwillig Zutritt zu Geschäftsräumen zu gewähren, sodass man sich auf der Grundlage einer Duldungsanordnung gegebenenfalls Zutritt mit Hilfe der Polizei verschaffen müsste, um der Gefahr einer Veränderung vor Ort und damit einer Vereitelung einer Kontrolle der tatsächlichen Gegebenheiten zu begegnen. Andererseits hat eine unangekündigte und damit überraschende Kontrolle auch für den Verantwortlichen den Vorteil, dass keine Manipulationen oder die Vorspiegelung einer rechtmäßigen Verarbeitung unterstellt werden können.
Vor Ort zeigte sich der Verantwortliche über das überraschende Eintreffen der Datenschutzaufsichtsbehörde zwar nicht erfreut, ermöglichte aber anstandslos und kooperativ die Durchführung der Kontrolle, die zum Ziel hatte, die Rechtmäßigkeit der Veröffentlichung von personenbezogenen Daten Beschäftigter in Form mehrerer Aushänge unter Hinweis auf den Impfstatus als gegen das Coronavirus nicht immunisierte Arbeitnehmer zu überprüfen.
Vor Ort wurden die streitigen „Steckbriefe“ in Augenschein genommen. Der Geschäftsführer der Verantwortlichen schilderte, man habe

sich dazu aus verschiedenen Gründen entschlossen. Die Arbeitsstätte sei geprägt durch eine hohe Hitzeentwicklung. Darüber hinaus herrsche eine hohe Geräuschbelastung, die eine Verständigung der Beschäftigten untereinander erschwere oder unmöglich mache. Der Mindestabstand sei unter Einhaltung des mit dem Gesundheitsamt abgestimmten Hygienekonzepts daher nicht immer möglich. Daher hätten sich die Mitarbeiter an die Geschäftsleitung gewandt mit der Bitte, auf das Tragen einer Mund-Nasen-Bedeckung während der Arbeitszeit auch im Hinblick auf mögliche Lockerungen für geimpfte und genesene Personen nach der zum damaligen Zeitpunkt zu erwartenden geänderten Corona-Verordnung ab Oktober 2021 zu verzichten. Die Geschäftsleitung nahm Vorschläge aus der Belegschaft zur Abschaffung beziehungsweise Einschränkung der internen Maskenpflicht entgegen und hielt die Variante des Aushangs, nach der nicht immunisierte Personen für die vollständig geimpften oder genesenen Personen erkennbar sein sollten, um den notwendigen Abstand einhalten zu können, für umsetzbar. Die Aushänge habe man mit Bildern der Mitarbeiter versehen, weil diese sich untereinander teilweise nicht alle persönlich und dem Namen nach kannten und es auf diese Art für die Mitarbeiter einfacher war, die erforderlichen Hygienemaßnahmen umzusetzen.
In Einzelgesprächen mit den Beschäftigten, die sich als nicht geimpft oder genesen meldeten, sei weder nach dem Impfstatus gefragt noch eine Überprüfung der Angaben durchgeführt worden. Die betroffenen Mitarbeiter hatten sich durch Unterschrift mit der Nennung ihres Namens und der Verwendung eines Bildes mit dem beabsichtigten Aushang auf einer erstellten Liste jeweils einverstanden erklärt.
Auf dem Aushang im Pausenraum waren alle nicht immunisierten Mitarbeiter verzeichnet und auf den Aushängen in den Abteilungen nur die dort tätigen Mitarbeiter. Weiterhin habe man darauf geachtet, dass der Aushang nicht allzu exponiert angebracht werde, ihn aber alle jeweils dort befindlichen Personen wahrnehmen könnten, damit bei Betreten des entsprechenden Bereichs durch eine abgebildete Person die entsprechenden Maßnahmen getroffen werden könnten.
Während des Vor-Ort-Termins wurde die Geschäftsleitung darauf hingewiesen, dass die dargelegte Vorgehensweise zur Verarbeitung von Beschäftigtendaten und auch Gesundheitsdaten auf Einwilligungsbasis grundsätzlich möglich sei (Art. 6 Abs. 1 Satz 1 Buchstabe a) DS-GVO, § 26 Abs. 2 und 3 Bundesdatenschutzgesetz [BDSG] in Verbindung mit Art. 9 DS-GVO). Allerdings ist die Einwilligung an konkrete Voraussetzungen und Formen gebunden. Die

Unterschrift auf der Liste allein genügt den Anforderungen nicht. Insbesondere sei die Freiwilligkeit im Beschäftigungsverhältnis aufgrund des Unter-/Überordnungsverhältnisses in der Regel fragwürdig. Nach der Schilderung des Ablaufs zur Unterschrift zur Erteilung einer Einwilligung zum internen Aushang auf der Liste konnte die Freiwilligkeit der Einwilligung der Beschäftigten auf der Basis eines gleichgelagerten Interesses von Arbeitgeber und Beschäftigten allerdings vorliegen (§ 26 Abs. 2 Satz 2 BDSG).
Überzeugend vorgetragen war das beiderseitige Anliegen, die Maskenpflicht im Betrieb so weit wie möglich einzuschränken, um die Arbeitsbelastung für die Beschäftigten zu erleichtern. Darüber hinaus wurde von den Mitarbeitern des TLfDI darauf hingewiesen, dass mit der Einholung der Einwilligung auf der Liste beziehungsweise mit der Unterschriftsleistung die Gesundheitsdaten der jeweils anderen Beschäftigten zur Kenntnis gelangen (können), wofür es keine Rechtsgrundlage gebe.
Insoweit wurde von den Mitarbeitern des TLfDI deutlich gemacht, dass hinsichtlich der Form der Einwilligungserklärungen Nachbesserungsbedarf bestehe. Die Einwilligungserklärungen sollten daher in der vorgeschriebenen Form (schriftlich, unter Darlegung des konkreten Zwecks der Verarbeitung der Gesundheitsdaten, unter Hinweis auf die Freiwilligkeit der Erklärung und der Widerrufsmöglichkeit) nochmals einzeln eingeholt werden. Dabei muss auch dem Transparenzgebot gegenüber den betroffenen Personen Rechnung getragen werden (Art. 13 DS-GVO). Dem wollte die Geschäftsleitung umgehend nachkommen, weil den Beschäftigten, die zum größten Teil bereits vollständig geimpft oder genesen waren, nicht zugemutet werden sollte, ab sofort wieder ausnahmslos Masken zu tragen.
Weitergehende Maßnahmen nach Art. 58 Abs. 2 DS-GVO, hier insbesondere Buchstabe f), zur Entfernung des Aushangs wurden vor Ort nicht angeordnet. Diese der Datenschutzaufsicht zur Verfügung stehende Maßnahme erlaubt die Anweisung einer vorübergehenden oder endgültigen Beschränkung bis hin zu einem Verbot einer Verarbeitung. Dabei ist die Schwere des Verstoßes und die damit verbundene Beeinträchtigung der Betroffenenrechte abzuwägen mit den Folgen für die verarbeitende Stelle. Sind mildere Mittel voraussichtlich zur Zielerreichung ausreichend, so sind diese vorzuziehen (Verhältnismäßigkeit und Angemessenheit der Mittel). Da es unter Berücksichtigung der Umstände vor Ort wahrscheinlich war, dass die Beschäftig-

ten auch mit einer formgerechten Einwilligungserklärung dem Aushang in der beschriebenen Form zustimmen würden, wurde das in diesem Zusammenhang mildere Mittel nach Art. 58 Abs. 2 Buchstabe d) DS-GVO vorbehalten, nach dem der Verantwortliche angewiesen werden kann, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit der DS-GVO zu bringen. Auch bei dieser Maßnahme ist das Verhältnismäßigkeitsprinzip zu beachten, das heißt, die Maßnahme muss zur Beendigung des rechtswidrigen Zustands geeignet, erforderlich und angemessen sein. Da der Verantwortliche ohne Vorbehalte zugesagt hatte, formell entsprechende Einwilligungen unverzüglich einzuholen, war eine solche Maßnahme vor Ort nicht als angemessen auszusprechen und konnte im Nachhinein unter Fristsetzung zur Vorlage beim TLfDI vorbehalten werden.
Allerdings gingen beim TLfDI anschließend erste Hinweise darauf ein, dass Abbildungen der Aushänge nunmehr im Internet für jedermann zugänglich seien. Damit waren die Gesundheitsdaten von wenigen Beschäftigten ohne deren Einwilligung einer Vielzahl von unbekannten Empfängern zur Kenntnis gelangt, was auch ein großes Medieninteresse nach sich gezogen hat. Wie im Nachgang bekannt geworden ist, wurden die internen Aushänge im Unternehmen zwischenzeitlich abgehängt und sollten auch nicht wieder ausgehängt werden. Weitere Ausführungen zur formellen rechtmäßigen Einwilligung durch die Betroffenen erübrigten sich daher.
Da die Aushänge entfernt wurden, war von eventuellen weiteren Maßnahmen gegen die verantwortliche Stelle im Übrigen abzusehen, da zu diesem Zeitpunkt keine den Regelungen der DS-GVO widersprechende Datenverarbeitung mehr feststellbar war.
Der TLfDI prüfte, welche Möglichkeiten bestehen, gegen die Veröffentlichung der Gesundheitsdaten der Beschäftigten im Internet vorzugehen. Dies stieß auf eine Fülle von Schwierigkeiten. Zunächst müssen Verantwortliche festgestellt werden, gegen die gegebenenfalls Maßnahmen ergriffen werden können. Die Namensangaben müssen nicht mit den tatsächlichen Namen übereinstimmen und es muss die Wohnadresse ermittelt werden, um Forderungen zustellen zu können. Der TLfDI stellte klar, dass die Beschäftigten sich mit einer formlosen Beschwerde nach Art. 77 DS-GVO selbstverständlich an ihn wenden könnten. Hiervon wurde allerdings kein Gebrauch gemacht. Stattdessen ging eine hohe Anzahl von „Beschwerden“ nicht betroffener anderer Personen ein, die sich teilweise unsachlich mit dem Vorgehen

des Unternehmens auseinandersetzten. Auch diese Mitteilungen wurden seitens des TLfDI in der gebotenen Form beantwortet.

3.2 Können Datenschutzgründe der Annahme einer Initiativbewerbung entgegenstehen?

Potentielle Arbeitgeber sind grundsätzlich nicht verpflichtet, Initiativbewerbungen per E-Mail entgegenzunehmen und zu berücksichtigen. Insbesondere, wenn Gefahren für die IT-Sicherheit nicht auszuschließen sind und die internen Festlegungen zum Umgang mit Bewerbungen dem entgegenstehen, besteht kein Anspruch von Bewerbern darauf, dass Bewerbungen per E-Mail geöffnet werden.

Ein Bürger wollte sich initiativ bei einer Firma bewerben. Das Unternehmen nahm aber seine Bewerbung unter Hinweis auf Datenschutzgründe nicht entgegen. Der Betroffene wandte sich daher an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und fragte nach, welche Datenschutzgründe denn eine Initiativbewerbung unmöglich machen würden.
Offenbar stellte das Unternehmen die Gründe dafür, dass es keine Initiativbewerbungen entgegennehmen möchte, verkürzt und reduziert als „Datenschutzgründe“ dar. Was aber konkret gemeint war, konnte aus dem Schreiben des Unternehmens an die betroffene Person nicht entnommen werden.
Der TLfDI prüfte anhand des Vorbringens und der Ablehnung, woran es liegen könnte: Unternehmen müssen Bewerberdaten nach Art. 88 Datenschutz-Grundverordnung in Verbindung mit § 26 Bundesdatenschutzgesetz vertraulich behandeln und auch intern gegen Zugriff Unbefugter schützen. Personenbezogene Daten in Initiativbewerbungen über einen allgemeinen Firmen-E-Mailaccount könnten von einer Vielzahl von Personen zur Kenntnis genommen werden, die letztendlich weder mit der Bewerberauswahl noch mit Aufgaben der Personalverwaltung beauftragt sind. Bei einer Initiativbewerbung liegt es im Risikobereich des Bewerbers, dass damit auch unbefugte Kenntnis über die mit einer Bewerbung verbundenen personenbezogenen Daten erfolgen kann. Aus dem datenschutzrechtlichen Blickwinkel wird daher regelmäßig gefordert, dass ein Unternehmen von Bewerbern **nicht verlangen** darf, sich über die allgemeine E-Mail-Adresse zu bewerben, auf deren Account nicht nur diejenigen Personen Zugriff haben,

die aufgabenbezogen Zugriff auf Bewerberdaten nehmen dürfen. Daher ist – sofern Bewerbungen über E-Mail erwünscht sind – grundsätzlich ein gesonderter Account einzurichten, über den sich Bewerber auf bestimmte Stellen bewerben können und auf den intern auch nur die Personen zugreifen können, die mit dem Auswahlverfahren betraut sind.
Bei Bewerbungen per E-Mail besteht für den Empfänger darüber hinaus generell ein Risiko, dass mit umfangreichen Dateien auch Schadware auf die IT gelangen kann. Insoweit kann ein Bewerber auch nicht verlangen, dass Initiativbewerbungen ohne Bezug auf konkrete Stellenangebote vom Unternehmen geöffnet werden.
Eine Norm, die potentielle Arbeitgeber verpflichtet, solche Initiativbewerbungen entgegenzunehmen und gegebenenfalls auch zu berücksichtigen, ist nicht bekannt.
Im Übrigen waren aus der Rückantwort des Unternehmens keine Anhaltspunkte für die Nichteinhaltung der datenschutzrechtlichen Vorgaben zu entnehmen. Insoweit bestand auch kein Anlass, an das Unternehmen als Datenschutzaufsicht heranzutreten. Dies wurde dem Anfragenden mitgeteilt.

3.3 Beschwerde über Arbeitgeber wegen Veröffentlichungen zum Beschäftigungsende

Personalangelegenheiten sind vom Arbeitgeber vertraulich zu behandeln. Grundsätzlich verbietet es sich, Dritte über das Ausscheiden eines Mitarbeiters zu informieren.

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichten im Berichtszeitraum mehrere Beschwerden von Betroffenen, deren ehemalige Arbeitgeber sich nach Beendigung des Beschäftigungsverhältnisses veranlasst sahen, diesen Umstand Dritten (Behörden, Kunden, den verbleibenden Mitarbeitern oder sogar Verwandten der gekündigten Person) mündlich, schriftlich teilweise unter Angabe der Kündigungsgründe oder per Newsletter oder Rundmail mitzuteilen.
Auch nach Beendigung eines Beschäftigtenverhältnisses sind die beschäftigtendatenschutzrechtlichen Normen auf den Umgang mit den personenbezogenen Daten der ehemaligen Beschäftigten weiterhin anzuwenden. Das heißt, die Beschäftigten genießen weiterhin deren

Schutz. Zentrale Norm im Beschäftigtendatenschutz ist § 26 Bundesdatenschutzgesetz (BDSG). Danach dürfen personenbezogene Daten von Beschäftigten nur für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung oder zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung (Kollektivvereinbarung) ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten **erforderlich** ist. Dabei gelten auch Beschäftigte, deren Beschäftigungsverhältnis beendet ist, als Beschäftigte im Sinne dieser Vorschrift (§ 26 Abs. 8 Nr. 8 BDSG). Die Beendigung des Beschäftigtenverhältnisses stellt ein Personalaktendatum dar, das nur in wenigen Fällen vom Arbeitgeber Dritten gegenüber offenbart werden darf.
So hat beispielsweise ein Arbeitgeber bei Beendigung eines bei ihm versicherungspflichtig Beschäftigten diesen Umstand der Sozialversicherung zu melden (§ 28a Abs. 1 Nr. 2 SGB IV). Die Meldepflicht beim Arbeitsamt liegt beim Arbeitnehmer (§ 38 Abs. 1 SGB III). Der Arbeitgeber hat den Arbeitnehmer lediglich auf seine Meldepflichten beim Arbeitsamt hinzuweisen (§ 2 Abs. 2 Nr. 3 SGB III). Hinsichtlich der Information an Kunden könnte sich unter Umständen eine Rechtfertigung der bloßen Information, dass die betreffende Person nicht mehr im Unternehmen tätig ist, aus Art. 6 Abs. 1 Satz 1 Buchstabe f) Datenschutz-Grundverordnung (DS-GVO) ergeben. Danach können personenbezogene Daten zur erforderlichen Wahrung berechtigter Interessen des Verantwortlichen verarbeitet werden, sofern nicht die Interessen oder Grundrechte der betroffenen Personen der Mitteilung entgegenstehen. Zumindest für die Mitteilung der Tatsache, seit wann jemand nicht mehr im Betrieb tätig ist, kann zwar ein berechtigtes Interesse des ehemaligen Arbeitgebers liegen, da hinsichtlich der Arbeitsabläufe organisatorische Maßnahmen zu treffen sind und bei Kundenkontakt die Kunden gegebenenfalls wissen müssen, dass nunmehr ein anderer Ansprechpartner für sie zuständig ist. In jedem Fall sind aber die Gründe der Kündigung und auch die Tatsache einer Kündigung dabei nicht von Belang und es ist nicht erforderlich, derartige Informationen an Kunden zu geben.
Diese Bewertung gilt im Übrigen auch in der eigenen Belegschaft. Ist die Kenntnis von der Beendigung des Beschäftigungsverhältnisses zur internen Organisation der Arbeitsabläufe für andere Kolleginnen und

Kollegen relevant, so dürfen diese über die Beendigung auch informiert werden, nicht jedoch über die Gründe der Kündigung. Handelt es sich bei dem Gekündigten um einen Minderjährigen, ist auch eine Bestätigung einer Kündigung gegenüber anderen Verwandten als den Eltern unzulässig, ebenso wie gegenüber zufällig gemeinsamen Bekannten oder Freunden.
In einem Fall hat der TLfDI es für zulässig angesehen, Kunden allgemein darüber zu informieren, dass namentlich genannte Mitarbeiter ausgeschieden sind. Hintergrund war, dass es sich um einen von besonderem Vertrauen zwischen dem Unternehmen und der Kundschaft geprägten Geschäftsbereich handelte und die Kundenbindung stark auf die jeweils zuständigen Mitarbeiter bezogen war. Darüber hinaus hatte der Arbeitgeber auch nur allgemein in einem Newsletter den Wechsel der Ansprechpartner dargestellt. Somit war ein besonderes Interesse des Arbeitgebers zu bejahen, dass die Interessen der ausgeschiedenen Mitarbeiter, keine derartigen Informationen weiterzugeben, überwog. Die Mitarbeiter waren nämlich zwischenzeitlich für ein anderes Unternehmen desselben Geschäftsbereichs tätig und einzelne Kunden gingen weiterhin davon aus, sie stünden immer noch in Geschäftsbeziehung mit dem ehemaligen Arbeitgeber und wandten sich daher mit Nachfragen an sie.
In einem anderen Fall konnten Kunden zwar durch Internetrecherche leicht feststellen, dass der ehemalige Mitarbeiter sich zwischenzeitlich im selben Geschäftsfeld selbstständig gemacht hatte, die mündliche Auskunft darüber war dennoch für die Aufgabenerfüllung des Arbeitgebers nach § 26 Abs. 1 BDSG nicht erforderlich und daher unzulässig; von einer Offenkundigkeit der Selbstständigkeit konnte aufgrund der Internetpräsenz des ehemaligen Beschäftigten nicht ausgegangen werden.
Prägend in den geprüften Fällen war, dass die Beschwerdeführer sich jeweils noch in gerichtlichen Auseinandersetzungen mit dem jeweiligen Arbeitgeber befanden. Selbstverständlich kann jede betroffene Person sich mit einer Beschwerde nach Art. 77 DS-GVO an die Datenschutzaufsicht mit dem Vorbringen wenden, dass unter Verstoß gegen datenschutzrechtliche Vorschriften ihre personenbezogenen Daten verarbeitet werden oder wurden. Die Datenschutzaufsichtsbehörde prüft den Sachverhalt selbstverständlich pflichtgemäß, bewertet sie auf Rechtmäßigkeit und trifft gegebenenfalls Maßnahmen nach Art. 58 Abs. 2 DS-GVO gegenüber dem Verantwortlichen.

Darüber hinaus kann sich ein Ordnungswidrigkeitenverfahren mit der Verhängung empfindlicher Bußgelder anschließen. Dies kann von den Beschwerdeführern nicht gestoppt werden, indem die Beschwerde bei der Datenschutzaufsicht zurückgenommen wird, weil sie sich beispielsweise in einem Vergleich mit dem ehemaligen Arbeitgeber hierzu verpflichtet haben oder das gerichtliche Verfahren für sie günstig ausgegangen ist und der TLfDI nur „Munition" für die eigenen Belange liefern sollte. Der TLfDI verweist insoweit auf § 11 Abs. 1 Thüringer Datenschutzgesetz in Verbindung mit § 40 Abs. 1 BDSG, Art. 55 Abs. 1 DS-GVO) sowie Art. 57 und 58 DS-GVO. Nach Art. 57 Abs. 1 Buchstabe a) DS-GVO überwacht jede Aufsichtsbehörde in ihrem Hoheitsgebiet die Anwendung der DS-GVO und setzt diese durch. Dabei kann es dahingestellt werden, aus welchem Grund die Aufsichtsbehörde zunächst tätig wird. Der Beschwerde betroffener Personen kommt zwar erhebliche Bedeutung zu, jedoch ist die Aufgabenerfüllung der Aufsichtsbehörde nicht davon abhängig, dass eine Beschwerde eingelegt wird, besteht oder später zurückgezogen oder für erledigt erklärt wird.

3.4 Franchisenehmer unter Druck

Die interne Festlegung eines Franchisegebers, von so vielen Kunden wie möglich die Einwilligung zu Werbemaßnahmen zu erhalten und daran Provisionszahlungen des Franchisenehmers zu knüpfen, verstößt nicht gegen das Koppelungsverbot aus Art. 7 Abs. 4 DS-GVO.

Ein Franchisenehmer im Einzelhandel stellte eine Anfrage an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) zur Einholung einer Einwilligung. Aufgrund einer firmeninternen Zielvorgabe sollten möglichst für alle abgeschlossenen Verträge auch Einwilligungen zur Kontaktaufnahme und werblichen Ansprache per Post, E-Mail oder Telefon eingeholt werden. Zusätzlich für das Erreichen dieser Quote wurde vertrieblicher Druck ausgeübt und bei Erreichen durch hohe Bonuszahlungen honoriert. Die Frage des Franchisenehmers bezog sich auf die Zulässigkeit der Praxis des Franchisegebers, die Einholung der Einwilligung an die Bonuszahlungen zu koppeln.
Der TLfDI bewertete diese Anfrage hinsichtlich der Zulässigkeit und kam zu dem Ergebnis, dass eine derartige Einwilligung in die Nutzung von personenbezogenen Daten nur dann wirksam ist, wenn sie den

Voraussetzungen der Art. 4 Nr. 11 und Art. 7 Datenschutz-Grundverordnung (DS-GVO) entspricht. Die Einwilligung muss freiwillig, für einen bestimmten Fall, in informierter Weise und unmissverständlich abgegeben werden. Freiwillig ist sie nur, wenn die betroffene Person, also der Kunde, eine echte oder freie Wahl hat und damit in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden (Erwägungsgrund 42 DS-GVO). Wenn die Kunden also transparent informiert werden, für welche Zwecke sie ihre personenbezogenen Daten zur Verfügung stellen und sich dann aus freien Stücken dazu entschließen, ihre Einwilligung zu erteilen, ist diese auch wirksam. Dass die Franchisenehmer dazu angehalten werden, so viele Einwilligungen wie möglich von ihren Kunden zu erlangen und nur dann einen Bonus vom Franchisegeber bekommen, verstößt grundsätzlich nicht gegen Grundsätze des Datenschutzrechts. Erst in dem Moment, indem die Kunden dazu gedrängt werden, eine Einwilligung in die Datennutzung zu erteilen und ohne diese Einwilligung der Kauf oder die Dienstleistung nicht erfüllt werden, verstößt dies gegen das Koppelungsverbot.
Das Koppelungsverbot in Art. 7 Abs. 4 DS-GVO bezieht sich auf die Freiwilligkeit der Einwilligung der Kunden und daran angeknüpfte Bedingungen, die für die eigentliche Vertragserfüllung nicht erforderlich wären. Die Tatsache, dass der Franchisenehmer keine Provision erhält, wenn dieser nicht genug Kunden dazu bringt, eine Einwilligung zu erteilen, ist keine Koppelung im Sinne des Art. 7 Abs. 4 DS-GVO, da es nicht dasselbe Vertragsverhältnis betrifft.

3.5 Überwachung der Exfrau durch GPS-Sender im Fahrzeug

Bei den durch einen in einem Fahrzeug fest eingebauten GPS-Sender aufgezeichneten und über eine Funkschnittstelle (SIM-Karte) übertragenen Standort-Daten handelt es sich um personenbezogene Daten im Sinne von Art. 4 Nr. 1 DS-GVO, wenn diese einer bestimmten Person zugeordnet werden können. Dies gilt insbesondere dann, wenn das Fahrzeug einer Person zur alleinigen Nutzung zur Verfügung steht, da die Standortdaten dann ausschließlich ihr zuzuordnen sind.

Bei der Staatsanwaltschaft hatte eine Fahrzeughalterin Anzeige erstattet, weil in ihrem Fahrzeug ohne ihr Wissen fest ein GPS-Sender verbaut worden war. Da der angezeigte Sachverhalt weder den Tatbe-

stand der Nachstellung gemäß § 238 Strafgesetzbuch noch einen anderen Straftatbestand erfüllte, übersandte die Staatsanwaltschaft Meiningen die Akte eines Ermittlungsverfahrens zur Verfolgung einer Ordnungswidrigkeit gemäß § 43 Ordnungswidrigkeitengesetz an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI).
In diesem Zusammenhang berichtete die geschädigte Fahrzeughalterin in ihrer Anzeige, dass es bereits im Jahr 2017 zur Trennung von ihrem Exmann gekommen sei. Trotzdem habe ihr dieser immer wieder zum Vorwurf gemacht, wo sie sich gerade aufhalte und welcher Beschäftigung sie nachgehe. Da sie sich beobachtet und überwacht gefühlt habe, untersuchte der Schwager der Geschädigten auf ihre Bitte hin ihr Fahrzeug und stellte hierbei ein GPS-Ortungsgerät mit einer SIM-Karte fest. Dieser GPS-Sender war an der Batterie des Fahrzeuges angeschlossen und mit Kabelbinder und Klebeband an der Karosserie unterhalb eines Scheinwerfers so befestigt, dass er fast nicht sichtbar war.
Nach einer weiteren Vernehmung der Geschädigten und einer technischen Analyse des GPS-Senders durch das Technikreferat des TLfDI wurde der betroffene Exmann wegen einer Ordnungswidrigkeit gemäß Art. 83 Abs. 5 Buchstabe a) Datenschutz-Grundverordnung (DS-GVO) angehört, machte jedoch keine Angaben zum Sachverhalt. Im Rahmen der weiteren Ermittlungen des TLfDI konnte jedoch zweifelsfrei nachgewiesen werden, dass der Betroffene den GPS-Sender über einen Zeitraum von circa drei Monaten hinweg betrieben und so die Standortdaten seiner Exfrau erhoben hatte. Der Nachweis konnte geführt werden, da der Betroffene die Identifikationsnummer des GPS-Senders zusammen mit der SIM-Karte zum Zwecke der Nutzung kostenpflichtig auf einem Web-Portal angemeldet und hierbei seine Kontaktdaten angegeben hatte. Der Betreiber des Web-Portals konnte so auf Anfrage des TLfDI den Nutzer und den Nutzungszeitraum ermitteln.
Aufgrund dieser Sach- und Rechtslage erging ein Bußgeldbescheid gegen den Betroffenen. Nach Art. 83 Abs. 5 Buchstabe a) DS-GVO handelt ordnungswidrig, wer gegen die Grundsätze für die Verarbeitung, einschließlich der Bedingungen für die Einwilligung, gemäß den Artikeln 5, 6, 7 und 9 DS-GVO verstößt. Die durch den GPS-Sender aufgezeichneten und über die Funkschnittstelle/SIM-Karte übertragenen Standort- beziehungsweise GPS-Daten sind als personenbezogene Daten im Sinne des Art. 4 Nr. 1 DS-GVO einzuordnen. Aufgrund des

Umstandes, dass das Fahrzeug, in welches der GPS-Sender eingebaut gewesen ist, der Geschädigten zur alleinigen Nutzung zur Verfügung stand, waren die ermittelten Standortdaten ausschließlich ihr zuzuordnen beziehungsweise bezogen sich ausschließlich auf sie. Das Erheben und die Speicherung dieser personenbezogenen Daten stellt eine Verarbeitung gemäß Art. 4 Nr. 2 DS-GVO dar. Da der GPS-Sender ausweislich der auf dem Web-Portal hinterlegten Kontaktdaten von dem Betroffenen betrieben wurde, war dieser auch Verantwortlicher gemäß Art. 4 Nr. 7 DS-GVO. Die Verarbeitung dieser Daten erfolgte unrechtmäßig. Nach Art. 5 Abs. 1 Buchstabe a) DS-GVO müssen personenbezogene Daten auf rechtmäßige Weise verarbeitet werden. Aus Art. 6 Abs. 1 DS-GVO ergibt sich, dass nur unter den dort genannten Bedingungen eine Datenverarbeitung zulässig ist. Es handelt sich somit um ein Verbot mit Erlaubnisvorbehalt. Vorliegend konnte die Verarbeitung der personenbezogenen Daten nicht auf die Einwilligung der betroffenen Personen nach Art. 6 Abs. 1 Satz 1 Buchstabe a) DS-GVO gestützt werden. Hierzu wäre es erforderlich gewesen, dass die Geschädigte vor der Erfassung ihrer Standortdaten durch den Betroffenen unter Nennung des Zweckes in die Verarbeitung eingewilligt hätte. Eine solche Einwilligung lag dem Betroffenen jedoch nicht vor. Auch kann die Verarbeitung der personenbezogenen Daten nicht auf den einzig noch in Betracht zu ziehenden Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO gestützt werden. Demnach wäre die Verarbeitung rechtmäßig, wenn sie zur Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen. Da die Ermittlung der Standortdaten ausschließlich dem Zweck diente, die Geschädigte zu rein privaten Zwecken zu überwachen, fehlt es bereits an einem berechtigten Interesse. In jedem Fall stehen die schutzwürdigen Interessen der Geschädigten entgegen.
Bei der Bemessung der Geldbuße gemäß Art. 83 Abs. 2 DS-GVO musste durch den TLfDI zulasten des Betroffenen ein vorsätzliches Handeln und die Eingriffsintensität und Dauer des Verstoßes berücksichtigt werden. Auch wurde berücksichtigt, dass der Verstoß nicht durch den Betroffenen selbst beendet wurde, sondern der GPS-Sender durch den Schwager der Geschädigten entdeckt und ausgebaut wurde. Die in dem inzwischen rechtskräftigen Bußgeldbescheid festgesetzte Geldbuße im oberen dreistelligen Bereich war damit zugleich wirksam, verhältnismäßig wie ausreichend abschreckend für die Zukunft.

3.6 Versand einer Bewerbungsmappe für Mietwohnung per E-Mail durch einen Immobilienmakler

Bei dem Versand der Bewerbungsmappe einer Person durch einen Verantwortlichen an eine andere Person kann ein berechtigtes (Dritt-) Interesse im Sinne des Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO darin bestehen, der anderen Person ein Muster für ihre Bewerbung zur Verfügung zu stellen. Hierbei ist jedoch zwingend eine Anonymisierung vorzunehmen, da für den Empfänger der Bewerbungsmappe die Kenntnis der personenbezogenen Daten nicht erforderlich ist.

Mit einer Ordnungswidrigkeitenanzeige wandte sich eine Rechtsanwältin im Berichtszeitraum an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und rügte für ihre Mandantin die Verletzung des Rechts auf informationelle Selbstbestimmung und einen damit einhergehenden Verstoß gegen die Datenschutz-Grundverordnung (DS-GVO) durch eine in Thüringen ansässige Immobiliengesellschaft.
Demnach habe sich die geschädigte Mandantin der Rechtsanwältin nach erfolgter Besichtigung für die Anmietung einer Wohnung entschieden. Da vom Vermieter so gefordert, habe sie eine umfangreiche Bewerbungsmappe erstellt und an die verantwortliche Immobiliengesellschaft als Maklerin der Wohnung gesendet. Die Bewerbungsmappe habe neben einem Anschreiben und einer Mieterselbstauskunft auch Kopien des Personalausweises und diverser Verdienstabrechnungen und Versicherungsbescheinigungen enthalten. Die Verantwortliche habe diese Bewerbungsmappe später an einen anderen Mietinteressenten per E-Mail weitergeleitet, um diesem ein Muster für die vom Vermieter geforderten Bewerbungsunterlagen zur Verfügung zu stellen. Hierbei habe die Verantwortliche die Bewerbungsmappe ohne jegliche Anonymisierung der personenbezogenen Daten der Betroffenen an den Mietinteressenten versandt.
Auf Grundlage dieser Schilderungen leitete der TLfDI umgehend ein Verfahren wegen einer Ordnungswidrigkeit gemäß Art. 83 Abs. 5 Buchstabe a) DS-GVO gegen die Immobiliengesellschaft ein. Im Zuge der Ermittlungen wurden sodann mehrere schriftliche Zeugenvernehmungen durchgeführt und die Verantwortliche zur Sache angehört. Der Geschäftsführer der Verantwortlichen zeigte sich geständig und räumte die Ordnungswidrigkeit umgehend ein. Er erklärte, dass

er die Bewerbungsunterlagen der Betroffenen wegen Zeitdrucks versehentlich nicht noch einmal durchgesehen und daher ohne Anonymisierung weitergeleitet habe. Der Geschäftsführer versicherte zudem, dass ihm ein solcher Fehler nicht noch einmal passieren werde.
Aufgrund dieser Sach- und Rechtslage erging ein Bußgeldbescheid gegen die Verantwortliche. Nach Art. 83 Abs. 5 Buchstabe a) DS-GVO handelt ordnungswidrig, wer gegen die Grundsätze für die Verarbeitung, einschließlich der Bedingungen für die Einwilligung, gemäß den Artikeln 5, 6, 7 und 9 DS-GVO verstößt. Die in der Bewerbungsmappe unter anderem enthaltenen Angaben zur Anschrift, E-Mail-Adresse und Telefonnummer der Betroffenen einschließlich der Daten des Personalausweises sind als personenbezogene Daten im Sinne des Art. 4 Nr. 1 DS-GVO einzuordnen. Mit dem Versand dieser personenbezogenen Daten in der nicht anonymisierten Bewerbungsmappe als E-Mail-Anhang wurden diese gegenüber einem Dritten offengelegt, was eine Verarbeitung gemäß Art. 4 Nr. 2 DS-GVO darstellt. Hierbei handelte die Immobiliengesellschaft als Verantwortliche gemäß Art. 4 Nr. 7 DS-GVO. Die Verarbeitung dieser Daten erfolgte unrechtmäßig. Nach Art. 5 Abs. 1 Buchstabe a) DS-GVO müssen personenbezogene Daten auf rechtmäßige Weise verarbeitet werden. Aus Art. 6 Abs. 1 DS-GVO ergibt sich, dass nur unter den dort genannten Bedingungen eine Datenverarbeitung zulässig ist. Es handelt sich somit um ein Verbot mit Erlaubnisvorbehalt. Vorliegend konnte die Verarbeitung der personenbezogenen Daten nicht auf die Einwilligung der betroffenen Person nach Art. 6 Abs. 1 Satz 1 Buchstabe a) DS-GVO gestützt werden. Hierzu wäre es erforderlich gewesen, dass die Betroffene vor dem Versand des E-Mail-Anhangs unter Nennung des Zweckes in die Verarbeitung eingewilligt hätte. Eine solche Einwilligung lag der Verantwortlichen jedoch nicht vor.
Auch konnte die Verarbeitung nicht auf den einzig noch in Betracht zu ziehenden Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO gestützt werden. Demnach wäre die Verarbeitung rechtmäßig, wenn sie zur Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen. Soweit der Geschäftsführer der Verantwortlichen im Rahmen der Anhörung angegeben hatte, dass der Versand des E-Mail-Anhangs dem Zweck diente, einem Mietinteressenten eine Musterbewerbung zur Verfügung zu stellen, ist hierin grundsätzlich ein berechtigtes Drittinteresse zu sehen. Allerdings ist

das Kriterium der Erforderlichkeit vorliegend nicht erfüllt. Eine Datenverarbeitung jeglicher Art ist nur im Rahmen ihrer Erforderlichkeit als zulässig zu erachten. Erlaubt ist eine Verarbeitung auf Grundlage des Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO, wenn die berechtigten Interessen nicht auf anderem Weg ebenso effektiv verwirklicht werden können und hierbei die Rechte und Interessen der betroffenen Person weniger beeinträchtigt werden. Vorliegend hätten die Bewerbungsunterlagen der Betroffenen auch mit anonymisierten personenbezogenen Daten versendet werden können, da für den Empfänger der E-Mail lediglich die Art und Weise der Bewerbungsunterlagen als Muster relevant war, nicht aber die Angaben zur Person der Betroffenen. Mit entsprechenden Schwärzungen hätte daher das Interesse des E-Mail-Empfängers ebenso effektiv verwirklicht werden können.
Bei der Bemessung der Geldbuße gemäß Art. 83 Abs. 2 DS-GVO berücksichtigte der TLfDI zunächst ein fahrlässiges Handeln des Geschäftsführers der Verantwortlichen. Soweit dieser es wegen Zeitdrucks unterlassen hatte zu prüfen, ob der Inhalt der Bewerbungsmappe eine Anonymisierung personenbezogener Daten erforderlich machte, wurde die notwendige Sorgfalt außer Acht gelassen. Zudem wirkte sich mildernd aus, dass sich der Geschäftsführer der Verantwortlichen geständig gezeigt und zudem versichert hatte, dass ihm ein solcher Fehler nicht erneut passieren werde. Schärfend war hingegen durch den TLfDI zu berücksichtigen, dass in erheblichem Umfang zum Teil auch sehr sensible Daten der Betroffenen von der Verarbeitung berührt waren. Die in dem inzwischen rechtskräftigen Bußgeldbescheid festgesetzte Geldbuße im oberen dreistelligen Bereich war damit zugleich wirksam, verhältnismäßig wie ausreichend abschreckend für die Zukunft.

3.7 Versicherungswerbung per E-Mail

Stützt ein Verantwortlicher die Verarbeitung personenbezogener Daten auf die Einwilligung gemäß Art. 6 Abs. 1 Satz 1 Buchstabe a) DS-GVO, so muss er gemäß Art. 7 Abs. 1 DS-GVO gegenüber der Aufsichtsbehörde nachweisen können, dass die betroffene Person eingewilligt hat. Diese Nachweispflicht entfällt auch nicht durch ein Löschungsverlangen der betroffenen Person.

Mit einer Beschwerde wurde dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) bekannt, dass

ein Unternehmen in Thüringen, welches als Versicherungsmakler mit der erforderlichen Erlaubnis nach § 34d Gewerbeordnung diverse Internetpräsenzen betreibt und auf diesen den Abschluss von Versicherungsverträgen vermittelt, eine Versicherungswerbung per E-Mail versendet hatte.
Auf die mehrfache Nachfrage der Beschwerdeführerin zur Herkunft ihrer Daten teilte ihr das Unternehmen per E-Mail mit, dass die Beschwerdeführerin diese selbst auf einem von dem Unternehmen betriebenen Internetportal angegeben und in diesem Zuge auch ihre Einwilligung zur Nutzung dieser Daten erteilt habe. Da sich die Beschwerdeführerin nicht erinnern konnte, das besagte Internetportal besucht zu haben, bat sie das Unternehmen erneut um Auskunft hinsichtlich der Herkunft der Daten und forderte dieses zudem dazu auf, ihre personenbezogenen Daten unverzüglich zu löschen und nicht an Dritte weiterzugeben.
Da eine Antwort des Unternehmens dieses Mal ausblieb, wandte sich die Beschwerdeführerin an den TLfDI. Auf dessen Auskunftsersuchen gemäß Art. 58 Abs. 1 Buchstabe a) Datenschutz-Grundverordnung (DS-GVO) hin benannte das Unternehmen einen konkreten Zeitpunkt, an dem die Beschwerdeführerin auf dem Internetportal ihre Einwilligung erteilt haben soll. Der darauffolgenden Aufforderung des TLfDI zum Nachweis der Einwilligung kam die Betroffene nicht mehr nach und erklärte, dass sich der ursprünglich mitgeteilte Zeitpunkt der Einwilligungserklärung nach interner Überprüfung auf eine andere Person bezogen habe und die Einwilligungserklärung der Beschwerdeführerin aufgrund ihres Löschungsverlangens tatsächlich nicht mehr gespeichert sei.
Hierauf sprach der TLfDI gegenüber dem Unternehmen eine Verwarnung nach Art. 58 Abs. 2 Buchstabe b) DS-GVO aus, weil die Wirksamkeit einer Einwilligung gemäß Art. 7 Abs. 1 DS-GVO gegenüber der Aufsichtsbehörde nachzuweisen ist, soweit die Verarbeitung personenbezogener Daten auf Art. 6 Abs. 1 Satz 1 Buchstabe a) DS-GVO gestützt wird und dieser Nachweis nicht erbracht wurde.
Die hiergegen form- und fristgerecht erhobene Klage des Unternehmens blieb in der Sache ohne Erfolg. Das Verwaltungsgericht Weimar bestätigte die Rechtsauffassung des TLfDI in seinem Urteil vom 30. Juni 2021 zum Az. 3 K 1927/19 We und unterstrich in seiner Begründung, dass die Nachweispflicht hinsichtlich einer Einwilligung

nicht durch das Löschungsverlangen der von der Verarbeitung der personenbezogenen Daten betroffenen Person entfalle. Zu den Einzelheiten:
Mit der Versendung der Werbe-E-Mail durch das Unternehmen kam es in Bezug auf den Namen, die Wohnanschrift und die E-Mail-Adresse – welche personenbezogene Daten gemäß Art. 4 Nr. 1 DS-GVO darstellen – zu einer Verarbeitung im Sinne des Art. 4 Nr. 2 DS-GVO dar. Das Unternehmen war hierbei Verantwortlicher gemäß Art. 4 Nr. 7 DS-GVO. Nach Art. 5 Abs. 1 Buchstabe a) DS-GVO müssen personenbezogene Daten auf rechtmäßige Weise verarbeitet werden. Aus Art. 6 Abs. 1 Satz 1 DS-GVO ergibt sich, dass nur unter den dort genannten Bedingungen eine Datenverarbeitung zulässig ist. Es handelt sich somit um ein Verbot mit Erlaubnisvorbehalt.
Die Verarbeitung dieser personenbezogenen Daten war hier rechtswidrig erfolgt. Wie das Unternehmen gegenüber dem TLfDI selbst mitgeteilt hatte, stützte es die Verarbeitung der personenbezogenen Daten der Beschwerdeführerin auf eine Einwilligung, konnte den entsprechenden Nachweis jedoch nach eigenen Angaben nicht erbringen. Eine weitere Rechtsgrundlage gemäß Art. 6 Abs. 1 Satz 1 DS-GVO war nicht ersichtlich. Gemäß Art. 4 Nr. 11 DS-GVO ist eine Einwilligung jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist. Hierbei war das Unternehmen als Verantwortliche verpflichtet, den entsprechenden Nachweis darüber zu führen. Die DS-GVO enthält in Ansehung der hierzu ergangenen Rechtsprechung und der herrschenden Literaturmeinung mit Art. 7 Abs. 1 DS-GVO insoweit eine ausdrückliche Beweislastregel für das Vorliegen einer wirksamen Einwilligung. Den Verantwortlichen trifft demnach nicht nur die Verantwortung für die Einhaltung der in Art. 5 Abs. 1 DS-GVO geregelten Grundsätze für die Verarbeitung personenbezogener Daten, er muss ihre Einhaltung auch nachweisen können. Diese Nachweispflicht kann er durch entsprechende Dokumentation oder ein Daten-Management-System erfüllen. Die Nichterweislichkeit des Vorliegens der Einwilligung ging hier zulasten des Unternehmens.
Die Nachweispflicht ist auch nicht durch das Löschungsverlangen der Beschwerdeführerin entfallen. Gemäß Art. 17 Abs. 3 Buchstabe b) DS-GVO ist die Löschung personenbezogener Daten ausgeschlossen,

soweit diese zur Erfüllung einer rechtlichen Verpflichtung erforderlich sind, welche die Verarbeitung nach dem Recht der Union oder der Mitgliedsstaaten erfordert, dem der Verantwortliche unterliegt. Diese Sonderregelung entspricht der Rechtsgrundlage für die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung aus Art. 6 Abs. 1 Satz 1 Buchstabe c) DS-GVO. Zu diesen Rechtspflichten zählen insbesondere Speicher-, Dokumentations- und Aufbewahrungspflichten, zu denen auch die in Art. 5 Abs. 2 und Art. 7 Abs. 1 DS-GVO geregelten Nachweispflichten zählen. Das Verwaltungsgericht Weimar wies in diesem Zusammenhang ausdrücklich darauf hin, dass andernfalls das Kontrollrecht der Aufsichtsbehörde nach Art. 58 DS-GVO faktisch leerlaufen würde.
Offengelassen, da für den Fall nicht relevant, hat das Gericht lediglich die Beantwortung der Frage, welche konkrete Aufbewahrungsfrist für den Nachweis der Einwilligung mangels ausdrücklicher Regelung in der DS-GVO zu Grunde zu legen ist. Der TLfDI stellt hier auf eine Frist von drei Jahren ab, da nach Ablauf dieses Zeitraums ein Bußgeldverfahren in der Regel als verjährt anzusehen ist.
Mit seiner Entscheidung hat das Verwaltungsgericht Weimar im Ergebnis die Befugnisse und Kontrollrechte der Aufsichtsbehörde gemäß Art. 58 DS-GVO gestärkt und auch hinsichtlich der Rechenschaftspflichten der Verantwortlichen für Klarheit gesorgt. Die gegen diese Entscheidung zunächst eingelegte Berufung zum Thüringer Oberverwaltungsgericht wurde durch das Unternehmen zwischenzeitlich wieder zurückgenommen. Die Entscheidung des Verwaltungsgerichts Weimar ist damit rechtskräftig.

3.8 Missbrauch von Gesundheitsdaten bei Wahl der Schwerbehindertenvertretung

Die Information, ob ein Mitarbeiter zur Gruppe der schwerbehinderten Bediensteten gehört, ist ein Gesundheitsdatum im Sinne des Art. 4 Nr. 15 sowie eine besondere Kategorie personenbezogener Daten nach Art. 9 Abs. 1 DS-GVO und gilt als sensibles Datum. Von diesen Datenkategorien geht ein erhöhtes Diskriminierungsrisiko aus. Ein Verstoß gegen die Verarbeitungsgrundsätze stellt einen hohen Eingriff in das Grundrecht auf Datenschutz nach Art. 8 GRCH beziehungsweise auf das informationelle Selbstbestimmungsrecht dar.

Eine Mitarbeiterin in einer Bundesbehörde – welche ihren Hauptsitz in Thüringen hat – beschaffte sich eine Liste der schwerbehinderten Menschen, die in der Dienststelle beschäftigt waren. In dieser Liste waren die Namen, die Vornamen, die Stelle innerhalb der Behörde und der Dienstort von insgesamt 95 Personen erfasst. Es handelte sich dabei um die Wählerliste für die Wahl der Schwerbehindertenvertretung. Sie wurde den wahlberechtigten schwerbehinderten und gleichgestellten Menschen der Bundesbehörde gemäß § 3 Abs. 1 Schwerbehindertenwahlverordnung (SchwbVWO) im Zusammenhang mit der Wahl der Schwerbehindertenvertretung vom Wahlvorstand zur Einsicht in den verschiedenen Dienststellen der Bundesbehörde ausgelegt, § 3 Abs. 2 SchwbVWO. In der Folge verfasste die Mitarbeiterin ein nicht näher datiertes und von ihr persönlich unterzeichnetes Rundschreiben in Verbindung mit der Wahl der Schwerbehindertenvertretung bei der Bundesbehörde. Darin erklärte sie, die Wahl zur Vertrauensperson und die Wahl zu den Vertretern der Vertrauensperson der schwerbehinderten Menschen der Bundesbehörde beim Arbeitsgericht angefochten zu haben. Als Anlage war ein nicht rechtskräftiger Beschluss des Arbeitsgerichts angefügt. Das Rundschreiben und den beigefügten Beschluss versandte die Mitarbeiterin mit der Dienstpost an alle in der Wählerliste erfassten 95 Personen. Zum Tatzeitpunkt war die Mitarbeiterin in einer Dienststelle der Bundesbehörde in Sachsen beschäftigt.

Nachdem der Behördenleiter zahlreiche Beschwerden betroffener Beschäftigter zu dem genannten Rundschreiben erhielt, stellte er eine Ordnungswidrigkeitenanzeige beim Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI). Es war festzustellen, dass die Mitarbeiterin dienstfremde Zwecke verfolgte und als eigene Verantwortliche im Sinne des Art. 4 Nr. 7 Datenschutz-Grundverordnung (DS-GVO) handelte. Dieses Verhalten nennt man Mitarbeiterexzess. Sie versandte an alle auf der Liste enthaltenen Personen ein Rundschreiben, um private Interessen kundzutun. Die Erhebung und weitere Verwendung der auf oben genannter Liste enthaltenen personenbezogenen Daten schwerbehinderter Menschen war für ihre Tätigkeit in der Dienststelle zum Tatzeitpunkt nicht erforderlich. Auch konnte sich die Betroffene nicht darauf berufen, dass die Versendung des Rundschreibens im Amt als Stellvertretung der Vertrauensperson der schwerbehinderten Menschen erfolgte. Zum Zeitpunkt der Auslage der Liste schwerbehinderter Menschen in Vorbereitung zur Wahl

der Schwerbehindertenvertretung war die Betroffene weder Vertrauensperson noch hatte sie ein Amt der Stellvertretung inne. Der Datenschutzverstoß war folglich nicht der Bundesbehörde zuzurechnen. Daher musste das Ordnungswidrigkeitenverfahren vom BfDI an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) abgegeben werden.
Der Leiter dieser Bundesbehörde mit Hauptsitz in Thüringen, in der das genannte Rundschreiben versandt wurde, fertigte bereits vor Einleitung des Bußgeldverfahrens einen Bescheid zur Herausgabe der unbefugt erhobenen Wählerliste zur Schwerbehindertenvertretung unter Androhung eines Zwangsgeldes. Da die Mitarbeiterin die Liste nicht an den Dienstherren herausgab, wurde ein Zwangsgeld festgesetzt, welches sie auch zahlte. Dennoch legte sie Widerspruch gegen den Herausgabebescheid ein. Das Verfahren ist beim Verwaltungsgericht Chemnitz anhängig. Eine abschließende Entscheidung zur Herausgabe der Wählerliste erging noch nicht.
Für den TLfDI besteht eine Zuständigkeit nach § 37 Abs. 1 Nr. 1, 2. Alt. Gesetz über Ordnungswidrigkeiten (OWiG). Der TLfDI ist örtlich zuständig, da die Ordnungswidrigkeit in seinem Zuständigkeitsbezirk entdeckt worden ist. Die Beschwerden über die Zusendung eines nicht rechtskräftigen Beschlusses zur Wahl der Schwerbehindertenvertretung gingen zunächst direkt bei der Bundesbehörde in Thüringen ein. Diese ging der Beschwerde nach und stellte fest, dass die Betroffene die zur Wahl der Schwerbehindertenvertretung ausgelegte Liste wahlberechtigter Personen zugänglich gemacht und zweckentfremdet verwendet hat. „Die Owi ist entdeckt, wenn es angezeigt ist, dem aufgrund konkreter Tatsachen begründeten Verdacht der Owi nachzugehen, also das Bußgeldverfahren einzuleiten“, so Gürtler in Göhler, OWiG, 16. Auflage, § 37, Rn. 3. Weiter heißt es „Es ist nicht notwendig, dass gerade Ermittlungsbeamte der Verwaltungsbehörde die Owi entdecken. Maßgebend ist die ‚dienstliche‘ Entdeckung; die Entdeckung durch eine Privatperson begründet den Entdeckungsort demnach nicht.“ Es ist festzustellen, dass die Ordnungswidrigkeit im Zuständigkeitsbereich des TLfDI, nämlich in Thüringen, bekannt geworden ist. Es kommt nicht darauf an, ob die entdeckende Behörde für die Verfolgung der in Rede stehenden Ordnungswidrigkeit zuständig ist (vergleiche Lampe in: Karlsruher Kommentar OWiG, 4. Auflage, § 37, Rn. 5).
Gleichwertig neben der Zuständigkeit des Entdeckungsortes steht die des Wohnsitzes nach § 37 Abs. 1 Nr. 2 OWiG. Danach ergibt sich eine

Doppelzuständigkeit des TLfDI nach dem Entdeckungsort und des Sächsischen Datenschutzbeauftragten nach dem Wohnsitz. Zwischen den einzelnen, die örtliche Zuständigkeit der Verwaltungsbehörde begründenden Umständen besteht keine Rangordnung (vergleiche Lampe in: Karlsruher Kommentar OWiG, 4. Auflage, § 37, Rn. 2): „Zuständig für die Verhängung von Geldbußen ist nach § 41 Bundesdatenschutzgesetz (BDSG) die zuständige Aufsichtsbehörde gemäß den innerstaatlichen Zuständigkeitsregeln (Art. 83 Abs. 7 DS-GVO), das heißt im Regelfall die zuständige Landesdatenschutzbehörde. Die örtliche Zuständigkeit ist nach § 37 OWiG zu bestimmen. Da ‚Tatort' in der Regel der Sitz des Unternehmens/der Behörde ist, wird ein Verfahren zumeist vom Landesdatenschutzbeauftragten geführt, in dessen räumlichen Zuständigkeitsbereich der Sitz liegt. In diesem Fall liegt der Hauptsitz der Dienststelle der Betroffenen in Thüringen, dem Zuständigkeitsbereich des TLfDI. Bei Betroffenheit mehrerer Länder koordinieren sich die Landesdatenschutzbehörden." (Becker in: Plath, DS-GVO/BDSG, 3. Auflage 2018, § 41, Rn. 10). Danach stimmte sich letztlich der TLfDI mit den Sächsischen Datenschutzbeauftragten zur Zuständigkeitsbestimmung ab. Nach Lampe in Karlsruher Kommentar OWiG, 4. Auflage, § 37, Rn. 4 soll „die mit der Sache befasste Verwaltungsbehörde das Bußgeldverfahren durchführen können, selbst wenn die Ordnungswidrigkeit zu einem früheren Zeitpunkt außerhalb ihres Bezirks begangen ist und der Täter seinen Wohnsitz außerhalb des Bezirks der Verwaltungsbehörde hat, die bereits mit der Sache befasst ist." Dieser Auffassung schloss sich die Sächsische Datenschutzaufsichtsbehörde an, sodass für die Verfolgung dieser Ordnungswidrigkeit die örtliche Zuständigkeit beim TLfDI gegeben ist. Zudem regelt § 39 Abs. 1 Satz 1 OWiG bei mehrfacher Zuständigkeit den Vorzug der Verwaltungsbehörde, die wegen der Tat den Betroffenen zuerst vernommen hat.

Der TLfDI erließ nach Prüfung der Sach- und Rechtslage gegen die Mitarbeiterin einen Bußgeldbescheid nach Art. 83 Abs. 5 Buchstabe a) DS-GVO mit einer Geldbuße in Höhe von insgesamt 1.925 Euro. Durch das Erheben und Verwenden der auf der Liste schwerbehinderter Menschen der Bundesbehörde enthaltenen personenbezogenen Daten und das darauffolgende Rundschreiben an diese Personen hat die Mitarbeiterin besondere Kategorien personenbezogener Daten verarbeitet, ohne dass hierfür eine Rechtsgrundlage gegeben war. Personenbezogene Daten sind nach Art. 4 Nr. 1 DS-GVO alle Informationen, die sich auf eine identifizierte Person beziehen.

Gesundheitsdaten sind nach Art. 4 Nr. 15 DS-GVO personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen. Nach Art. 5 Abs. 1 Buchstabe a) DS-GVO müssen personenbezogene Daten auf rechtmäßige und in einer für die von der Datenverarbeitung betroffenen Personen nachvollziehbaren Weise verarbeitet werden. Die Verarbeitung personenbezogener Daten im Sinne des Art. 4 Nr. 2 DS-GVO ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten. Da es sich bei oben genannter Liste um eine Liste schwerbehinderter Menschen der Bundesbehörde handelt, hatte die Mitarbeiterin zweifelsohne auch personenbezogene Gesundheitsdaten verarbeitet. Die behördliche Anerkennung als Schwerbehinderter ist ein Gesundheitsdatum (vergleiche Weichert in: Kühling/Buchner, DS-GVO/BDSG, 2. Auflage, Art. 4, Rn. 6). Rückschlüsse auf den Gesundheitszustand, nämlich, dass die betroffenen Personen eine körperliche oder geistige Behinderung haben, sind uneingeschränkt möglich. Art. 9 Abs. 1 DS-GVO untersagt die Verarbeitung personenbezogener Gesundheitsdaten einer natürlichen Person. Eine weitergehende Verarbeitung von Gesundheitsdaten zu einem anderen Zweck als zur Wahl der Schwerbehindertenvertretung ist nur unter den engen Voraussetzungen des Art. 9 Abs. 2 DS-GVO zulässig. Die von der Datenverarbeitung betroffenen Personen sind die auf oben genannter Liste enthaltenen schwerbehinderten Menschen, welche bei der Bundesbehörde beschäftigt sind. Die Wählerliste zur Schwerbehindertenvertretung war im vorliegenden Fall gemäß § 3 Abs. 2 SchwbVWO zur Einsichtnahme ausgelegt und nur für die Wahl der Vertrauensperson der schwerbehinderten Menschen und deren Vertreter bestimmt. Diese Liste war – ebenfalls nach § 3 Abs. 2 SchwbVWO – bis zum Abschluss der Stimmabgabe ausgelegt. Die Mitarbeiterin hat die Liste schwerbehinderter Menschen der Bundesbehörde unbefugt für eigene private Zwecke erhoben und verwendet. Die Voraussetzungen einer rechtmäßigen Datenverarbeitung nach Art. 9 Abs. 2 Buchstabe a) bis j) DS-GVO lagen somit nicht vor. Der Mitarbeiterin lagen keine Einwilligungserklärungen nach Buchstabe a) der betroffenen Personen vor. Dies ergibt sich insbesondere aus den zahlreichen Beschwerden der betroffenen Personen beim Behördenleiter. Auch war die Erhebung und weitere Verwendung der auf oben genannter Liste enthaltenen personenbezogenen Daten schwerbehinderter Menschen der

Bundesbehörde für ihre Tätigkeit in der Dienststelle zum Tatzeitpunkt nicht erforderlich. Die Zulässigkeit einer Datenverarbeitung nach Art. 9 Abs. 2 Buchstabe b) DS-GVO muss von vornherein abgelehnt werden, da die Mitarbeiterin zum Tatzeitpunkt weder in der Personalverwaltung noch im Wahlvorstand tätig war.
Es lagen auch keine sonstigen Gründe zur Zulässigkeit der Erhebung der personenbezogenen Gesundheitsdaten mit der Liste schwerbehinderter Menschen nach Art. 9 Abs. 2 DS-GVO vor. Dies spielte jedoch keine Rolle, da bereits die Voraussetzungen aus Art. 9 Abs. 3 DS-GVO zur Verarbeitung personenbezogener Gesundheitsdaten nach Abs. 2 nicht vorlagen. Hiermit werden die datenschutzrechtlichen Schutzvorschriften für sensible Daten nach Art. 9 Abs. 1 DS-GVO mit den Berufsgeheimnissen verzahnt. Danach dürfen sensible Daten für Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin nur verarbeitet werden, wenn diese Daten von Fachpersonal oder unter dessen Verantwortung verarbeitet werden und dieses Fachpersonal dem Berufsgeheimnis unterliegt. Berufsgeheimnisse bestehen in Deutschland nach § 203 Abs. 1 Strafgesetzbuch (StGB) sowie nach der Heilberufsordnung für Ärzte, Apotheker oder Psychologen in Form des sogenannten Patientengeheimnisses beziehungsweise der beruflichen (ärztlichen) Schweigepflicht. Dieser Berufsgruppe gehörte die Mitarbeiterin nachweislich nicht an. Erlaubt ist zwar auch die Verarbeitung durch „eine andere Person“, wenn diese ebenfalls einer Geheimhaltungspflicht unterliegt. Dies ist zum Beispiel bei Rechtsanwälten, Steuerbevollmächtigten oder Angehörigen eines Unternehmens der privaten Versicherung oder einer Verrechnungsstelle (wie auch bei allen anderen in § 203 Abs. 1 StGB genannten Schweigepflichten) gegeben, wenn sie in ihrer beruflichen Funktion tätig werden (vergleiche Weichert in: Kühling/Buchner, DS-GVO/BDSG, 2. Auflage, Art. 9 Rn. 139, 144).
Im Ergebnis war festzustellen, dass die Mitarbeiterin die Liste schwerbehinderter Menschen der Bundesbehörde nicht im Zusammenhang mit ihren dienstlichen Aufgaben verarbeitete. Sie verarbeitete die personenbezogenen Daten aus der Wählerliste zum Zweck der Bekanntgabe des Beschlusses des Amtsgerichts. Im Laufe des Verfahrens berief sich die Mitarbeiterin darauf, dass die von ihr verarbeiteten personenbezogenen Daten öffentlich zugänglich gewesen seien. Dies trifft nicht zu. Aus den im Intranet der Bundesbehörde und auch im Telefonverzeichnis zugänglichen Daten der Bediensteten ergibt sich keine

Zugehörigkeit zur Gruppe der schwerbehinderten Menschen. Daneben existiert auch keine frei zugängliche Liste mit diesen Informationen. Vielmehr ist die Schwerbehinderteneigenschaft von Bediensteten ein Personalaktendatum, welches von der personalverwaltenden Dienststelle nur für Zwecke der Personalverwaltung oder -bewirtschaftung genutzt werden darf.
Nach Auffassung des TLfDI besteht auch bei der Datenverarbeitung durch die Versendung des Rundschreibens keine Rechtsgrundlage aus Art. 6 Abs. 1 Satz 1 DS-GVO. Da sich die Mitarbeiterin die personenbezogenen Daten aus der Wählerliste unbefugt beschafft hat, ist auch eine weitere Nutzung dieser Daten unzulässig. Zudem überwogen die schutzwürdigen Grundrechte und Grundfreiheiten der betroffenen Personen am Ausschluss der Verarbeitung. Gesundheitsdaten sind eine besondere Kategorie personenbezogener Daten nach Art. 9 Abs. 1 DS-GVO und gelten als sensible Daten. Darüber hinaus schafft Art. 9 DS-GVO für sensible Datenkategorien einen erhöhten Schutzbedarf. Von diesen Datenkategorien geht ein erhöhtes Diskriminierungsrisiko und damit die Gefahr einer Verletzung von Art. 21 der Grundrechtscharta ([GRCh] aus, vergleiche Art. 3 Abs. 3 Grundgesetz, Art. 14 Europäische Menschenrechtskonvention. Das besondere Schutzregime dient auch dem Schutz spezifischer Grundrechte, so speziell dem Recht der sozialen Sicherheit und dem Gesundheitsschutz aus Art. 34 und 35 GRCh. Gesundheitsdaten haben einen höchstpersönlichen Charakter und können für die Betroffenen identitätsstiftend sein. Dementsprechend hat der Missbrauch von Gesundheitsdaten ein großes Schadenspotenzial für die Betroffenen, individuell oder als Angehöriger einer Gruppe (vergleiche Weichert in: Kühling/Buchner, DS-GVO/BDSG, 2. Auflage, Art. 9. Rn. 14 bis 17). Es lag insoweit ein hoher Eingriff in das Grundrecht auf Datenschutz nach Art. 8 GRCH beziehungsweise auf das informationelle Selbstbestimmungsrecht der betroffenen Personen vor.
Die Mitarbeiterin legte form- und fristgerecht Einspruch gegen den Bußgeldbescheid beim TLfDI ein. Im Einspruchsverfahren prüft der TLfDI die mit dem Einspruch vorgetragenen Argumentationen. Danach kann der TLfDI das Bußgeldverfahren einstellen oder zur abschließenden Entscheidung an das Amtsgericht abgeben. Dort wird in einer öffentlichen Sitzung über den Verstoß und die Höhe des Bußgeldes verhandelt.
Das Einspruchsverfahren ist noch nicht abgeschlossen. Fortsetzung folgt!

3.9 Unberechtigte Abrufe von Patientendaten der Ex-Freundin

Abrufe zu Patientendaten ohne dienstlichen Grund stellen einen sogenannten Exzess dar. Damit ist die Weitergabe dienstlicher Informationen an die Privatperson – oft an sich selbst – zu eigenen Zwecken gemeint. Solche Verstöße gegen die DS-GVO können mit empfindlichen Geldbußen geahndet werden.

Eine Bürgerin beschwerte sich beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) über ihren Ex-Freund. Dieser war als psychologischer Psychotherapeut in einem städtischen Krankenhaus tätig und hatte ihre Patientendaten in der elektronischen Patientenakte abgerufen. Sie vermutete zunächst, dass er sich Zugriff auf die Behandlungsberichte verschafft hatte, um diese in einem Strafverfahren zu ihren Ungunsten einfließen zu lassen. Er hatte sie bereits als Patientin in einer anderen Klinik kennengelernt und war mit ihr eine Beziehung eingegangen. Dort war sie allerdings nicht seine Patientin gewesen. Dennoch wurde dem TLfDI im Laufe des Verfahrens bekannt, dass bereits in dieser Klinik unbefugte Abrufe zu den Patientendaten der damaligen Freundin stattgefunden hatten.
Nach Beendigung der Beziehung wurde ein Strafverfahren gegen den Therapeuten wegen sexueller Belästigung der Ex-Freundin eingeleitet. Als nun ein Abteilungswechsel im städtischen Krankenhaus bevorstand, rief er die Patientendaten in der elektronischen Patientenakte seiner Ex-Freundin ab. Zweck der Recherche war festzustellen, ob sich die Ex-Freundin in der neuen Abteilung des städtischen Krankenhauses in Behandlung befand. Der Therapeut wollte Berührungspunkte vermeiden und dadurch auch sicherstellen, dass der Behandlungserfolg seiner Ex-Freundin nicht beeinträchtigt wird. Aus der vorangegangenen Beziehung war dem Therapeuten wohl bekannt, dass sie sich bereits seit mehreren Jahren in eben dieser Abteilung des städtischen Krankenhauses in Behandlung befand.
Der TLfDI stellte fest, dass mit den zwei Abrufen aus der elektronischen Patientenakte Gesundheitsdaten im Sinne des Art. 4 Nr. 15 Datenschutz-Grundverordnung (DS-GVO) verarbeitet wurden. Mit dem Wissen, in welcher Abteilung des Krankenhauses die Ex-Freundin behandelt wurde, ergab sich für den psychologischen Psychotherapeuten zunächst ein zuordenbares, wenn auch zunächst abstraktes Krankheitsbild der Ex-Freundin. Für eine rechtmäßige Datenverarbeitung

nach Art. 5 Abs. 1 Buchstabe a) DS-GVO müssen personenbezogene Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden. Zudem untersagt Art. 9 Abs. 1 DS-GVO die Verarbeitung personenbezogener Gesundheitsdaten einer natürlichen Person. Eine Verarbeitung von Gesundheitsdaten ist nur unter den engen Voraussetzungen des Art. 9 Abs. 2 Buchstabe a) bis j) DS-GVO zulässig.
Diese lagen im hiesigen Verfahren nicht vor. Eine Einwilligung der Ex-Freundin zu den Abrufen aus der elektronischen Patientenakte war nicht gegeben. Ebenso wenig waren diese Abrufe für die damalige Tätigkeit des Therapeuten im städtischen Krankenhaus erforderlich. Die Ex-Freundin war keine Patientin aus dem Fachgebiet des Therapeuten. Damit war er kein Behandler der Ex-Freundin. Es lagen auch keine sonstigen Gründe zur Zulässigkeit oben genannter Abrufe vor. Da dem Therapeuten aus der vorangegangenen Beziehung bereits bekannt war, dass sich die Ex-Freundin in seiner neuen Abteilung des städtischen Krankenhauses in Behandlung befand, waren die Abrufe aus der elektronischen Patientenakte von vornherein nicht erforderlich. Es wäre ihm möglich gewesen, den potenziellen neuen Arbeitgeber zum Tatzeitpunkt auch ohne die beiden Abrufe über den Rechtsstreit mit der Ex-Freundin zu informieren und bestehende Bedenken mit der Tätigkeit in der neuen Abteilung vorzutragen. Folglich hätte der Arbeitgeber die gleichen Vorkehrungen zum Schutz des Behandlungserfolgs der Ex-Freundin treffen können.
Jedenfalls überwog des Recht auf informationelle Selbstbestimmung gemäß Art. 6 Abs. 2 Thüringer Verfassung der Ex-Freundin die Interessen des Therapeuten an den Abrufen aus der elektronischen Patientenakte. Art. 9 DS-GVO dient mit dem Schutz der Intimsphäre der Abwehr von Angriffen auf den Kernbereich privater Lebensgestaltung. Mit den Verstößen gegen Art. 9 DS-GVO durch die Abrufe verletzte der Therapeut die Intimsphäre seiner Ex-Freundin. Der Grundrechtseingriff in das Persönlichkeitsrecht war hoch zu bewerten. Die Abfragen erfolgten ohne Information an die Ex-Freundin und in zugriffsgesicherten IT-Systemen des städtischen Krankenhauses und unter Ausnutzung der beruflichen Stellung als psychologischer Psychotherapeut. Die Ex-Freundin fühlte sich keinesfalls durch den beruflichen Wechsel geschützt. Vielmehr wurde durch den Interessenkonflikt der Behandlungserfolg der Patientin stark beeinträchtigt, da die

Therapeutin der Patientin nun durch den Ex-Freund als Kollegen voreingenommen war. Die Therapie konnte in dieser Klinik nach hiesigem Kenntnisstand nicht fortgesetzt werden.
Im Ergebnis war festzustellen, dass schon die Weitergabe dienstlicher Informationen an die Privatperson – an sich selbst – nicht mit der Datenschutz-Grundverordnung vereinbar ist. Zudem galt im städtischen Krankenhaus eine Dienstvereinbarung, die es untersagte, Einsicht in die Daten von Patienten oder Beschäftigten zu nehmen, die nicht im Zusammenhang mit den dienstlichen Aufgaben stehen.
Der TLfDI erließ gegenüber dem Therapeuten nach Art. 83 Abs. 5 Buchstabe a) DS-GVO einen rechtskräftigen Bußgeldbescheid mit einer Geldbuße in Höhe von 600 Euro. Bei der Bemessung der Geldbuße wurden vorsätzliches Handeln sowie die Eingriffsintensität in das Persönlichkeitsrecht der Ex-Freundin verschärfend berücksichtigt. Die Informationen wurden unter Ausnutzung der beruflichen Stellung gewonnen. Unter Würdigung der bereits bei einem ehemaligen Arbeitgeber unbefugt vorgenommenen Abrufe zu Patientendaten der Ex-Freundin erschien eine niedrigere Geldbuße nicht ausreichend abschreckend für die Zukunft.
Zusätzlich musste nach § 49a Abs. 2 des Gesetzes über Ordnungswidrigkeiten in Verbindung mit § 14 Abs. 1 Nr. 4b) Einführungsgesetz zum Gerichtsverfassungsgesetz von Amts wegen die rechtskräftig verhängte Geldbuße an die zuständige Psychotherapeutenkammer gemeldet werden. Die Bußgeldentscheidung des TLfDI kann im Disziplinarverfahren ohne nochmalige Prüfung zugrunde gelegt werden, § 16 Abs. 2 Thüringer Disziplinargesetz.

3.10 Unrechtmäßige Beschaffung einer Geburtsurkunde beim Meldeamt

Nach einer Adoption dürfen den leiblichen Verwandten gemäß § 1758 BGB ohne Zustimmung der Adoptiveltern und des Adoptierten keine Auskünfte erteilt werden. Wenn personenbezogene Daten aus Geburtsurkunden unrechtmäßig erhoben werden, ist jede weitere Verarbeitung dieser personenbezogenen Daten in der Folge ebenfalls unrechtmäßig.

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichte eine Beschwerde eines Adoptivva-

ters. Darin ging es um eine unbefugte Datenerhebung seitens der leiblichen Mutter seiner Tochter. Diese hatte beim Standesamt des Geburtsortes des Kindes vorgesprochen und zwei einfache Geburtsurkunden der Tochter verlangt, welche ihr vom Standesbeamten gegen eine Gebühr ausgestellt wurden. Eine einfache Geburtsurkunde ist eine Bescheinigung der Geburt und enthält Angaben zu den Eltern. Da das Kind adoptiert worden war, waren in den Geburtsurkunden die personenbezogenen Daten der Adoptiveltern enthalten. Auf Grundlage der ausgestellten Geburtsurkunden erfolgte sowohl eine Kenntniserlangung der Namen der Adoptiveltern als auch eine Kontaktaufnahme der leiblichen Mutter mit deren Tochter. Weiterhin übermittelte die Mutter die personenbezogenen Daten an die Stiefschwester, welche ebenfalls Kontakt mit dem Adoptivvater über das soziale Netzwerk Facebook aufnahm.

Zunächst war zu prüfen, aus welchen Gründen und auf welcher Rechtsgrundlage die Herausgabe der beiden einfachen Geburtsurkunden basierte. Den leiblichen Verwandten dürfen gemäß § 1758 Bürgerliches Gesetzbuch (BGB) keine Auskünfte erteilt werden, wenn nicht die Adoptiveltern und der Adoptierte zugestimmt haben. Nach § 1626 Abs. 1 BGB umfasst die elterliche Sorge die Pflicht und das Recht, für das minderjährige Kind zu sorgen. Sie beinhaltet die Personen- und Vermögenssorge sowie die Vertretung des Kindes. Minderjährige sind alle Kinder unter 18 Jahren. Das bedeutet, so lange das adoptierte Kind minderjährig ist, obliegt die Zustimmung den Sorgeberechtigten. Das Sorgerecht liegt hier bei den Adoptiveltern. In diesem Fall lagen weder die Einwilligung der Adoptiveltern noch die des adoptierten Kindes vor. Im Rahmen eines Amtshilfeersuchens trug die zuständige Stadtverwaltung vor, dass es sich bei der Ausstellung der Geburtsurkunde durch den Standesbeamten um ein Augenblickversagen („Blackout“) gehandelt habe. Der Betroffene betonte, dass die Voraussetzungen und das einzuhaltende Verfahren bei der Ausstellung von Geburtsurkunden bestens bekannt seien. Einen Antrag und die dazugehörige Begründung der Mutter zur Ausstellung oben genannter Geburtsurkunden sowie weiterer Schriftverkehr in dieser Sache konnten dem TLfDI allerdings nicht vorgelegt werden. Vielmehr wurde darauf verwiesen, dass die Geburtsurkunden im Rahmen einer mündlichen Vorsprache der leiblichen Mutter auf der Grundlage ihres mündlichen Antrages sowie ihres sonstigen Vorbringens ausgestellt und übergeben wurden. In Ergänzung der Geburtsurkunden übermittelte die Stadtverwaltung einen Nachweis über die gezahlten Gebühren in

Höhe von 20 Euro für die Ausstellung der beiden einfachen Geburtsurkunden. Das gegen den Standesbeamten eingeleitete Ordnungswidrigkeitenverfahren musste im Ergebnis eingestellt werden. Nach § 61 Abs. 1 Nr. 1 Thüringer Datenschutzgesetz (ThürDSG) handelt ordnungswidrig, wer entgegen den Bestimmungen der Datenschutz-Grundverordnung (DS-GVO), des ThürDSG oder einer anderen Rechtsvorschrift über den Schutz personenbezogener Daten solche Daten übermittelt. Diese Norm verlangt zur Tatbestandverwirklichung vorsätzliches Handeln, welches bei dem Standesbeamten nicht feststellbar war. Der Standesbeamte trug im Anhörungsverfahren vor, weder Angaben zum mündlichen Vortrag der leiblichen Mutter noch zur Rechtsgrundlage der Übermittlung oben genannter Geburtsurkunden machen zu können. Aufgrund der Vielzahl an Besuchern pro Tag und der bereits verstrichenen Zeitspanne könne er sich nicht an den Vorgang einer unberechtigten Herausgabe von zwei Geburtsurkunden erinnern. Weiterhin trug er vor, dass die Möglichkeit der Vorlage einer Vollmacht einer bezugsberechtigten Person ohne deren Kenntnis bestehe. Da dieser Vorgang seiner arbeitstäglichen Praxis widerspreche, könne sich der Betroffene den Sachverhalt nicht erklären. Der Standesbeamte ließ im Ergebnis das zu verlangende Maß an Sorgfalt außer Acht. Da es für die Verfolgung einer Ordnungswidrigkeit bereits am Vorsatz fehlte, lag ein Verfahrenshindernis vor. Das Ordnungswidrigkeitenverfahren wurde nach § 170 Abs. 2 Satz 1 Strafprozessordnung (StPO) in Verbindung mit § 46 Abs. 1 Satz 2 des Gesetzes über Ordnungswidrigkeiten (OWiG) aus rechtlichen Gründen eingestellt.
Gleichzeitig wurde gegen die Mutter nach § 14 OWiG ein Ordnungswidrigkeitenverfahren wegen unbefugter Datenerhebung und Übermittlung eingeleitet. Indem sie die Geburtsurkunden angefordert hatte, beteiligte sie sich an der Ordnungswidrigkeit und handelte danach selbst ordnungswidrig. Ihr wurde im Ordnungswidrigkeitenverfahren weiterhin vorgeworfen, jeweils die Namen sowie die Geburtsnamen der Adoptiveltern erhoben zu haben. Damit verarbeitete die leibliche Mutter die Geburtsurkunden ohne Rechtsgrundlage. Auch nach mehrmaliger schriftlicher Aufforderung durch die zuständige Stadtverwaltung gab sie die zwei Geburtsurkunden nicht an diese zurück. Ferner übermittelte die Mutter die personenbezogenen Daten der Adoptiveltern an die Stiefschwester des Kindes, welche in der Folge über Facebook jeweils Kontakt zum adoptierten Kind sowie zum Adoptivvater aufnahm.

Nach Art. 5 Abs. 1 Buchstabe a) DS-GVO müssen personenbezogene Daten auf rechtmäßige und in einer für die oben genannten betroffenen Personen nachvollziehbaren Weise verarbeitet werden. In Art. 6 Abs. 1 Satz 1 DS-GVO ist ein Verbot mit Erlaubnisvorbehalt geregelt. Danach ist eine Datenverarbeitung nur unter den dort genannten Voraussetzungen zulässig. Nach Art. 6 Abs. 1 Satz 1 Buchstabe a) DS-GVO in Verbindung mit § 1747 BGB wäre die Verarbeitung rechtmäßig, wenn das adoptierte Kind oder die Adoptiveltern ihre Einwilligung zur Verarbeitung ihrer personenbezogenen Daten erteilt hätten. Nach § 1747 BGB dürfen Tatsachen, die geeignet sind, die Annahme und ihre Umstände aufzudecken ohne Zustimmung des Annehmenden und des Kindes nicht offenbart oder ausgeforscht werden, es sei denn, dass besondere Gründe des öffentlichen Interesses dies erfordern. Eine solche Einwilligung lag der leiblichen Mutter zu keinem Zeitpunkt vor. Auch waren besondere Gründe des öffentlichen Interesses nicht ersichtlich. Jedenfalls hatte sich die Mutter zu keiner Zeit auf diese berufen und dargelegt.

Damit verarbeitete die Mutter mithin seit mehr als zwei Jahren vorsätzlich unbefugt die personenbezogenen Daten des Kindes sowie von dessen Adoptiveltern. Da sie die Geburtsurkunden unrechtmäßig besaß und aufbewahrte, waren diese an die Stadtverwaltung herauszugeben. Mehrmaligen Aufforderungen der Stadtverwaltung kam die Mutter nicht nach.

Diese weitere Übermittlung der personenbezogenen Daten aus den Geburtsurkunden an die Stiefschwester des adoptierten Kindes unterliegt ebenfalls den Vorgaben des Art. 6 Abs. 1 Satz 1 DS-GVO. Da schon die Erhebung der beiden Geburtsurkunden unzulässig erfolgte, war auch die Übermittlung dieser Daten unzulässig. Der einzig in Frage kommende Erlaubnistatbestand des Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO ist nicht einschlägig. Hierfür fehlt es nicht nur an der in § 1747 BGB geforderten Einwilligung, sondern auch am berechtigten Interesse. In jedem Fall aber überwogen die Grundrechte und Grundfreiheiten der betroffenen Personen, insbesondere in Ausformung ihres informationellen Selbstbestimmungsrechts. Die Eingriffsintensität in die Grundrechte und Grundfreiheiten der betroffenen Personen ist hoch. Die Übermittlung der Daten an die Stiefschwester erfolgte ohne Rechtsgrundlage und war als unzulässig zu bewerten.

Auch war die anschließende Kontaktaufnahme der Mutter über das soziale Netzwerk mit dem adoptierten Kind rechtswidrig, da schon die

Datenerhebung unzulässig war. Die Mutter erklärte dem adoptierten Kind über Facebook, dass sie von seiner Familie adoptiert wurde und sie die leibliche Mutter sei. Die Mutter hatte die personenbezogenen Daten aus den Geburtsurkunden unrechtmäßig erhoben. Jede weitere Verarbeitung dieser personenbezogenen Daten ist in der Folge ebenfalls unrechtmäßig. Zusätzlich fehlte es an der einzig in Betracht kommenden Rechtsgrundlage des Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO. Hier überwogen die Grundrechte und Grundfreiheiten des Kindes und der Adoptiveltern. Die Mutter griff in deren Recht auf informationelle Selbstbestimmung ein. Das Adoptivkind und die Adoptiveltern wünschten selbstbestimmt zu entscheiden, ob und wann eine Kontaktaufnahme zu den leiblichen Eltern und gegebenenfalls Geschwisterkindern erfolgt. Gegen die leibliche Mutter wurde ein Bußgeld in Höhe von 800 Euro festgesetzt. Die Familie war nach den Kontaktaufnahmen emotional stark aufgewühlt. Die Familie wünschte sich, dass das Kind selbst entscheidet, ob und wann es Kontakt zur Mutter aufnimmt. Zu diesem Zeitpunkt war es noch nicht bereit dazu. Daher wäre eine niedrigere Geldbuße unverhältnismäßig und nicht ausreichend abschreckend für die Zukunft gewesen.

3.11 Videoüberwachung im Einkaufszentrum

Videoüberwachungen in großen Einkaufszentren werden durch die Aufsichtsbehörde in einer Einzelfallbetrachtung bewertet. Insbesondere wird beim Einsatz einer Videoüberwachung zur Gefahrenabwehr in einem Einkaufscenter nicht von vornherein eine abstrakte Gefahrenlage hinsichtlich etwaiger Eigentumsdelikte und Delikte gegen das Leben und die Gesundheit angenommen. Die Betreiber beziehungsweise Eigentümer der Einkaufszentren sollten daher genau darlegen können, woraus sich eine konkrete Gefährdung für ihr Einkaufszentrum ergibt und die Zwecke mittels entsprechender Nachweise vor der Installation einer Videoüberwachung ausreichend dokumentieren.

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) erhielt Kenntnis über eine betriebene Videoüberwachung in einem Einkaufszentrum. Dort sollten unter anderem die gesamten Ladenpassagen, Restaurantbereiche und die öffentlichen Bereiche des davor befindlichen Platzes überwacht werden.
Daraufhin wandte sich der TLfDI mit einem Auskunftsverlangen zunächst an das Betreiberunternehmen des Einkaufszentrums. Dieses

teilte mit, dass insgesamt 38 Videokameras seitens der Eigentümerin betrieben werden. Die Kameras erfassten die Ladenstraßen im Einkaufszentrum, die Eventetage mit entsprechenden Gasttischbereichen sowie den kompletten öffentlich zugänglichen Platz und andere öffentliche Bereiche. Als Zwecke wurden im Laufe des Verwaltungsverfahrens unter anderem die Wahrnehmung des Hausrechts, der Schutz von Leib, Leben und Gesundheit und Schutz vor Beschädigungen an den Schaufenstern beziehungsweise Fassaden (Graffiti et cetera) benannt. Auch die Vermeidung von Straftaten und Ermöglichung der Strafverfolgung wurden als Zweck angegeben. Zudem sei das Einkaufscenter Sammelpunkt der Kriminalität, sodass durch die Anonymität und die Masse der einkaufenden Kunden ein Gefühl der Sicherheit für potentielle Täter entstünde und Taschendiebstähle nicht auszuschließen seien. Ferner sollten die ausländischen Kunden vor rechtsextremistischen Übergriffen geschützt werden.
Art. 6 Abs. 1 Satz 1 Buchstabe f) Datenschutz-Grundverordnung (DS-GVO) ist die einzige Norm nach der sich die Rechtmäßigkeit der hier vorgenommenen Verarbeitung von personenbezogenen Daten mittels der Videokameras richtet. Das Bundesverwaltungsgericht hat bereits kurz nach Geltung der Datenschutz-Grundverordnung in seinem Urteil vom 27. März 2019 (Az.: 6 C 2.18, Rn. 47) klargestellt, dass § 4 Bundesdatenschutzgesetz (BDSG) für nicht-öffentliche Kamerabetreiber, also Unternehmen und Privatpersonen, nicht anwendbar ist. Eine Öffnungsklausel in der DS-GVO existiert in diesem Bereich nicht, sodass der nationale Gesetzgeber keinerlei Regelungsbefugnis für diesen Bereich innehatte. Dennoch wird die Wertung des § 4 Abs. 3 Satz 2 BDSG, insbesondere der Schutz von Leben, Gesundheit oder Freiheit der sich in einem Einkaufszentrum aufhaltenden Personen, von den Aufsichtsbehörden im Rahmen der Interessenabwägung berücksichtigt.
Die Prüfung der Zulässigkeit einer Videoüberwachung von nicht-öffentlichen Stellen richtet sich also nach Art. 6 Abs. 1 Buchstabe f) DS-GVO. Danach ist die Verarbeitung nur rechtmäßig, soweit die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

Soll die Videoüberwachung wie in diesem Fall zur Gefahrenabwehr eingesetzt werden, kann dann von einem berechtigten Interesse ausgegangen werden, wenn eine konkrete Gefährdungslage nachgewiesen wurde. Dies kann durch Nennung von Vorkommnissen in der Vergangenheit oder Vorlage etwaiger Strafanzeigen geschehen. Ausnahmsweise kann auch eine abstrakte Gefahrenlage angenommen werden, wenn eine Situation vorliegt, die nach der Lebenserfahrung typischerweise gefährlich ist. Insoweit ist der TLfDI hinsichtlich etwaiger Beschädigungen und Schmierereien aufgrund des großen Gebäudekomplexes des Einkaufszentrums von einer abstrakten Gefährdungslage ausgegangen. Für die übrigen Zwecke wurde ein Nachweis über das Vorliegen einer Gefährdungslage gefordert. Dies ist während des Verwaltungsverfahrens nicht in ausreichendem Maße geschehen. Es wurden lediglich allgemeine Darlegungen gemacht, welche die Annahme für eine Terrorgefahr oder überhaupt eine Gefahr für Leib und Leben der Kunden nicht begründen konnte. Auch eine übermäßige Anzahl an Übergriffen oder Diebstählen im Bereich des Einkaufszentrums wurde nicht dargelegt. Auch wenn es vermehrt zu Taschendiebstählen gekommen wäre, ist es Sache der Besucher, auf sich und das Eigentum aufzupassen. Insoweit besteht im öffentlichen Raum seitens der Bürger beziehungsweise Unternehmen keine allgemeine Berechtigung überall dort, wo möglicherweise Straftaten vorkommen können, eine Videoüberwachung zu installieren. Die seitens der Kamerabetreiberin genannte Strafverfolgung kann kein berechtigtes Interesse darstellen, da dies den Sicherheitsbehörden beziehungsweise Strafverfolgungsbehörden obliegt und nicht einem privaten Kamerabetreiber. Lediglich Beweissicherungsinteressen für etwaige Regressansprüche sind hier zu berücksichtigen.
Im Rahmen der Erforderlichkeit einer Videoüberwachung ist insbesondere auch der räumliche Umfang der Überwachung anhand der genannten Zwecke zu überprüfen. Im vorliegenden Fall wurden insbesondere die Kameras, welche die öffentlichen Bereiche wie zum Beispiel Straßen, Gehwege und den kompletten Platz überwachen für nicht erforderlich gehalten. Da es dem Kamerabetreiber insbesondere um die Feststellung von Beschädigungen an der Fassade und den Schaufenstern ging, wurde hier die Einschränkung des videoüberwachten Bereichs auf die Hauswand (beziehungsweise maximal einen Meter von der Hauswand entfernt) gefordert (AG Berlin-Mitte, Urteil vom 18. Dezember 2003, Az.: 16 C 427/02).

Weiterhin fordert Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO eine Interessenabwägung mit den schutzwürdigen Interessen der betroffenen Personen. Hierbei sind auch die vernünftigen Erwartungen der betroffenen Personen zu berücksichtigen. Ob vernünftige Erwartungen bestehen, beurteilt sich danach, ob die Videoüberwachung in bestimmten Bereichen der Sozialsphäre typischerweise akzeptiert ist oder eventuell wegen eines Beziehungszusammenhangs sogar verlangt wird oder nicht. Im vorliegenden Fall wurde die flächendeckende Überwachung der Ladenpassagen als unzulässig angesehen. Gerade in öffentlich zugänglichen Räumen, in denen sich Menschen typischerweise länger aufhalten und/oder miteinander kommunizieren, ist die Schutzbedürftigkeit der betroffenen Personen regelmäßig sehr hoch. In diesen Bereichen können die betroffenen Personen erwarten, überwachungsfreie Räume vorzufinden. Zwar dienen die Ladenstraßen einerseits als Durchgangspassage, andererseits aber sollen die Besucherinnen und Besucher durch die Schaufensterauslagen und gegebenenfalls die vor den Geschäften aufgestellten Verkaufsstände zum Stehenbleiben und Verweilen angeregt werden. Gleiches gilt für die dort befindlichen Sitz- und Ruhebereiche, insbesondere die Gastronomiebereiche in der Eventetage. Eine ständige Überwachung in diesen Bereichen, die zu einer längeren Aufenthaltsdauer und zur Entfaltung sozialer Kommunikation einladen, stellt eine erhebliche Beeinträchtigung der Persönlichkeitsrechte der betroffenen Personen dar, die durch die bloße Möglichkeit des Nachweises etwaiger Diebstähle oder ähnlicher Straftaten nicht aufgewogen werden kann.
Da seitens der Verantwortlichen während des Verwaltungsverfahrens trotz mehrmaliger Hinweise des TLfDI keinerlei Änderungen hinsichtlich der Videoüberwachung vorgenommen wurden, erließ dieser schließlich einen Bescheid nach Art. 58 Abs. 2 DS-GVO. Darin wurde unter anderem das Überwachen der Ladenpassagen und der öffentlichen Bereiche untersagt beziehungsweise die Einschränkung auf die Hausfassade gefordert. Das Verfahren ist derzeit am Verwaltungsgericht Weimar anhängig.

3.12 Bespitzelung durch TLfDI bei Verlangen einer Auskunft?

Der TLfDI ist auch bei Videoüberwachungen von Privatpersonen berechtigt, eine Auskunft zu verlangen, um seinen Aufgaben nach Art. 57 DS-GVO nachkommen zu können. Ob letztendlich das Datenschutzrecht zur Anwendung kommt, kann erst durch Beantwortung

des Auskunftkunftsverlangens gegenüber dem TLfDI beurteilt werden. Zudem ist ein Auskunftsverlangen vollständig, richtig und aktuell – im jeweiligen zeitlichen Zusammenhang – zu beantworten und nachvollziehbar darzustellen (ThürOVG, Beschluss vom 19. März 2021, Az.: 3 EO 423/20, Rn. 47).

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) erhielt durch eine Beschwerde Kenntnis von einer Videoüberwachung, welche unter anderem auf das Grundstück der in dem Haus des Grundstückseigentümers lebenden Beschwerdeführerin gerichtet sein sollte. Die Kamerabetreiberin hatte zunächst nur eine Videokamera an ihrem privaten Einfamilienhaus angebracht. Im Laufe des Verwaltungsverfahrens wurde eine weitere Kamera an der Dachrinne des Gebäudes installiert.
Zunächst wurde seitens des TLfDI eine Auskunft nach Art. 58 Abs. 1 Buchstabe a) Datenschutz-Grundverordnung (DS-GVO) in Verbindung mit § 40 Abs. 4 Bundesdatenschutzgesetz seitens der Verantwortlichen gefordert. Danach ist die Aufsichtsbehörde befugt, den Verantwortlichen anzuweisen, alle Informationen bereitzustellen, die für die Erfüllung ihrer Aufgaben erforderlich sind. Daneben wurde auch eine Akte zu einem zivilgerichtlichen Verfahren beigezogen, in dem die erste angebrachte Videokamera bereits Gegenstand war. Aus der Akte selbst ergaben sich jedoch keine ausreichenden Informationen, welche eine datenschutzrechtliche Bewertung der Kamera möglich gemacht hätten. Zudem wurde das Verfahren mit einem Vergleich beendet. Die Beschwerdeführerin war nicht beteiligt an diesem Verfahren.
Die Kamerabetreiberin wies das Auskunftsersuchen des TLfDI unter Hinweis auf das bereits geführte und beendete zivilgerichtliche Verfahren und die darin enthaltenen Informationen zurück. Ferner würde nur das eigene Grundstück überwacht, sodass die Haushaltsausnahme nach Art. 2 Abs. 2 Buchstabe c) DS-GVO greife und der TLfDI keine Auskunft fordern dürfe. Nach nochmals mehrmaliger Aufforderung zur Beantwortung des Auskunftsverlangens teilte diese daraufhin mit, dass es sich um eine einfache Kamera ohne Mikrofon und Zoomfunktion mit temporärer Aufzeichnung handele, die nur das eigene Grundstück erfasse. Nachweise in Form von Kameraaufnahmen wurden nicht vorgelegt. Hinsichtlich der zweiten Videokamera erfolgte keine Beantwortung des ergänzend gestellten Auskunftsverlangens. Der TLfDI erließ daraufhin einen kostenpflichtigen Bescheid, in dem die

Kamerabetreiberin zur Beantwortung der seitens des TLfDI gestellten Fragen zur Beurteilung der Videoüberwachung verpflichtet wurde.
Dieser Bescheid beschäftigte dann das Verwaltungsgericht und das Thüringer Oberverwaltungsgericht im Eil- und im Klageverfahren, da die Verantwortliche gegen den Bescheid mittels Klage und im einstweiligen Rechtsschutzverfahren sowie im Beschwerdeverfahren vor dem Thüringer Oberverwaltungsgericht vorging. In dem gerichtlichen Verfahren wurde der bisherige Vortrag aus dem Verwaltungsverfahren weitestgehend wiederholt. Die Kamerabetreiberin machte geltend, dass dem TLfDI alle Informationen bereits vor Erlass des Bescheides vorlagen und dieser sich aus den entsprechenden Schreiben und aus der Gerichtsakte alle Antworten zusammenstellen könne. Zudem sei er an den zivilgerichtlichen Vergleich gebunden und habe kein Recht mehr die Videoüberwachung zu prüfen, auch aufgrund der Tatsache, dass hier kein Datenschutzrecht zur Anwendung gelange. Weiter wurden während des Gerichtsverfahrens widersprüchliche Angaben bezüglich der Kameras gemacht.
Im Beschwerdeverfahren führte das Thüringer Oberverwaltungsgericht in seinem Beschluss vom 19. März 2021 (Az.: 3 EO 423/20) letztendlich zur Erforderlichkeit einer zu erteilenden Auskunft gegenüber dem TLfDI unter Beachtung des Auskunftsverweigerungsrechts aus, dass es nach Art. 57 DS-GVO die Aufgabe der Aufsichtsbehörde sei, eine Beschwerde im angemessenen Umfang zu untersuchen. Das gestellte Auskunftsverlangen diene der Sachverhaltsermittlung, um einen etwaigen Verstoß abstellen oder überhaupt die Zuständigkeit des TLfDI feststellen zu können. Insoweit dürfe der TLfDI nicht auf den Inhalt einer zivilgerichtlichen Akte, aus der sich in diesem Fall keine ausreichenden Informationen zur Funktionsweise der Kamera ergaben, verwiesen werden. Auch sei dieser nicht an die Entscheidung aus dem Vergleich im zivilgerichtlichen Verfahren gebunden, da die Beschwerdeführerin nicht Partei dieses Rechtsstreits war. Auch müsse sich der TLfDI die Informationen aus verschiedenen Verfahren und vorgelegten Unterlagen nicht zusammensuchen, um eine Beantwortung des gestellten Auskunftsverlangens zu erzielen. Hierzu führte das Gericht aus: „*Wie bereits aufgezeigt geht die Auskunftspflicht der Antragstellerin dahin, dem Auskunftsverlangen des Antragsgegners vollständig, richtig und aktuell sowie nachvollziehbar zu entsprechen. Sowohl unter Vollständigkeitsgesichtspunkten, jedenfalls aber unter den Aspekten der Aktualität und Nachvollziehbarkeit kann der Antrags-*

gegner und das Verwaltungsgericht hier nicht auf Dokumente und Unterlagen verwiesen werden, die im Laufe eines längeren Verwaltungs- und anschließenden Gerichtsverfahrens zusammengetragen wurden, unterschiedliche Zustände zu unterschiedlichen Zeitpunkten oder für unterschiedliche Zeiträume beschreiben und Informationen nicht vollständig enthalten sind oder sich nur in Zusammenschau sukzessiv bereitgestellter Teilinformationen ergeben. Ein Auskunftsverlangen ist daher vollständig, richtig und aktuell – im jeweiligen zeitlichen Zusammenhang zu beantworten und nachvollziehbar darzustellen. Insoweit ist die bisherige Art und Weise, in der die Antragstellerin dem Antragsgegner Informationen bereitstellen will, offenkundig und rechtserheblich defizitär."

Das Thüringer Oberverwaltungsgericht hat hier in seiner Entscheidung nochmals die Befugnisse des TLfDI gestärkt und die Reichweite der Auskunftspflicht nach der Datenschutz-Grundverordnung dargelegt. Die vollständige Entscheidung ist bei JURIS und auch auf der Webseite www.landesrecht.thüringen.de veröffentlicht beziehungsweise abrufbar.

Die erforderliche Auskunft wurde erst in dem noch zu entscheidenden Klageverfahren vor dem Verwaltungsgericht Weimar erteilt. Insoweit konnte aufgrund der gemachten Angaben zwischenzeitlich das Verwaltungsverfahren abgeschlossen werden. Auf Grundlage der im Gerichtsverfahren gemachten Auskünfte konnte eine Verletzung der Rechte der Beschwerdeführerin nicht festgestellt werden, da die Kameraaufnahmen nur das eigene Grundstück der Kamerabetreiberin zeigten. Der TLfDI musste daher keine weiteren Abhilfemaßnahmen gegenüber dieser ergreifen.

3.13 Videoüberwachung in einem Autohaus

Die Videoüberwachung eines Autohauses während der Geschäftszeiten ist nicht ohne Weiteres zulässig. Zwar werden im Innen- und Außenbereich durch die zu verkaufenden Fahrzeuge erhebliche Warenwerte ausgestellt. Jedoch ist auch hier im Rahmen des berechtigten Interesses des Betreibers eine konkrete Gefährdung für dessen Rechtsgüter während der Geschäftszeiten nachzuweisen.

Dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) wurde durch eine Beschwerde bekannt,

dass auf dem Gelände eines Autohauses eine Videoüberwachung betrieben werden würde, welche unter anderem die öffentliche Straße und Gehwege miterfasst. Daraufhin wandte sich der TLfDI an das Betreiberunternehmen des Autohauses. Es wurde mitgeteilt, dass auf dem Gelände tatsächlich insgesamt sechs Videokameras betrieben werden. Ein Teil der Kameras überwachte das Außengelände des Autohauses mit den darauf befindlichen Neu- und Gebrauchtfahrzeugen. Auf den Kameraaufnahmen waren im Hintergrund die gesamte öffentliche Straße, sowie gegenüberliegende Gebäude erkennbar. Im Innenbereich des Autohauses wurden ein Teil der Ausstellung und ein Bedientisch für Kundengespräche überwacht. Die Aufnahmen der Kameras wurden 14 Tage gespeichert.
Die Zulässigkeit der seitens des Unternehmens betriebenen Videoüberwachung richtet sich vorliegend nach Art. 6 Abs. 1 Satz 1 Buchstabe f) Datenschutz-Grundverordnung (DS-GVO). Danach ist die Verarbeitung nur rechtmäßig, soweit die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.
Als Zweck für die Videoüberwachung wurde die Wahrnehmung des Hausrechts benannt. Weiterhin sollte die Videoüberwachung der Gefahrenabwehr dienen.
Ein berechtigtes Interesse kann ideeller, wirtschaftlicher oder rechtlicher Natur sein. Die Wahrnehmung des Hausrechts beinhaltet die Eigensicherung der Liegenschaften, das heißt, hierdurch sollen Schäden an dem überwachten Gebäude und den sich darin aufhaltenden Personen oder das Betreten durch unbefugte Personen verhindert beziehungsweise zur Beweissicherung dokumentiert werden. Bei Geschäftsbetrieben stellt die Wahrung des Hausrechts nur außerhalb der Geschäftszeiten ein berechtigtes Interesse zum Betreiben von Videokameras dar, da innerhalb der Geschäftszeiten durch anwesendes Personal das entsprechende Hausrecht ausgeübt werden kann. Sofern die Videoüberwachung zur Gefahrenabwehr dient, zum Beispiel, um vor Einbrüchen, Diebstählen oder Vandalismus zu schützen, kann darin grundsätzlich ein berechtigtes Interesse gesehen werden, sofern hier eine konkrete Gefahrenlage seitens des Verantwortlichen nachgewiesen wird. Hierbei sind konkrete Tatsachen als Nachweis zu fordern, aus denen sich die Gefährdung ergibt. Dies kann durch Nennung von

Beschädigungen, besonderen Vorfällen in der Vergangenheit oder durch Nennung von polizeilichen Tagebuchnummern beziehungsweise staatsanwaltschaftlichen Aktenzeichen erfolgen. Es ist hier grundsätzlich Sache des Verantwortlichen (Kamerabetreiber) darzulegen, warum er eine Videoüberwachung für erforderlich hält. Dies ist sorgfältig mittels entsprechender Nachweise zu dokumentieren. Bereits vor der Installation einer Anlage sollte eine solche Dokumentation mit entsprechend getroffenen Maßnahmen zum Schutz des Objektes erfolgen. Seitens des Autohausbetreibers wurden hier diverse Vorfälle wie Diebstähle und Sachbeschädigungen an den abgestellten Fahrzeugen benannt und auch entsprechende Nachweise vorgelegt. Diese Vorfälle fanden jedoch nachts oder an den Wochenenden statt.
Im Rahmen der Erforderlichkeit einer Videoüberwachung ist neben der Geeignetheit auch der räumliche und zeitliche Umfang zu prüfen. Die Videoüberwachung im vorliegenden Fall war zwar geeignet, um etwaige Beweise zu sichern, jedoch musste aufgrund der ausschließlich außerhalb der Geschäftszeiten stattgefundenen Straftaten beziehungsweise Vorfälle die Erforderlichkeit der Überwachung während der Geschäftszeiten abgelehnt werden. Eine Gefährdungslage für die Liegenschaft während der Geschäftszeiten konnte seitens des verantwortlichen Unternehmens gegenüber dem TLfDI nicht dargelegt werden. Auch die Überwachung der öffentlichen Straße und der angrenzenden Gehwege war für die hier genannten Zwecke nicht erforderlich, sodass diese von der Überwachung auszunehmen war.
Ferner wurde die Dauer der Speicherung der Videoaufnahmen von 14 Tagen seitens des TLfDI für unzulässig gehalten. Die DS-GVO enthält zwar keine konkret auf die Speicherdauer bezogene Regelung. Entsprechend Art. 17 Abs. 1 Buchstabe a) DS-GVO sind die personenbezogenen Daten der Videoüberwachung unverzüglich zu löschen, wenn sie für die Erreichung der Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen. Unter Berücksichtigung von Art. 5 Abs. 1 Buchstabe c) DS-GVO „Datenminimierung“ und Abs. 1 Buchstabe e) DS-GVO „Speicherbegrenzung“ sind die Speicherfristen stets auf das unbedingt erforderliche Mindestmaß zu beschränken. Derzeit gehen die Aufsichtsbehörden von einer zulässigen Speicherdauer von 48 Stunden bis maximal 72 Stunden bei Wochenenden oder Feiertagen aus, da bei einem entsprechenden Vorfall eine Sicherung des Materials in dieser Zeit geklärt werden kann (nähere Informationen in der

Orientierungshilfe Videoüberwachung, abrufbar unter https://www.tlfdi.de/datenschutz/videoueberwachung/). Eine längere Speicherdauer bedarf einer Begründung zur Erforderlichkeit der Dauer der Speicherung, welche das Unternehmen nicht vorgetragen hatte.
Dem Unternehmen wurde entsprechend mittels verwaltungsrechtlicher Anhörung die Möglichkeit gegeben, die geforderten Anpassungen vorzunehmen. Dies geschah hier nicht im ausreichenden Maße, sodass der TLfDI einen Bescheid nach Art. 58 Abs. 2 DS-GVO erlassen musste. Darin wurde dem Unternehmen die Videoüberwachung während der Geschäftszeiten des Unternehmens untersagt. Ferner wurden die Verpixelung beziehungsweise Schwärzung der öffentlichen Bereiche sowie die Anpassung der Speicherdauer auf 48 Stunden angeordnet. Der Bescheid wurde zwischenzeitlich bestandskräftig und das Unternehmen hat die Maßnahmen aus dem Bescheid ebenfalls ausreichend umgesetzt.

3.14 Videoüberwachung einer gemeinschaftlich genutzten Grundstückszufahrt

Bei der Installation von Videoüberwachungsanlagen auf einem Privatgrundstück muss durch den Eigentümer sichergestellt werden, dass weder der angrenzende öffentliche Bereich noch benachbarte Privatgrundstücke oder der gemeinsame Zugang zu diesen von der Videoüberwachung erfasst werden. Hintergrund ist, dass betroffene Personen grundsätzlich selbst entscheiden dürfen, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden und wann und unter welchen Voraussetzungen die persönlichen Daten preisgegeben und verwendet werden. Dieser Grundsatz gilt nur dann nicht, insofern die Interessen des Kamerabetreibers gegenüber dem Persönlichkeitsrecht der Betroffenen überwiegen.

Ein Bürger erstattete Anzeige bei der Polizei wegen einer Videoüberwachung der gemeinschaftlich genutzten Grundstückszufahrt durch seinen Nachbarn. Dieses Verfahren wurde zur Verfolgung einer Ordnungswidrigkeit an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) abgegeben. Vor diesem Hintergrund wandte sich der TLfDI mit einer Anhörung an den Kamerabetreiber. Dieser teilte mit, dass es sich bei der Zufahrt um sein

Eigentum handele und der Nachbar nur ein Fahr- und Wegerecht besäße.
Der TLfDI hatte im vorliegenden Fall zu prüfen, ob der Kamerabetreiber gegen die Grundsätze für die Verarbeitung, einschließlich der Bedingungen für die Einwilligung, gemäß den Artikeln 5, 6 und 7 Datenschutz-Grundverordnung (DS-GVO) verstoßen hat.
Die durch die Kameras aufgezeichneten Daten vom Befahren und Betreten der gemeinschaftlich genutzten Grundstückszufahrt sind als personenbezogene Daten im Sinne des Art. 4 Nr. 1 DS-GVO einzuordnen. Auch Besucher, die nicht damit rechnen müssen, heimlich gefilmt zu werden, könnten in den Fokus der Videoüberwachung geraten. Allein die Informationen darüber, wo sich eine bestimmte oder bestimmbare Person aufhält, mit wem sie sich trifft oder unterhält, das Betreten und Befahren der gemeinschaftlich genutzten Grundstückszufahrt sind eine Angabe über persönliche Verhältnisse, die mittels der Videoüberwachung erhoben wird. Diese Daten sind nicht allgemein zugänglich.
Aufgrund des unbestimmbaren Personenkreises, welcher sich im Bereich der Zufahrt aufhalten könnte, ist die Einholung einer Einwilligung regelmäßig nicht möglich.
Im vorliegenden Fall kam daher nur ein Erlaubnistatbestand für eine Datenverarbeitung mit den Kameras nach Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO in Betracht, soweit die Kameras zur Wahrnehmung der berechtigten Interessen des Kamerabetreibers erforderlich sind und nicht die Interessen oder Grundrechte und Grundfreiheiten der von der Videoüberwachung betroffenen Personen zum Schutz ihrer personenbezogenen Daten überwiegen. Die berechtigten Interessen können hierbei ideeller, wirtschaftlicher oder rechtlicher Natur sein.
Als Grund für die Videoüberwachung gab der Kamerabetreiber an, die Autos auf seinem Grundstück vor angeblicher Sachbeschädigung schützen zu wollen. Aufgrund der hierzu fehlenden Nachweise konnte vom TLfDI allerdings kein berechtigtes Interesse festgestellt werden.
Bei der Angabe des Kamerabetreibers, dass es sich bei der videoüberwachten Grundstückszufahrt um sein Eigentum handele, ist zu beachten, dass betroffene Personen grundsätzlich selbst entscheiden dürfen, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden und wann und unter welchen Voraussetzungen die persönlichen Daten preisgegeben und verwendet werden. Somit muss auch bei der Installation von Videoüberwachungsanlagen auf einem

Privatgrundstück sichergestellt sein, dass weder der angrenzende öffentliche Bereich noch benachbarte Privatgrundstücke oder der gemeinsame Zugang zu diesen von den Kameras erfasst werden. Dieser Grundsatz gilt nicht, insofern die Interessen des Kamerabetreibers gegenüber dem Persönlichkeitsrecht der Betroffenen überwiegen.
Die Befugnis, den eigenen räumlichen Bereich mit Videokameras zu überwachen steht unter dem Schutz des Eigentumsgrundrechts gemäß Art. 14 Grundgesetz (GG). Zulässig wäre somit eine Videoüberwachung, die sich auf den eigenen privaten Bereich beschränkt, der nur für den Eigentümer selbst und für die Familienangehörigen zugänglich ist. Insofern darf der Eigentümer eine Überwachungskamera installieren, sofern diese ausschließlich auf das eigene Grundstück gerichtet ist und eine Verletzung der Rechte Dritter ausgeschlossen ist. Auch eine Kamera, die grundsätzlich nur das eigene Grundstück erfassen soll, kann unter das Datenschutzrecht fallen und muss dann den dortigen Voraussetzungen genügen. Die DS-GVO findet zwar nach Art. 2 Abs. 2 Buchstabe c) DS-GVO keine Anwendung, wenn eine Verarbeitung von personenbezogenen Daten durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten erfolgt (Haushaltsausnahme). Zu beachten ist jedoch, dass der Betrieb eines Kamerasystems an einem Einfamilienhaus zum Zweck des Schutzes des Eigentums, der Gesundheit und des Lebens der Besitzer des Hauses, **das auch den öffentlichen Raum überwacht**, keine Datenverarbeitung darstellt, die zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten vorgenommen wird (vergleiche EuGH, Urteil vom 11. Dezember 2014 – in der Rechtssache C-212/13, Rn. 33). Demzufolge wird das Datenschutzrecht nur nicht auf Videoaufnahmen angewendet, die von einer natürlichen Person lediglich zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten ohne Einbeziehung des öffentlichen Raums und auch ohne Bezug zu einer beruflichen oder wirtschaftlichen Tätigkeit vorgenommen werden (vergleiche Art. 2 Abs. 2 Buchstabe c) und Erwägungsgrund 18 Satz 1 DS-GVO).
Da im vorliegenden Fall die installierte Videoüberwachung aber zumindest auch Bereiche erfasste, die für den Anzeigeerstatter und eventuelle Besucher zugänglich waren, wurden die berechtigten Interessen der von den Videoaufnahmen betroffenen Personen berücksichtigt. Diesen Personen steht ein Recht auf informationelle Selbstbestimmung als besondere Ausprägung des Allgemeinen Persönlichkeitsrechts zu. Das Allgemeine Persönlichkeitsrecht aus Art. 2 Abs. 1 GG

in Verbindung mit Art. 1 Abs. 1 GG vermittelt nämlich jedem einen Anspruch auf Achtung und Entfaltung seiner Persönlichkeit und auch den Schutz seines Privatbereichs. Es umfasst auch die Freiheit vor unerwünschten Videoaufnahmen. Dieses Grundrecht, welches auch im Art. 6 Abs. 2 der Verfassung des Freistaats Thüringen erfasst ist, gilt auch auf einem Privatgrundstück. Durch die Videoaufnahmen kann das Persönlichkeitsrecht und zudem auch die Privat- oder gar die Intimsphäre eines Dritten schwerwiegend verletzt werden. Im vorliegenden Fall kam solch eine Beeinträchtigung der Rechte auch für den Anzeigeerstatter als Grundstücksnachbar in Betracht, da er sich der Überwachungsmaßnahme nicht entziehen konnte und gezwungen war, dementsprechende Verkehrsflächen zu nutzen.
Durch die Videoüberwachung ist es dem Kamerabetreiber möglich gewesen, Erkenntnisse über persönliche oder sachliche Verhältnisse einzelner natürlicher Personen zu erlangen, die sich – wenn auch nur zufällig – im Bereich der Überwachung aufhielten. Die gemeinschaftliche Grundstückszufahrt nutzten alle Personen, die dort wohnen oder zu Besuch waren, daher war eine Ausweichmöglichkeit nicht gegeben. Der Anzeigeerstatter war stets dem von der Videoüberwachungsanlage ausgehenden Überwachungsdruck ausgesetzt.
Im Ergebnis konnte der TLfDI feststellen, dass die Interessen der von der Videoüberwachung betroffenen Personen überwogen und somit eine unrechtmäßige Datenverarbeitung hinsichtlich der personenbezogenen Daten des Anzeigeerstatters und etwaiger Besucher erfolgte. Aufgrund des damit gegebenen Verstoßes gegen die Grundsätze für die Verarbeitung von personenbezogenen Daten, einschließlich der fehlenden Bedingungen für die Einwilligung, gemäß den Artikeln 5, 6 und 7 DS-GVO wurde nach Art. 83 Abs. 5 Buchstabe a) DS-GVO eine Geldbuße gegen den Kamerabetreiber verhängt.

3.15 Allgemeines zu Mieterselbstauskünften – Freiwilligkeit, Zeitpunkt der Übermittlung der Mieterselbstauskunft und weitere Unterlagen?

Den TLfDI erreichen immer wieder Beschwerden über Vermieter, die wegen umfangreicher Mieterselbstauskünfte und der Anforderung zahlreicher Unterlagen auffallen. Bereits zur Mieterselbstauskunft besteht Erklärungsbedarf: Wann darf eine solche angefordert werden, sind die Angaben tatsächlich freiwillig und welche Unterlagen muss ein Mietinteressent zu welchem Zeitpunkt übermitteln?

Im Berichtszeitraum erreichten den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) zahlreiche Beschwerden über Mieterselbstauskünfte. Mittels Mieterselbstauskünften wollen Vermieter den geeignetsten Mietkandidaten ausfindig machen. Dabei werden von den Mietinteressenten neben Angaben zur Person (Name, Geburtsdatum, bisherige Anschrift, derzeitiger Arbeitgeber) unter anderem Angaben zu Mitbewohnern und zu ihrem finanziellen Hintergrund (Verdienst, finanzielle Verpflichtungen) und zu persönlichen Vorlieben (Raucher, Haustiere, Spielen von Musikinstrumenten) erfragt. Nicht alle diese personenbezogenen Daten darf der Vermieter datenschutzrechtlich zulässig verarbeiten. Da es viele Ideen von Vermietern gibt, nach welchen Kriterien Mietinteressenten ausgewählt werden könnten und es keine Muster-Mieterselbstauskünfte gibt, stellt in der Praxis fast jeder Vermieter sein eigenes Musterformular „Mieterselbstauskunft“ zusammen.
Im vorliegenden Fall spielte jedoch weniger die Frage nach der datenschutzrechtlichen Zulässigkeit der einzelnen Fragen die entscheidende Rolle, sondern eher nach dem Zeitpunkt einer solchen Auskunft allgemein. Die Beschwerdeführerin hatte eine Mieterselbstauskunft vor Erhalt eines Besichtigungstermins ausgefüllt. Darin bezeichnete der Vermieter die Mieterselbstauskunft als „freiwillige Selbstauskunft“ und meinte eine Einwilligung zur Datenverarbeitung mit der Mieterselbstauskunft einzuholen. Darüber hinaus forderte der Vermieter die Mietinteressentin auf, nachdem sie sich für die Wohnung entschieden hatte, folgende Unterlagen zu übermitteln: Kopie des Personalausweises, Kopie der letzten zwei Verdienstbescheinigungen, Mietschuldenfreiheitsbestätigung des Vorvermieters, Nachweis (Police) einer Haftpflichtversicherung. Hiergegen wandte sich die Beschwerdeführerin und legte Beschwerde beim TLfDI ein.
Zunächst war die Frage zu klären, zu welchem Zeitpunkt der Vermieter einen Mietinteressenten grundsätzlich bitten darf, eine Mieterselbstauskunft auszufüllen. Bei der Beurteilung der Zulässigkeit von Datenverarbeitungen im Rahmen von Mieterselbstauskünften muss entsprechend der Orientierungshilfe zur „Einholung von Selbstauskünften bei Mietinteressentinnen“ der Datenschutzkonferenz zwischen drei Zeitpunkten differenziert werden:
- dem Besichtigungstermin (A.),
- der vorvertraglichen Phase, in welcher der Mietinteressent dem künftigen Vermieter mitteilt, eine konkrete Wohnung anmieten zu wollen (B.) und

- der Entscheidung des künftigen Vermieters für einen bestimmten Mietinteressenten (C.).

Die Zulässigkeit der Erhebung personenbezogener Daten der Mietinteressentin richtet sich im Besichtigungstermin regelmäßig nach Art. 6 Abs. 1 Satz 1 Buchstabe f) der Datenschutz-Grundverordnung (DS-GVO). Die Mietinteressentin hatte sich noch nicht für die Anmietung der Wohnung entschieden, als sie zur Übersendung der umfangreichen Mieterselbstauskunft aufgefordert worden war. In dieser Phase (A) der Vertragsanbahnung dürfen lediglich Angaben zur Identifikation des Mietinteressenten erfragt werden. Eine Rechtsgrundlage für die Datenverarbeitung weiterer personenbezogener Daten aus einer Mieterselbstauskunft besteht vor Erreichen der vorvertraglichen Phase (B) nicht aus dem möglicherweise später zu schließenden Vertrag. Erst wenn der Mietinteressent erklärt, eine konkrete Wohnung anmieten zu wollen, ist das Stadium der Vertragsanbahnung erreicht, das zur Datenverarbeitung personenbezogener Daten im Rahmen der Vertragsanbahnung nach Art. 6 Abs. 1 Satz 1 Buchstabe b) DS-GVO berechtigt. Fraglich ist daneben, ob eine Einwilligung in einem derartigen Fall überhaupt in Betracht kommt. Die Einwilligung nach Art. 7 DS-GVO muss freiwillig, für einen konkreten Fall, nach ausreichender Information des Betroffenen und unmissverständlich abgegeben werden. Damit eine Einwilligung freiwillig ist, muss der Betroffene eine echte Wahl haben. Es gilt das sogenannte Kopplungsverbot. So darf ein Vertragsabschluss nicht von der Einwilligung zur Verarbeitung weiterer personenbezogener Daten abhängig gemacht werden, die für die Durchführung des Geschäftes nicht nötig sind (Kurzpapier Nr. 20 – Einwilligung nach der DS-GVO, Datenschutzkonferenz, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_20.pdf).

Das Problem der Beschwerdeführerin war, dass die Selbstauskunft als „freiwillige Selbstauskunft“ bezeichnet worden war. Dennoch war ihr sehr bewusst, dass sie im Falle der Nichtbeantwortung aller Fragen nicht einmal die Chance erhalten würde, in die Auswahl als Mieterin zu gelangen. Datenschutzrechtlich täuschte der Vermieter mit diesem Hinweis vor, die personenbezogenen Daten auf Grundlage einer Einwilligung nach Art. 6 Abs. 1 Satz 1 Buchstabe a), Art. 7 DS-GVO zu verarbeiten.

Das Ausfüllen der Mieterselbstauskunft und die Übergabe aller Unterlagen sind Voraussetzung für eine Berücksichtigung im Rahmen

der Mieterauswahl und daher Voraussetzung für das Zustandekommen eines Mietvertrages. Wird die Datenverarbeitung auf eine Einwilligung nach Art. 6 Abs. 1 Satz 1 Buchstabe a) DS-GVO gestützt, wird dem Betroffenen signalisiert, es komme gerade auf sein Einverständnis für die Zulässigkeit der Datenverarbeitung an. Dem Betroffenen wird die Illusion der Kontrolle über die Datenverarbeitung suggeriert, die ihm auch bei einem Widerruf seiner Einwilligung sodann nicht zusteht. Hier besteht für den Mietinteressenten eine Zwangslage, die nicht mit dem Verhältnis Mieter/Vermieter vergleichbar ist. Ein Mieter hat gegenüber dem Vermieter eine starke rechtliche Stellung, die sich aus dem abgeschlossenen Mietvertrag und den gesetzlichen Regelungen speist. Im Unterschied hierzu gerät der Mietinteressent in eine Zwangslage, da der Abschluss des Mietvertrages von der Übermittlung aller Daten abhängig gemacht wird. Mangels Freiwilligkeit scheidet die Einwilligung daher als Rechtsgrundlage zur Verarbeitung personenbezogener Daten, die aus der Mieterselbstauskunft gewonnen werden, aus.
Spätestens nach der Erklärung der Mietinteressenten, eine konkrete Wohnung anmieten zu wollen (Phase B), entsteht ein vorvertragliches Schuldverhältnis zu den künftigen Vermieter:innen, sodass dann, wie auch im vorliegenden Fall, Art. 6 Abs. 1 Satz 1 Buchstabe b) DS-GVO maßgebend ist. In dieser Phase verlangte der Vermieter zahlreiche Unterlagen von der Beschwerdeführerin. Es war daher zu klären, welche Unterlagen (und damit personenbezogenen Daten) der Vermieter in dieser Phase datenschutzrechtlich zulässig verarbeiten darf. Zunächst ist der Vermieter befugt, bei einer Wohnungsbesichtigung, die Angaben des Mietinteressenten zur Identifikation (Name, Vorname, Anschrift) durch Vorlage des Personalausweises zu überprüfen und diesen Umstand der Überprüfung zu dokumentieren. Mit der Anfertigung der Kopie werden zusätzliche Daten, wie Foto, Unterschrift, Seriennummer verarbeitet, die zu diesem Zeitpunkt nicht erforderlich sind. Die Verarbeitung von personenbezogenen Daten aus dem Personalausweis, die nicht benötigt werden, stellt einen Verstoß gegen das Gebot der Datenminimierung nach Art. 5 Abs. 1 Buchstabe c) DS-GVO dar. Mithin ist die Anfertigung einer Ausweiskopie ohne Schwärzung der nicht benötigten personenbezogenen Daten nicht erforderlich und damit unzulässig.
Bereits in Phase B besteht seitens des Vermieters ein Interesse daran, die Bonität des Mietinteressenten beurteilen zu können. Daher darf die Einkommenshöhe erfragt werden. Zu diesem Zeitpunkt überwiegt das

Interesse des Vermieters, Sicherheit über die Bonität des Mietinteressenten zu erhalten (mittels Einkommensnachweis) noch nicht das informationelle Selbstbestimmungsrecht des Interessenten. Erst in Phase C – Entscheidung für einen Vertragspartner – tritt die schutzwürdige Position des zukünftigen Mieters hinter das Interesse des Vermieters zurück. Zu diesem Zeitpunkt darf der Vermieter sein Sicherheitsbedürfnis befriedigen und Einkommensnachweise verlangen. Dieses Vorgehen entspricht auch dem Grundsatz der Datenminimierung, Art. 5 Abs. 1 Buchstabe c) DS-GVO. Erst wenn ein Vertragsschluss kurz bevorsteht, überwiegt das Interesse des Vermieters, die Bonität mittels Einkommensnachweisen überprüfen zu können. Im vorliegenden Fall wurde die Mietinteressentin nicht in die engere Auswahl genommen. Das bedeutet, das Auswahlverfahren ist für die Mietinteressentin nicht über Phase B hinausgelangt. Die Gehaltsunterlagen durfte die Vermieterin noch nicht anfordern.

Im Rahmen einer Mieterselbstauskunft ist weiter zu beachten, dass bisherige Vermieter diesen gegenüber nicht verpflichtet sind, eine Mietschuldenfreiheitsbescheinigung zu erstellen (BGH, Urteil vom 30. September 2009, Az.: VIII ZR 238/08). Folglich kann eine solche Bescheinigung vom Mietinteressenten bei der beabsichtigten Neuanmietung von Wohnraum nicht verlangt werden.

Es besteht keine gesetzliche Verpflichtung zum Abschluss einer privaten Haftpflichtversicherung. Auch beeinflusst sie nicht die Bonität des Mietinteressenten und der Vermieter ist nicht Begünstigter einer solchen Versicherung. Daher ist der Nachweis des Abschlusses einer Haftpflichtversicherung nicht für den Abschluss des Vertrages erforderlich und damit die Frage nach Bestehen einer solchen Haftpflichtversicherung nach Art. 5 Abs. 1 Buchstabe a) DS-GVO unzulässig.

Der Verantwortliche wurde nach Art. 58 Abs. 2 Buchstabe b) DS-GVO verwarnt und hat seine Mieterselbstauskunft entsprechend den Vorgaben des TLfDI angepasst.

Weitere Informationen zur datenschutzrechtlichen Zulässigkeit von Mieterselbstauskünften finden sich in der **Orientierungshilfe zur „Einholung von Selbstauskünften bei Mietinteressent:innen“ der Datenschutzkonferenz,** abrufbar unter: https://www.datenschutzkonferenz-online.de/media/oh/20180207_oh_mietauskuenfte.pdf.

3.16 Daten hin, Daten her, rundherum ist gar nicht schwer – oder?

Die Falschversendung von Paketen mit beiliegender Rechnung stellt eine unzulässige Offenbarung von personenbezogenen Daten dar. Das vom Verantwortlichen veranlasste gegenseitige Austauschen falsch versendeter Waren unter den Kunden ist datenschutzrechtlich nicht möglich, da die aufgrund eines Vertrages mit dem Verantwortlichen erhobenen Daten nicht ohne Weiteres an Dritte weitergegeben werden dürfen.

Der Beschwerdeführer hatte über die Plattform www.amazon.de einen Artikel bestellt. Der Händler, der den Artikel anbot und der in Thüringen seinen Sitz hat, nutzte die Plattform, um eigenständig seine Waren zu vertreiben. Nach Abwicklung der Bestellung erhielt der Beschwerdeführer aber die falsche Ware und auch eine falsche Rechnung zugesandt mit den personenbezogenen Daten eines Dritten. Er machte den Händler darauf aufmerksam. Als Antwort wurde dem Beschwerdeführer mitgeteilt, dass der Artikel versehentlich vertauscht worden sei und der Empfänger des anderen Artikels sich auch bereits gemeldet hätte. Der Beschwerdeführer würde nun eine Postmarke vom Händler erhalten, worauf die Anschrift des anderen Empfängers vermerkt wäre und der Beschwerdeführer sowie der andere falsch belieferte Kunde sollten die Artikel sozusagen gegenseitig austauschen. Die Rechnungen enthielten jeweils die personenbezogenen Daten des Kunden wie Name, Adresse, E-Mail-Adresse, Kundennummer. Den Austausch lehnte der Kunde unter Hinweis auf eine Verletzung des Datenschutzes ab und wandte sich mit einer Beschwerde an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI).
Daraufhin wurde der Sachverhalt beim Händler als Verantwortlichem weiter ermittelt. Der Verantwortliche gab an, dass dies nach seiner Ansicht der schnellste Weg gewesen sei, um den Kunden die richtigen Warenlieferungen zukommen zu lassen. Er gab weiterhin an, dass dies eine Ausnahme und nicht das übliche Prozedere gewesen sei.
Auch wenn in dieser praktischen Handhabung möglicherweise eine erhebliche Zeitersparnis liegen kann, bedarf es dazu auf datenschutzrechtlicher Seite einer Norm für die Übermittlung beziehungsweise für den Austausch der Adressdaten der Kunden. Nach Art. 5 Abs. 1

Datenschutz-Grundverordnung (DS-GVO) müssen personenbezogene Daten auf rechtmäßige Weise verarbeitet werden. Die Verarbeitung ist nur dann rechtmäßig, wenn mindestens eine rechtliche Grundlage aus Art. 6 Abs. 1 Satz 1 Buchstabe a) bis f) DS-GVO zutrifft. Die Übermittlung der Daten des jeweils anderen Kunden kann allerdings auf keine der dort vorhandenen rechtlichen Grundlagen gestützt werden. Auch eine Einwilligung der Kunden gemäß Art. 6 Abs. 1 Satz 1 Buchstabe a) DS-GVO hatte nicht vorgelegen, noch vertragliche Ansprüche, da diese nur jeweils mit dem Verantwortlichen selbst bestehen und daher keine gültige Rechtsgrundlage nach Art. 6 Abs. 1 Satz 1 Buchstabe b) DS-GVO darstellen, noch ein berechtigtes Interesse oder gesetzliche Ansprüche vorlagen.
Durch die Falschversendung kam es auch zu einer Offenbarung von personenbezogenen Daten des jeweils anderen Kunden, also Namen, Adresse und Kundennummer, die sich aus der beiliegenden Rechnung ergaben und Informationen sind, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen, Art. 4 Nr. 1 DS-GVO. Für die Offenbarung dieser Daten an den jeweils anderen Kunden gibt es keine rechtliche Grundlage und diese Offenbarung ist daher auch eine Datenschutzverletzung. Dies ist dann der Fall, wenn eine Verletzung der Sicherheit, die unbeabsichtigt oder unrechtmäßig zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden, Art. 4 Nr. 12 DS-GVO.
Als eine solche muss diese gemäß Art. 33 DS-GVO auch als Verletzung des Schutzes personenbezogener Daten behandelt werden und eine Meldung an die zuständige Aufsichtsbehörde unverzüglich und möglichst binnen 72 Stunden ergehen. Der TLfDI hat dazu eigens auf seiner Webseite www.tlfdi.de ein Meldeformular eingestellt, welches für die Meldung zu nutzen ist.
Gegenüber dem Verantwortlichen wurde durch den TLfDI eine Verwarnung dahingehend ausgesprochen, dass personenbezogene Daten nur auf rechtmäßige, für die betroffene Person nachvollziehbare Weise verarbeitet werden dürfen und daher entweder eine Einwilligung nach Art. 6 Abs. 1 Satz 1 Buchstabe a) DS-GVO oder eine anderweitige Rechtsgrundlage für eine Verarbeitung vorliegen muss und dass im Falle einer Verletzung des Schutzes personenbezogener Daten gemäß Art. 33 DS-GVO unverzüglich und möglichst binnen 72 Stunden die Verletzung an die zuständige Aufsichtsbehörde zu melden ist.

3.17 Prüfen heißt nicht Kopieren! Irrungen beim Nachweis der Befreiung von der Maskenpflicht

Eine Überprüfung der Einhaltung der Maskenpflicht oder von Ausnahmen dazu stellt keine rechtliche Grundlage für das Fertigen einer Kopie dieses Attestes dar, welche vorsorglich für den Fall einer Prüfung gefertigt wird.

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichte eine Beschwerde darüber, dass ein Ladengeschäft personenbezogene Daten verarbeite, ohne hierfür berechtigt zu sein. Hintergrund war, dass der Beschwerdeführer im November 2020 ein Ladengeschäft betreten hatte, ohne dabei einen Mund-Nasen-Schutz zu tragen. Daraufhin wurde er vom anwesenden Personal angesprochen und legte eine Befreiung in Form eines ärztlichen Attestes vor. Dieses Attest wurde vom Personal kopiert und ihm wurde mitgeteilt, dass es für zwei Wochen aufbewahrt werden würde. Einige Tage später stellte der Beschwerdeführer eine Löschungsforderung gegenüber dem Ladengeschäft. Er war mit dem Vorgehen nicht einverstanden und wandte sich daher auch an den TLfDI. Der TLfDI klärte daraufhin mit einem Auskunftsersuchen den Sachverhalt weiter auf und der Ladeninhaber wurde angehört. Er führte aus, dass die Speicherung der Befreiung von der Maskenpflicht erfolgte, um bei etwaigen Beschwerden oder Kontrollen durch das zuständige Gesundheitsamt/Ordnungsamt einen Nachweis erbringen zu können, warum gegebenenfalls ein Kunde im Geschäft keine Maske getragen habe.
Die Verwendung der personenbezogenen Daten des Kunden durch Erstellen einer Kopie des ärztlichen Attestes zur Befreiung von der Maskenpflicht stellte im vorliegenden Fall einen Verstoß gegen Art. 5 Abs. 1 Buchstabe a) Datenschutz-Grundverordnung (DS-GVO) dar. Nach Art. 5 Abs. 1 Buchstabe a) DS-GVO müssen personenbezogene Daten auf rechtmäßige Weise verarbeitet werden. Aus Art. 6 Abs. 1 DS-GVO ergibt sich, dass nur unter den dort genannten Bedingungen eine Datenverarbeitung zulässig ist. Es handelt sich somit um ein Verbot mit Erlaubnisvorbehalt. Da es sich bei dem Attest um Gesundheitsdaten und damit um besondere Kategorien von Daten handelte, ist hier zusätzlich der Art. 9 DS-GVO zu prüfen. Danach ist eine Datenverarbeitung grundsätzlich untersagt und nur möglich, wenn die betroffene Person in die Verarbeitung ausdrücklich eingewilligt hat.

Eine ausdrückliche Einwilligung nach Art. 6 Abs. 1 Satz 1 Buchstabe a), Art. 9 Abs. 2 Buchstabe a) DS-GVO durch den Kunden war jedoch nicht gegeben. Spätestens in dem Zeitpunkt, als der Kunde das Kopieren in Frage stellte und zur Löschung aufforderte, lag keine Einwilligung mehr vor. Hierin ist auf jeden Fall ein Widerruf gemäß Art. 7 Abs. 3 DS-GVO zu sehen. Ab diesem Zeitpunkt erfolgte auch eine Verarbeitung ohne jegliche rechtliche Grundlage, welche ebenfalls eine sofortige Pflicht zur Löschung nach Art. 17 Abs. 1 Buchstabe d) DS-GVO nach sich zieht.
Eine rechtliche Grundlage für die Erhebung der Daten aus der Befreiung besteht im Einzelhandel auch nicht aufgrund besonderer gesetzlicher Verpflichtungen nach Art. 6 Abs. 1 Satz 1 Buchstabe c) DS-GVO, denn die zu diesem Zeitpunkt gültigen Corona-Verordnungen des Landes und auch der Stadt gaben keine Veranlassung zur Speicherung von Attesten zur Maskenpflichtbefreiung. Die weitere Begründung des Ladeninhabers war, dass die Datenerhebung als Privatperson zum Schutze der Gesundheit und der seines gefährdeten Umfeldes inmitten einer Pandemie erfolge, damit es möglich wäre, im Falle einer Ansteckung die Information über den Besuch des Kunden an die entsprechenden Behörden weiterzugeben. Der Ladeninhaber begründete dies mit Art. 9 Abs. 2 Buchstabe i) DS-GVO. Dieser Tatbestand ist vorliegend aber nicht einschlägig. Er bezieht sich auf die öffentlichen Gesundheitsdienste und dabei insbesondere auf öffentliche Gesundheitsinteressen. Das bedeutet, dass sich Private oder private Unternehmen grundsätzlich nicht auf diese Alternative berufen können (Weichert in: Kühling/Buchner, Kommentar zur DS-GVO/BDSG, 2. Aufl., Art. 9 Rn: 116). Beim Kopieren des Attestes ist auch zu beachten, dass eine bequeme Erhebung der Daten als Kopie dem Grundsatz der Datensparsamkeit nach Art. 5 Abs. 1 Buchstabe c) DS-GVO widerspricht. Danach sind nur die Daten zu erheben, die dem Zweck angemessen und erheblich sowie auf das notwendige Maß beschränkt sind. Es bestand jedoch zu dieser Zeit keine Verpflichtung zur Kontaktnachverfolgung im Einzelhandel, denn dann hätte der Ladeninhaber auch von allen anderen Kunden Daten erheben müssen.
Dem Ladenbesitzer gegenüber wurde eine Verwarnung nach Art. 58 Abs. 2 Buchstabe b) DS-GVO ausgesprochen. Eine zusätzliche Löschungsanordnung war nicht erforderlich, da der Ladeninhaber auf Nachfrage des TLfDI mitgeteilt hat, dass das kopierte Attest nach ei-

ner Aufbewahrungszeit von 14 Tagen vernichtet wurde und das Dokument während dieser Zeit abgeschlossen und vor Zugriffen Dritter verwahrt wurde.

3.18 Gästedatenerfassung mit DARFICHREIN datenschutzgerecht?!

Die Corona-Pandemie machte die unkomplizierte, schnelle Kontaktdatenerfassung erforderlich, um das Hotel- und Gaststättengewerbe nicht vor weitere Herausforderungen zu stellen. Nicht alle Lösungen waren anfangs datenschutzkonform. Umso positiver war es, wenn der TLfDI nach einer Prüfung grünes Licht geben konnte.

Die Corona-Pandemie hatte Auswirkungen auf viele Branchen. Sie traf vor allem das Hotel- und Gaststättengewerbe hart. Nach einem kompletten Lockdown gab es eine vorsichtige Öffnung, allerdings mit der Verpflichtung, Kontaktdaten von allen Gästen für einen gewissen Zeitraum zu erfassen um im Falle einer Infektion die möglichen Kontakte nachverfolgen zu können. Dies bei laufendem Betrieb mit Formularen zu handhaben, erwies sich als sehr mühsam. Daher wurde nach anderen Lösungen gesucht. Zu fragen ist in diesem Zusammenhang immer, ob ein datenschutzkonformer Einsatz möglich ist.
So erreichte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) die Anfrage, ob das Tool DARFICHREIN bedenkenlos genutzt werden könne.
Die Anwendung wurde in einer Kooperation zwischen der Anstalt für kommunale Datenverarbeitung in Bayern (AKDB) und dem Bayerischen Hotel- und Gaststättenverband DEHOGA Bayern e. V. entwickelt. Mit einem QR-Code-System konnten Kontaktdaten von Gästen im Zusammenhang mit COVID-19 bei Gaststättenbesuchen erfasst und bei Erforderlichkeit dann vom Gesundheitsamt abgerufen werden. Der Gast musste bei Betreten des Lokals einen QR-Code scannen (browserbasiert und ohne Download einer App) und seine Kontaktdaten am Smartphone eingeben. Der Browser konnte die Kontaktdaten für weitere QR-Code-Scans lokal speichern. Der Gastronom erhielt einen privaten Schlüssel, mit dem er die auf dem Server verschlüsselt abgelegten Kontaktdaten seiner Gäste nur dann im Admin-Bereich entschlüsselte, wenn diese den Gesundheitsbehörden übergeben wer-

den sollten. Der DEHOGA THÜRINGEN e. V. hatte seinen angeschlossenen Betrieben das System zur Nutzung empfohlen. Daher kam das Tool auch in Thüringen zur Anwendung.
Der TLfDI nahm zur Prüfung des Systems Kontakt zur Datenschutzaufsichtsbehörde in Bayern, zum DEHOGA THÜRINGEN e. V. sowie zum Thüringer Ministerium für Arbeit, Soziales, Gesundheit, Frauen und Familie auf. Gleichzeitig unterzog er die Anwendung einer technischen Prüfung. Dabei stellte er durch die Produktdokumentation einige mögliche Angriffspunkte fest und hinterfragte, ob diese tatsächlich vorlagen.
Nach dem veröffentlichten Auftragsverarbeitungsvertrag (AVV) wurde zwar eine asymmetrische Verschlüsselung (RSA 4096 Bit) genutzt, um die Anmeldedaten zu verschlüsseln. Wie die Schlüsselgenerierung erfolgte, war dem TLfDI nicht bekannt. RSA mit 4096 Bit ist eine sichere Verschlüsselung, welche aus zwei Schlüsselteilen besteht. Wenn der Betreiber des Servers aber beide Teile kennt, da er sie selber erzeugt, ist die Verschlüsselung dennoch unsicher. Die beiden Teile dürfen nur dem Gastwirt beziehungsweise Veranstalter bekannt sein, während der Serverbetreiber nur einen Teil des Schlüssels kennen darf. In den FAQs (https://darfichrein.de/dir/faq) wurde lediglich mitgeteilt, dass der private Schlüssel dem Verantwortlichen im Laufe des Registrierungsprozesses bekanntgegeben und anschließend vom Server gelöscht wird. Dies bedeutete, dass der private Schlüssel dem Plattformbetreiber zumindest kurzzeitig bekannt war. Dieser erste Punkt wurde vom TLfDI bei der Prüfung thematisiert.
Bei der Übertragung der Kontaktdaten von Gästen in den Datenbereich des Verantwortlichen wurde nach Kenntnis des TLfDI die Übertragung nur durch eine Transportverschlüsselung gesichert. Dies bedeutete, dass die Daten vor der Speicherung in der Datenbank kurzzeitig unverschlüsselt am Server vorlagen und erst dort mit dem Schlüssel des Verantwortlichen verschlüsselt wurden.
Außerdem war unklar, wie das Recht auf Löschung, Berichtigung oder Auskunft vom Betroffenen wahrgenommen werden könnte, wenn nur verschlüsselte Daten auf dem Server des Betreibers dauerhaft gespeichert werden. Es stellte sich daher die Frage, ob es von Seiten des Providers spezielle Tools gab, um Datensätze gezielt durch den Verantwortlichen verändern zu können.
Im AVV wurde pauschal auf die technischen und organisatorischen Maßnahmen des Subunternehmens zur Sicherung der Zutrittskontrolle verwiesen. Es ist aber erforderlich, dass sich ein Verantwortlicher ein

adäquates Bild der Sicherheitsvorkehrungen machen kann. Deswegen sollten die technischen und organisatorischen Maßnahmen des Subunternehmens bekannt sein. Es war unklar, wie die Daten beim Nutzer selber sicher hinterlegt werden konnten. All diese Punkte wurden vom TLfDI beim DEHOGA THÜRINGEN e. V. angesprochen, um fehlerhafte Dokumentation oder tatsächliche Sicherheitslücken auszuschließen oder zu korrigieren.
Der DEHOGA THÜRINGEN e. V. ließ wissen, dass er sich ausführlich mit den am Markt angebotenen diesbezüglichen Programmen auseinandergesetzt habe und nach umfassender Prüfung zum Ergebnis gekommen sei, eine Partnerschaft mit DARFICHREIN zu begründen. Ausschlaggebend seien dabei insbesondere die Offenlegung aller relevanten Sachverhalte, insbesondere eben auch der datenschutzrechtlichen Aspekte gewesen, die bei anderen Angeboten so nicht zu verzeichnen gewesen waren, und schließlich auch die Gesellschafter DEHOGA Bayern e. V. und die AKDB. Man habe sich bei der Entscheidung auch davon leiten lassen, dass der Chaos-Computer-Club einige am Markt befindliche Systeme getestet und dabei insbesondere umfassende Mängel bezüglich des Datenschutzes aufgedeckt hatte und die DARFICHREIN-Lösung diesbezüglich ein sehr positives Prüfungsergebnis erhalten hätte. Der DEHOGA THÜRINGEN e. V. stellte weitere Informationen zur Bewertung des Systems zur Verfügung.
Daraus ergaben sich die Antworten auf die vom TLfDI aufgeworfenen Fragen: Die Kontaktdaten auf dem Smartphone im Browser-Storage sind durch eine vierstellige PIN geschützt worden. Bei der Kontoerstellung eines Gastwirtes/Veranstalters wurde das Schlüsselpaar im Browser des Gaststättenbetreibers generiert und nur der öffentliche Teil an den Server übermittelt. Der private Teil wurde als Datei beim Gaststättenbetreiber gespeichert und war für den Server von DARFICHREIN daher nie einsehbar. Bei der Übermittlung von Kontaktdaten vom Browser des Besuchers der Gaststätte zum Server von DARFICHREIN wurde die Verschlüsselung der Kontaktdaten mit dem öffentlichen Schlüssel des Gaststättenbetreibers im Browser des Gastes durchgeführt. Damit führte diese Verschlüsselung nicht der Server von DARFICHREIN durch, sondern das Gerät des Gastes selbst. Die Dokumentation der Software war somit irreführend. Diese Punkte stellten sich nach der Prüfung sicherer dar, als dies die Dokumentation nahegelegt hatte.

Damit waren die technischen Bedenken des TLfDI vollständig ausgeräumt und es bestanden keine weiteren Vorbehalte gegen den Einsatz dieses Systems. Dies wurde den im Verfahren Beteiligten mitgeteilt.

3.19 Darf jeder medizinische Mitarbeiter eines Klinikums auf alle Patientendaten zugreifen?

Ärztliche und pflegerisch tätige Mitarbeiter eines Klinikums dürfen nur auf die personenbezogenen Daten der Patienten zugreifen, die sie medizinisch behandeln und/oder pflegerisch versorgen. Dies betrifft in der Regel die personenbezogenen Daten von Patienten auf der Station beziehungsweise Abteilung des Krankenhauses, auf der die ärztlichen Mitarbeiter und Pflegkräfte jeweils tätig sind. Das Klinikum muss im Rahmen des Krankenhaus-Informationssystems über ein entsprechendes Rollen- und Rechtekonzept verfügen, das die Zugriffsrechte (Lese- und Schreibrechte) konkret regelt.

Im August 2021 erreichte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) eine Beschwerde von Mitarbeitern eines Thüringer Klinikums. Die Beschwerdeführer legten dar, dass alle Mitarbeiter des Klinikums, insbesondere das Pflegepersonal, auf sämtliche Patientenakten des Klinikums zugreifen könnten und das elektronische Aktensystem systematisch danach durchsuchen würden, ob sich Freunde oder Bekannte im Klinikum befänden. Weiterhin seien Patienten des Klinikums privat auf ihre medizinischen Diagnosen angesprochen worden, obwohl sie diese selbst nicht im Freundes- oder Bekanntenkreis kommuniziert hätten. Zudem könnten ärztliche Mitarbeiter des in der Beschwerde genannten Klinikums auf Patientenakten anderer Kliniken, die zum gleichen Konzern gehörten, zugreifen.
Aufgrund der Beschwerde führte der TLfDI im September 2021 eine Vor-Ort-Kontrolle in dem betreffenden Klinikum durch und ließ sich das Rollen- und Rechtekonzept sowie die zugehörigen Zugriffsrechte für ärztliche und pflegerische Mitarbeiter umfassend erläutern und demonstrieren. Hierbei stellte sich heraus, dass das Rollen- und Rechtekonzept des Krankenhaus-Informationssystems nicht den datenschutzrechtlichen Anforderungen entsprach und die Beschwerde insofern begründet war.
Das Rollen- und Rechtekonzept basierte lediglich auf Funktionsbereichen, das heißt, eine Krankenschwester des Klinikums konnte gemäß

ihrer fachlichen Funktion als Pflegekraft auf sämtliche Patientenakten des Klinikums zugreifen. Gleiches galt für die ärztlichen Mitarbeiter des Klinikums. Dass ärztliche Mitarbeiter des Klinikums auch auf Patientenakten anderer Kliniken oder Medizinischer Versorgungszentren (MVZ) des gleichen Konzerns zugreifen können, bestätigte sich im Rahmen der Vor-Ort-Kontrolle des TLfDI hingegen nicht.
Durch das festgestellte, lediglich funktionsbezogene Rollen- und Rechtekonzept wurde die Integrität und Vertraulichkeit der personenbezogenen Patientendaten verletzt, da für den Zugriff von Krankenschwestern auf Patientendaten anderer Stationen als der, auf der sie regelmäßig fachlich tätig waren, kein begründeter Zugriffszweck im Sinne von Art. 5 Abs. 1 Buchstabe b) Datenschutz-Grundverordnung DS-GVO bestand. Damit verstieß das Rollen- und Rechtekonzept des Klinikums gegen Art. 5 Abs. 1 Buchstabe f) DS-GVO. Der TLfDI wies das Klinikum auf diesen Verstoß hin und teilte im Rahmen einer Anhörung mit, dass das Rollen- und Rechtekonzept zu überarbeiten sei.
Die Geschäftsführung des Klinikums war über die datenschutzrechtliche Unzulässigkeit des Zugriffssystems jedoch seitens des in einem anderen Bundesland ansässigen Mutterkonzerns bereits informiert worden. Die Konzernzentrale hatte bereits aufgrund einer datenschutzrechtlichen Intervention des TLfDI in einem anderen Thüringer Klinikum, das ebenfalls zum Konzern gehörte, 2020 begonnen, eine Änderung des Zugriffssystems auf Patientenakten in den konzernzugehörigen Kliniken zu ändern. Die Änderung des Zugriffssystems musste jedoch in allen konzerneigenen Kliniken durch die Konzernzentrale implementiert werden, so auch im beschwerdegegenständlichen Klinikum. Der TLfDI informierte die für die Konzernzentrale zuständige Datenschutzaufsichtsbehörde über das datenschutzrechtliche Defizit im Rollen- und Rechtekonzept.
Das Projekt zur Änderung der Zugriffsrechte wurde mittlerweile abgeschlossen und das neue Rollen- und Rechtekonzept vollständig umgesetzt und von der ausschließlich funktionsbezogenen auf funktionsbezogene, fachbereichsbezogene und fachabteilungsbezogene Zugriffsrechte umgestellt. Dies wird im nächsten Berichtszeitraum vom TLfDI überprüft werden.

3.20 Corona macht's möglich: Gläserne Gesundheitsdaten auf Grundlage der 3G-Regel – oder doch nicht?

Gemäß Art. 9 Abs. 2 Buchstabe g) DS-GVO dürfen personenbezogene Gesundheitsdaten verarbeitet werden, wenn für die Verarbeitung eine Rechtsgrundlage besteht. Demgemäß ist die Verarbeitung dieser Daten zulässig, wenn die entsprechende Rechtsnorm angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht und die Datenverarbeitung aus Gründen eines erheblichen öffentlichen Interesses erforderlich ist. Weder aus der SARS-CoV-2-Verordnung (Thüringer SARS-CoV-2-Infektionsschutz-Maßnahmenverordnung - ThürSARS-CoV-2-IfS-MaßnVO-) in der Fassung vom 23. August 2021 noch aus dem (geänderten) IfSG ist eine Rechtsgrundlag ableitbar, die Gaststättenbetreiber oder deren Personal dazu befugt, Impf- und/oder Informationen zu Coronatests ihrer Gäste einzusehen beziehungsweise zu kontrollieren (verarbeiten).

Ständig änderte sich in der Hochphase der Pandemie die Rechtslage, was in der Bevölkerung oftmals zu Verunsicherung und auch zu vielen Fragen zum Datenschutz führte. So fragte eine Bürgerin beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) an, ob es datenschutzrechtlich zulässig sei, dass jeder Wirt oder Gaststättenbetreiber den Impf- oder Teststatus seiner Gäste kontrollieren dürfe, da es sich bei diesen Daten schließlich um medizinische und damit besonders schützenswerte Daten handele, zu denen nicht jedermann Zugang haben darf.
Der TLfDI teilte der Fragestellerin mit, dass es sich bei personenbezogenen Daten über bestehende Impfungen und/oder medizinische Testungen nach Art. 9 Abs. 1 Datenschutz-Grundverordnung (DS-GVO) um sogenannte besondere Kategorien von Daten handelt, vorliegend Gesundheitsdaten, die einem erhöhten Schutzniveau unterliegen, insbesondere hinsichtlich der Kenntnisnahme durch Dritte. Gemäß Art. 6 Abs. 1 Satz 1 Buchstabe c) DS-GVO und gemäß Art. 9 Abs. 2 Buchstabe g) DS-GVO dürfen personenbezogene (Gesundheits-)Daten verarbeitet werden, wenn für die Verarbeitung eine Rechtsgrundlage besteht, die bestimmte Anforderungen erfüllen muss.
Als Rechtsnormen, aus denen sich für die Verarbeitung von Impf- und Testdaten eine Rechtsgrundlage ableiten ließe, kamen das (geänderte)

Infektionsschutzgesetz (IfSG) und die Thüringer Verordnung zur Regelung infektionsschutzrechtlicher Maßnahmen zur Eindämmung des Coronavirus SARS-CoV-2-Verordnung (Thüringer SARS-CoV-2-Infektionsschutz-Maßnahmenverordnung -ThürSARS-CoV-2-IfS-MaßnVO-) in der Fassung vom 23. August 2021 infrage.
Nach datenschutzrechtlicher Prüfung kam der TLfDI jedoch zu dem Ergebnis, dass sich weder aus den geänderten Normen des IfSG, vorliegend § 28a IfSG, noch aus der ThürSARS-CoV-2-IfS-MaßnVO in der Fassung vom 23. August 2021 für Gastronomiebetreiber eine Befugnis zur Verarbeitung von Impf- und/oder Testdaten ihrer Gäste ableiten ließ. Vielmehr befugten die genannten Rechtsnormen Gastronomiebetreiber lediglich dazu, die Kontaktdaten ihrer Kunden aufzunehmen, das heißt zu verarbeiten.
Für die Verarbeitung (Vorlage, Mitteilung) von Informationen über Impf- und/oder Teststatus von betroffenen Personen gegenüber dem Gastronomiebetreiber sah der TLfDI weder im IfSG noch in der ThürSARS-CoV-2-IfS-MaßnVO in der Fassung 23. August 2021 eine Rechtsgrundlage. Diese war gemäß § 3 Abs. 4 in Verbindung mit § 12 ThürSARS-CoV-2-IfS-MaßnVO lediglich für die Aufnahme von Kunden-Kontaktdaten durch die Gastronomiebetreiber gegeben, jedoch nicht für die Verarbeitung von personenbezogenen Impf- und/oder Testdaten durch den Gastronomiebetreiber. Die zur Verarbeitung dieser Daten berechtigten Personengruppen waren in § 13 ThürSARS-CoV-2-IfS-MaßnVO in der Fassung vom 23. August 2021 benannt und Gastronomiebetreiber zählten nicht zu diesen Personengruppen.
Nach Art. 9 Abs. 2 Buchstabe g) DS-GVO müssen zudem die für die Verarbeitung personenbezogener Gesundheitsdaten bestehenden Rechtsgrundlagen zwingend „(…) spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person“ vorsehen und „(…) den Wesensgehalt des Rechts auf Datenschutz“ wahren. Entsprechende Passagen zur Wahrung der Grundrechte und/oder zum Datenschutz ließen sich jedoch weder im (geänderten) IfSG noch in der ThürSARS-CoV-2-IfS-MaßnVO in der Fassung vom 23. August 2021 finden.

3.21 Wechsel vom ärztlichen Angestelltenverhältnis in die ärztliche Selbstständigkeit – wechseln die Patientenakten in Kopie mit?

Ärzte sind nach § 630f Abs. 3 BGB und nach § 10 Abs. 4 der (Muster-)Berufsordnung Ärzte verpflichtet, „ihre“ Patientenakten mindestens zehn Jahre aufzubewahren. Längere Aufbewahrungsfristen können sich zudem aus spezialgesetzlichen Vorschriften ergeben, beispielsweise aus der Strahlenschutz- beziehungsweise der Röntgenverordnung und dem Transfusionsgesetz. Ist ein/e Arzt/Ärztin als angestellte/r ärztliche/r Mitarbeiter/in beispielsweise in einem MVZ tätig, so ist das MVZ Adressat dieser berufsrechtlichen Aufbewahrungspflichten und nicht der Arzt/die Ärztin. Dieses darf weder die originalen Patientenakten noch eine Kopie der Akten an den/die ausscheidende/n ärztliche/n Mitarbeiter/in weitergeben.

Eine bislang in einem Medizinischen Versorgungszentrum (MVZ) angestellte Ärztin fragte beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) nach, ob sie eine Kopie der vollständigen elektronischen Patientendokumentationen (Patientenakten) „ihrer“ bislang behandelten Patienten „mitnehmen“ dürfe, wenn sie jetzt gemeinsam mit einem ärztlichen Kollegen eine selbstständige Arztpraxis übernimmt. Die Ärztin bat den TLfDI darum, eine datenschutzrechtliche Einzelfallentscheidung zu treffen, um „ihre“ Patienten weiterbehandeln zu können.
Mit ihrer Anfrage hatte sich die Ärztin zunächst an die Kassenärztliche Vereinigung Thüringen (KVT) gewandt. Die KVT hatte der Ärztin unter anderem mitgeteilt, dass bezüglich ihrer Anfrage datenschutzrechtlich gegebenenfalls eine Einzelfallenscheidung getroffen werden könne. Um eine solche Einzelfallentscheidung bat die Ärztin den TLfDI. Dieser teilte der Ärztin mit, dass für eine Übernahme beziehungsweise „Mitnahme“ der (originalen) Patientenakten die Einwilligung der betroffenen Patienten erforderlich sei. Die Patienten der Ärztin müssen ihre Einwilligung dazu erteilen, dass das MVZ ihre Patientendokumentation zur künftigen Weiterbehandlung durch die Ärztin an diese abgeben darf.
Nach Art. 15 Abs. 3 Datenschutz-Grundverordnung (DS-GVO) sind nur die Betroffenen, also die Patienten selbst, befugt, eine Kopie der von ihnen verarbeiteten personenbezogenen Daten, das heißt der Pati-

entenakten, vom Verantwortlichen zu erhalten, jedoch nicht der (weiter-)behandelnde Arzt. Für die Übernahme von originalen elektronischen Patientenakten vom MVZ durch eine/n künftig selbstständige/n Arzt/Ärztin zur medizinischen Weiterbehandlung ist gemäß Art. 9 Abs. 2 Buchstabe a) DS-GVO die Einwilligung der betroffenen Patienten erforderlich.
Gemäß Art. 5 Abs. 1 Buchstabe a) DS-GVO muss jede Form der Verarbeitung personenbezogener Daten auf rechtmäßige Weise erfolgen und bedarf diesbezüglich einer Rechtsgrundlage. Für die medizinische Behandlung ergibt sich diese Rechtsgrundlage gemäß Art. 6 Abs. 1 Satz 1 Buchstabe c) DS-GVO aus dem Behandlungsvertrag, den der Arzt/die Ärztin zu erfüllen hat. Im vorliegenden Fall haben die Patienten „ihren" Behandlungsvertrag mit dem MVZ geschlossen. Somit kann dieser Behandlungsvertrag von der nunmehr selbstständig tätigen Ärztin nicht als Rechtsgrundlage für „ihre" Behandlung der Patienten herangezogen werden. Vielmehr muss die Ärztin mit den Patienten einen eigenen Behandlungsvertrag schließen, aus dem sich für sie unter anderem die Pflicht ergibt, vor der Durchführung einer medizinischen Maßnahme die Einwilligung der Patienten zur Verarbeitung ihrer personenbezogenen Daten, auch aus der Patientenakte, einzuholen (§ 630d Abs. 1 Bürgerliches Gesetzbuch [BGB]). Nach § 630d Abs. 3 BGB kann die Einwilligung durch die Patienten jederzeit und formlos widerruflich erteilt werden, sollte jedoch aus Nachweisgründen im Sinne von Art. 7 Abs. 1 DS-GVO schriftlich eingeholt und der Patientenakte beigefügt werden.
Im Hinblick auf die erforderliche Einwilligung der Patienten zum Übergang ihrer Patientenakten an die Ärztin empfahl der TLfDI als organisatorisch gangbaren Weg, im MVZ und in der künftigen selbstständigen Arztpraxis entsprechende Einwilligungsformulare für die Patienten auszulegen. Der TLfDI übersandte der Ärztin ein entsprechendes Musterformular für eine solche patientenseitige Einwilligung.

3.22 Personalausweis und Krankenversicherungskarte im postalischen Bermudadreieck

Nach Art. 5 Abs. 1 Buchstabe. f) DS-GVO in Verbindung mit Art. 32 Abs. 1 DS-GVO müssen die personenbezogenen Daten von betroffenen Personen so verarbeitet werden, dass eine angemessene Sicherheit

und ein entsprechender Schutz dieser Daten vor unbefugter oder unrechtmäßiger Verarbeitung und Verlust gewährleistet werden. Der Versand von sensiblen personenbezogenen Daten wie Personalausweisen und/oder Krankenversicherungskarten in einem „normalen“ Briefumschlag, die durch den Umschlag ertastet beziehungsweise erfühlt werden können, erfüllt diese Vorgaben nicht.

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) erhält nicht nur zahlreiche Beschwerden von Bürgerinnen und Bürgern über die Verletzung des Schutzes personenbezogener Daten, sondern viele Unternehmen aus dem Gesundheitsbereich, insbesondere Krankenhäuser und Kliniken, informieren den TLfDI darüber, dass es im täglichen Dienstbetrieb zu entsprechenden Datenschutzverletzungen gekommen sei.
Eine solche „Datenpanne“ nach Art. 33 Abs. 1 Datenschutz-Grundverordnung (DS-GVO) meldete ein Thüringer Klinikum dem TLfDI auch im Juli 2021. Das Klinikum hatte einem Patienten seinen Personalausweis und seine Krankenversicherungskarte mittels Einschreiben mit Rückschein übersandt. Kurze Zeit später erhielt das Klinikum den roten Rückschein des Einschreibens ohne Auslieferungsvermerk und ohne Unterschrift des Empfängers zurück. Ein paar Tage später ging beim Klinikum auch der Einschreibe-Brief selbst mit dem Vermerk „Empfänger / Brief unter der angegebenen Anschrift nicht zu ermitteln“ mit handschriftlichem Postzustellungsdatum wieder ein. In der Sendungsverfolgung der Deutschen Post fand sich die Angabe: „Die Sendung konnte nicht zugestellt werden und wurde am an den Absender zurückgesandt.“ Das konkrete Rücksendedatum war angegeben. Der an das Klinikum zurückgesandte Einschreibebrief war seitlich geöffnet worden, Personalausweis und Krankenversicherungskarte waren entwendet.
Das Klinikum hatte den Brief mit der korrekten Empfängeradresse des Patienten versehen; jedoch war der Nachname des Patienten falsch geschrieben. Gleichwohl war das Öffnen des Briefes nicht erforderlich gewesen, um ihn zurück an die Empfängeradresse zu senden, da diese auf der Vorderseite des (ungeöffneten) Briefes stand. Das Klinikum informierte den Patienten über den Vorfall; dieser teilte mit, dass ihm zwischenzeitlich von der Poststelle des Empfängerortes sein Personalausweis übersandt wurde. Die Krankenversicherungskarte des Patienten fehlte jedoch nach wie vor.

Im Rahmen seiner Zuständigkeiten und Aufgaben prüfte der TLfDI, ob das Klinikum nach Art. 5 Abs. 1 Buchstabe f) DS-GVO in Verbindung mit Art. 32 Abs. 1 DS-GVO die personenbezogenen Daten des Patienten auf eine Weise verarbeitet hatte, dass eine angemessene Sicherheit einschließlich des Schutzes vor unbefugter oder unrechtmäßiger Verarbeitung und Verlust gewährleistet werden konnte. Entscheidend hierfür war insbesondere die Frage, ob das Einschreiben mit Personalausweis und Krankenversicherungskarte des betroffenen Patienten in einem normalen Briefumschlag oder in einem Luftpolster- beziehungsweise festen Kartonumschlag versandt wurde.
Auf Nachfrage des TLfDI teilte das Klinikum mit, dass die Dokumente an den betroffenen Patienten in einem normalen Briefumschlag (DL-Umschlag mit den Maßen 110x220 mm) versandt worden waren. Dieser Umschlag ist jedoch für den Versand von sensiblen Dokumenten wie Personalausweis und Krankenversicherungskarte aus datenschutzrechtlicher Sicht problematisch, da man den Inhalt des Briefes, vorliegend die beiden Karten, die die Identität der betroffenen Person enthielten, durch einen solchen Umschlag „erfühlen“ kann. Das Briefgeheimnis, das das unbefugte Öffnen von Briefen unter Strafe stellt, bietet zwar eine angemessene Sicherheit der personenbezogenen Daten gegen unbefugte oder unrechtmäßige Verarbeitung, allerdings können Karten bei einem Luftpolster- oder festen Kartonumschlag nicht „erfühlt“ werden, sodass sensible personenbezogene Daten, die sich auf diesen Karten befinden, zum Schutz und zur Wahrung der Integrität gemäß Art. 5 Abs. 1 Buchstabe f) DS-GVO in Verbindung mit Art. 32 Abs. 1 DS-GVO in diesen Umschlägen versandt werden sollten. Daher empfahl der TLfDI dem Klinikum, in Zukunft entsprechende technische und organisatorische Maßnahmen nach Art. 32 Abs. 1 DS-GVO zu ergreifen, um die Integrität von personenbezogenen sensiblen Daten zu wahren und einer Verletzung des Schutzes dieser Daten vorzubeugen. Das Klinikum sicherte zu, Dokumente mit sensiblen personenbezogenen Daten, die durch den Umschlag ertastet beziehungsweise erfühlt werden können, nicht mit einem normalen Briefumschlag, sondern stattdessen immer in einem Luftposter- oder Kartonumschlag als Einschreiben mit Rückschein zu versenden.
Verantwortlicher für die Verletzung des Schutzes der personenbezogenen Daten des betroffenen Patienten war der Brief- und Paketversanddienstleister Deutsche Post. Zuständige Aufsichtsbehörde für die Deutsche Post ist der Bundesbeauftragte für den Datenschutz und die

Informationsfreiheit (BfDI). Daher übermittelte der TLfDI die Angelegenheit zur Prüfung an den BfDI und wies aufgrund der Verletzung des Briefgeheimnisses auch auf die strafrechtliche Relevanz des Vorfalls (§ 202 Abs. 1 Strafgesetzbuch) hin.
Nach Prüfung teilte der BfDI dem TLfDI im September 2021 mit, dass der Briefumschlag des betroffenen Patienten gegebenenfalls auch in einer Sortieranlage der Post beschädigt worden sein könnte und dass im Falle der mechanischen Beschädigung in der Sortieranlage der Post die im Brief enthaltenen Gegenstände unter die Sortiermaschine fallen, wonach sie in der Regel vernichtet werden, wenn ihnen keine Sendung mehr zugeordnet werden könne. Der TLfDI bedankte sich für diesen Hinweis, wies jedoch darauf hin, dass sowohl Personalausweis als auch Krankenkassen-Chipkarte die personenbezogenen Adressdaten der betroffenen Person enthielten. Gleichwohl wurde dem Empfänger nur der Personalausweis zugesandt; nicht jedoch seine Krankenversicherungskarte. Der BfDI dankte dem TLfDI und teilte mit, dass in dieser Angelegenheit datenschutzrechtlich keine weiteren Handlungsmöglichkeiten für den BfDI bestünden.

3.23 Lieber eine Einwilligung zu viel als eine zu wenig

Grundsätzlich handelt es sich bei der Veröffentlichung von Bildern um eine Verarbeitung personenbezogener Daten der abgebildeten Personen gemäß Art. 4 Nr. 2 Datenschutz-Grundverordnung (DS-GVO) – dies gilt auch für abgebildete Personen auf Flyern für Zwecke der Wahlwerbung. Somit ist eine Einwilligung einzuholen und zu dokumentieren.

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichte eine Beschwerde über die Veröffentlichung von Fotos auf Flyern zum Zwecke der Wahlwerbung, zu der es möglicherweise keine Einwilligung gab. Grundsätzlich handelt es sich nämlich bei der Veröffentlichung von Bildern um eine Verarbeitung personenbezogener Daten der abgebildeten Personen gemäß Art. 4 Nr. 2 Datenschutz-Grundverordnung (DS-GVO), somit war auch der Zuständigkeitsbereich des TLfDI eröffnet. Der TLfDI wollte nun wissen, ob die entsprechende Einwilligung der abgebildeten Personen eingeholt wurde und, falls nicht, auf welcher rechtlichen Grundlage die Veröffentlichung und damit die Verarbeitung von personenbezogenen Daten stattfand.

Dem TLfDI wurde mitgeteilt, dass man annahm, es bedürfe keiner Einwilligung, sofern es sich um Bilder handelt, die zur Zeitgeschichte gehören und nur als Beiwerk erscheinen. Darüber hinaus wurde mitgeteilt, dass es eine Erlaubnis zur Verwendung der Bilder für einen Internetauftritt geben würde. Man sei fälschlicherweise davon ausgegangen, dass dies auch für einen Flyer gelten würden.
Der TLfDI hat daraufhin den rechtlichen Standpunkt verdeutlicht:
Verantwortlich ist nach Art. 4 Nr. 7 DS-GVO, wer über die Zwecke und Mittel der Verarbeitung entscheidet. Für die Veröffentlichung von Fotos von Personen zu Zwecken des Wahlkampfes bedarf es nach Art. 5 Abs. 1 Buchstabe a) DS-GVO einer Rechtsgrundlage. Eine Einwilligung stellt eine Rechtsgrundlage für die Datenverarbeitung nach Art. 6 Abs. 1 Satz 1 Buchstabe a) DS-GVO dar. Sie ist aber nur wirksam, sofern sie den Voraussetzungen des Art. 7 DS-GVO entspricht. Nach Art. 7 Abs. 1 DS-GVO in Verbindung mit Art. 5 Abs. 2 DS-GVO muss der Verantwortliche nachweisen können, dass die jeweils betroffenen Personen in die Verarbeitung ihrer personenbezogenen Daten eingewilligt haben. Damit eine Einwilligung wirksam ist, muss sie folgende Bedingungen erfüllen:
Es bedarf einer unmissverständlich abgegebenen Willensbekundung der betroffenen Person, dass sie mit der Verarbeitung einverstanden ist. Notwendig ist ein aktives Verhalten. Die Einwilligung muss freiwillig erfolgen. Die betroffene Person muss eine echte und freie Wahl haben. Sie muss die Einwilligung jederzeit ohne Nachteile verweigern oder zurückziehen können. Zudem darf zwischen Verantwortlichem und betroffener Person kein klares Ungleichgewicht bestehen, wie es etwa gegenüber Behörden oder im Beschäftigungsverhältnis häufig der Fall ist. In diesen Fällen ist deshalb häufig keine Freiwilligkeit gegeben. Die Einwilligung muss zudem in informierter Weise erfolgen. Die Einwilligungserklärung selbst muss klar und verständlich sein. Zudem muss die betroffene Person darüber informiert werden, wer der Verantwortliche ist und zu welchen Zwecken die personenbezogenen Daten verarbeitet werden sollen. Sie ist darüber hinaus über die Art der verarbeiteten Daten zu informieren und über das Recht, die Einwilligung jederzeit widerrufen zu können.
Wenn ein solcher Nachweis nicht erbracht wird, kann man davon ausgehen, dass ein Verstoß gegen die Dokumentationspflicht nach Art. 5 Abs. 2 DS-GVO und gegen den Grundsatz der Rechtmäßigkeit der Verarbeitung nach Art. 5 Abs. 1 Buchstabe a) DS-GVO vorliegt. Der TLfDI hat daher eine Verwarnung nach Art. 58 Abs. 2 Buchstabe b)

DS-GVO gegenüber den Verantwortlichen ausgesprochen, die mittlerweile rechtskräftig ist.

3.24 Bei Überwachungsverdacht ist der TLfDI zur Stelle

Sofern es in seiner Macht steht, geht der TLfDI jedem Verdacht auf einen Datenschutzverstoß nach. Wenn es erforderlich ist, wird zeitnah eine Vorortkontrolle durchgeführt. Nicht immer bestätigt sich der anfängliche Verdacht.

Schlimmes ließ eine Beschwerde vermuten, die den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) am Ende des Jahres erreichte. Ein Beschäftigter einer Klinik äußerte den Verdacht, dass im Keller der Klinik Tonbandgeräte stünden, die alle Telefonate der Mitarbeiter und der Patienten aufzeichnen. Eine Kollegin hätte beobachtet, wie die Tonbänder ausgewechselt worden seien. Als andere Beschäftigte den Raum besichtigt hätten, seien sie von der Leitung angewiesen worden, über diesen Raum Stillschweigen zu wahren. Weder die Mitarbeiter noch die Patienten seien in irgendeiner Weise aufgeklärt worden.
Da der im Raum stehende Verdacht schwer wog, führte der TLfDI unverzüglich eine Vorortkontrolle durch. Diese wurde angekündigt, damit vorab alle notwendigen Coronaschutzmaßnahmen getroffen werden konnten. Allerdings wurde der konkrete Verdacht in der Kontrollankündigung nicht benannt, damit die Bänder nicht zwischenzeitlich entfernt oder gar vernichtet würden.
Bei der Vorortkontrolle wurde der beschriebene Raum, in dem sich die Bänder befinden sollten, durch die Mitarbeiter des TLfDI in Augenschein genommen. In dem elektrischen Betriebsraum des Klinikums, zu dem ausweislich der Darlegungen der bei der Kontrolle anwesenden Vertreter der Klinik und der getroffenen Festlegungen nur befugte Personen Zutritt haben, befand sich die Telefon- und Datenverarbeitungstechnik des Klinikums. Der TLfDI fand auch Bänder. Hierbei handelte es sich aber nicht um Tonbänder, sondern um Serverbänder für Datensicherungszwecke. Telefongespräche konnten mit diesen Bändern nicht aufgezeichnet werden, hierzu waren sie schlichtweg nicht geeignet. Technik zum Mitschnitt von Telefongesprächen wurde trotz intensiver Suche nicht aufgefunden.
Dies wurde dem Beschwerdeführer mitgeteilt, ohne dass weitere Angaben über die Gegebenheiten vor Ort gemacht wurden. Grund hierfür

ist, dass der TLfDI zwar alles datenschutzrechtlich Relevante überprüfen kann, nähere Informationen zur Durchführung der Datensicherung im Sinne des Art. 5 Abs. 1 Buchstabe f) DS-GVO können aus Sicherheitsgründen aber außenstehenden Dritten nicht detailliert beauskunftet werden. Mit dem Ergebnis zeigte sich der Beschwerdeführer zufrieden.

4. Entschließungen und Beschlüsse



© Matthias Enter - Stickman-idea-solution frage-idee-planung-loesung - fotolia.com

4.1 Coronavirus: Impfnachweis, Nachweis negativen Testergebnisses und Genesungsnachweis in der Privatwirtschaft und im Beschäftigungsverhältnis gehören gesetzlich geregelt!

Entschließung
der Konferenz der unabhängigen Datenschutzaufsichtsbehörden
des Bundes und der Länder
am 29. März 2021

Darf die Teilnahme an privatwirtschaftlichen Angeboten wie Restaurant- oder Konzertbesuche davon abhängig gemacht werden, dass die Besucher und Besucherinnen eine erfolgte Anti-Corona-Impfung oder eine überstandene Infektion nachweisen bzw. ein negatives Testergebnis vorlegen? Neben dieser etwa im Zusammenhang mit dem auf EU-Ebene geplanten „digitalen grünen Zertifikat“ vieldiskutierten Frage erreichen die Datenschutzaufsichtsbehörden fortlaufend Beratungsanfragen von Arbeitgebern, die Gesundheitsdaten wie die Körpertemperatur oder den Impfstatus von Beschäftigten erheben und verarbeiten wollen.
Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) weist darauf hin, dass die Verarbeitung

von Gesundheitsdaten zu privatwirtschaftlichen Zwecken (sei es im allgemeinen Wirtschaftsbereich oder im Beschäftigungsbereich) den Anforderungen der europäischen Datenschutz-Grundverordnung (DSGVO) genügen muss. Informationen über den Impfstatus einer Person sind ebenso Gesundheitsdaten wie das Ergebnis eines Coronatests oder der Nachweis einer überstandenen Infektion. Gesundheitsdaten stehen unter dem besonders strengen Schutz der DSGVO und dürfen nur unter eng zu verstehenden Ausnahmen verarbeitet werden. In aller Regel geboten sind konkrete gesetzliche Regelungen, die eine Verarbeitung solcher Gesundheitsdaten ausdrücklich zulassen, wie es etwa nach § 20 Infektionsschutzgesetz bei der Masernschutzimpfung im Bereich von Kindertageseinrichtungen der Fall ist. Derartige Regelungen zur Nachweispflicht einer Impfung, einer Genesung bzw. eines negativen Tests, um den Zugang zu privatwirtschaftlichen Veranstaltungen oder Einrichtungen zu ermöglichen, fehlen bislang im Zusammenhang mit der Coronapandemie weitestgehend.
In Ermangelung einer gesetzlichen Grundlage bedarf es somit in der Regel einer Einwilligung der Restaurant- oder Konzertbesucher, Arbeitnehmer etc. in die Erhebung und Verarbeitung ihrer Gesundheitsdaten, wobei vor allem im Beschäftigungsbereich die Freiwilligkeit der Einwilligung regelmäßig problematisch ist.
Ohne eine gesetzliche Regelung muss stets im Einzelfall geprüft werden, inwieweit die Verarbeitung von Daten über den Impfstatus oder im Rahmen einer Testung datenschutzrechtlich zulässig ist. Diese Einzelfallbetrachtung ist aufgrund der anzustellenden komplexen juristischen Abwägungen für alle Beteiligten mit großem Aufwand und rechtlichen Unsicherheiten verbunden. Ein uneinheitliches Vorgehen, etwa durch unterschiedliche Regelungen in den Kommunen, könnte zudem zu einer für die Bürgerinnen und Bürger schwer überblickbaren Praxis führen.
Um dies zu vermeiden und für die Datenerhebung und -verarbeitung im privatwirtschaftlichen Bereich Rechtsklarheit, Rechtssicherheit und eine einheitliche Lösung zu erreichen, bedarf es nach Ansicht der DSK einer auf die konkrete pandemische Lage bezogenen, zeitlich befristeten gesetzlichen Regelung. Hierin ist klar und transparent zu regeln, wer, von wem und unter welchen Voraussetzungen Impfdaten, Testergebnisse, Nachweise zu einer überstandenen Infektion und andere Gesundheitsdaten im privatwirtschaftlichen Kontext nutzen darf. Dabei muss das Gesetz den strengen Vorgaben des Artikels 9 Absatz 2 DSGVO genügen.

Die DSK fordert den Gesetzgeber auf, kurzfristig ein entsprechendes Gesetzgebungsverfahren in die Wege zu leiten.

4.2 Chancen der Corona-Warn-App 2.0 nutzen

Entschließung
der Konferenz der unabhängigen Datenschutzaufsichtsbehörden
des Bundes und der Länder
am 29. April 2021

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) erinnert angesichts der bereits seit mehr als einem Jahr andauernden Pandemie und der damit auch im Bereich des Datenschutzes einhergehenden Grundrechtseingriffe an das grundlegende rechtsstaatliche Erfordernis, diese Eingriffe fortlaufend kritisch zu bewerten und zu evaluieren. Die DSK bittet im Zuge einer solchen Evaluation und Anpassung infektionsschutzrechtlicher Instrumente durch Bund und Länder die mit der Version 2.0 der Corona-Warn-App (CWA) eröffneten datensparsameren Möglichkeiten der pseudonymisierten Clustererkennung und Kontaktbenachrichtigung eingehend und zeitnah zu prüfen.
Die DSK empfiehlt den Ländern, die Nutzung der CWA jedenfalls als ergänzende Möglichkeit zur Benachrichtigung potentiell infizierter Personen und zur Clustererkennung in ihren Konzepten zur Pandemiebekämpfung zu berücksichtigen.
Seit dem Update auf die Version 2.0 verfügt die CWA über eine entsprechende Funktion, die genutzt werden kann, um sich an Orten oder Veranstaltungen, wo viele Menschen zusammenkommen, zu registrieren. Auch wenn hierbei – anders als bei anderen Apps – keine personenbezogenen Daten erhoben und später an ein Gesundheitsamt übermittelt werden können, kann die pseudonymisierte Clustererkennung der CWA einen erheblichen Beitrag zur Unterbrechung von Infektionsketten leisten.
Durch die unmittelbare Vernetzung der CWA-Nutzenden werden Personen, die einem potentiellen Infektionsrisiko ausgesetzt waren, unmittelbar und somit schneller als über die Gesundheitsämter informiert. Zudem ist aufgrund der hohen Akzeptanz der CWA mit mittlerweile über 27 Millionen Downloads die Wahrscheinlichkeit hoch, dass Personen auf diese Möglichkeit der aus datenschutzrechtlicher Sicht zu bevorzugenden pseudonymen digitalen Registrierung zurückgreifen.
Die Förderung der Nutzung der CWA zur Clustererkennung könnte dazu führen, dass die App von noch mehr Personen genutzt werden

würde. Dies wiederum würde auch die Chance der Erkennung und Warnung vor Risikobegegnungen außerhalb der Nutzung der Clustererkennung weiter erhöhen und damit aktiv zur Pandemiebekämpfung beitragen.

4.3 „Energieversorgerpool“ darf nicht zu gläsernen Verbraucher*innen führen

Beschluss
der Konferenz der unabhängigen Datenschutzaufsichtsbehörden
des Bundes und der Länder
am 15. März 2021

Bei Auskunfteien und Energieversorgern gibt es Überlegungen, einen sog. Energieversorgerpool zu schaffen. In diesem zentralen Datenpool sollen auch Positivdaten der Kund*innen gespeichert und an andere Energieversorger übermittelt werden. Positivdaten sind Daten über Verträge, bei denen die Belieferten keinen Anlass zu Beanstandungen geben, sich also vertragskonform verhalten.
Informationen über die Anzahl abgeschlossener Verträge und die jeweilige Vertragsdauer können Hinweise darauf geben, ob Verbraucher*innen eine längere Vertragsbeziehung zu einem Stromversorger beabsichtigen oder etwa regelmäßig Angebote für Neukund*innen nutzen. Verbraucher*innen, die regelmäßig das für Sie kostengünstigste Angebot am Markt wählen und dazu den Anbieter wechseln möchten, könnten dann von Versorgungsunternehmen bei preislich attraktiven Angeboten ausgeschlossen werden.
Jede Bürgerin und jeder Bürger hat jedoch das Recht, den Wettbewerb zwischen den Energieversorgern zu nutzen und am Markt nach günstigen Angeboten zu suchen. Der Wunsch, vermeintliche „Schnäppchenjäger“ in einem zentralen Datenpool zu erfassen, um sie bei Vertragsanbahnung als solche identifizieren und ggf. von Angeboten ausschließen zu können, stellt kein berechtigtes Interesse i. S. d. Art. 6 Abs. 1 Satz 1 lit. f) DS-GVO dar. Es war gerade das Ziel des Gesetzgebers, durch die Liberalisierung des Energiemarktes einen wirksamen und unverfälschten Wettbewerb bei der Versorgung mit Elektrizität und Gas zu ermöglichen. Der Versuch, preisbewusste und wechselfreudige Verbraucher*innen zu identifizieren und sie ggf. von bestimmten Angeboten auszuschließen, liefe dieser Zielsetzung zuwider.
Selbst wenn die Interessen der Unternehmen als berechtigt angesehen würden, überwiegen in derartigen Fällen die schutzwürdigen Interessen und Grundrechte der Kund*innen. Vertragstreue Verbraucher*in-

nen dürfen zu Recht erwarten, dass keine über den Vertragszweck hinausgehende Verarbeitung ihrer Daten erfolgt, die ggf. ihre Möglichkeiten einschränkt, frei am Markt agieren zu können.
Die Speicherung und Übermittlung von Positivdaten durch einen Energieversorgerpool würde erheblich zu gläsernen Verbraucher*innen beitragen und wäre nach Art. 6 Absatz 1 Satz 1 lit. f) DS-GVO rechtswidrig.

4.4 Verarbeitung von Positivdaten von Privatpersonen aus Verträgen über Mobilfunkdienste und Dauerhandelskonten durch Auskunfteien

Beschluss
der Konferenz der unabhängigen Datenschutzaufsichtsbehörden
des Bundes und der Länder
am 22. September 2021

Die DSK beschließt Folgendes:
Nach erneuter Prüfung der Rechtslage wird der Beschluss der DSK vom 11.06.2018 aufrechterhalten, so dass weiterhin

1. die Übermittlung und Verarbeitung von sog. Positivdaten an bzw. durch Handels- und Wirtschaftsauskunfteien grundsätzlich nicht auf Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO gestützt werden kann und
2. es für eine Übermittlung und Verarbeitung von sog. Positivdatenregelmäßig einer wirksamen Einwilligung der betroffenen Person unter Beachtung der hohen Anforderungen an die Freiwilligkeit bedarf.

Begründung:
Die DSK hat mit Beschluss vom 11. Juni 2018 festgestellt, dass Handels- und Wirtschaftsauskunfteien sog. Positivdaten zu Privatpersonen grundsätzlich nicht auf Grundlage des Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO erheben können. Dabei sind Positivdaten Informationen, die keine negativen Zahlungserfahrungen oder sonstiges nicht vertragsgemäßes Verhalten zum Inhalt haben, sondern zum Beispiel die Informationen über die Tatsache, dass ein Vertrag abgeschlossen wurde. Bei solchen Positivdaten überwiegt regelmäßig das schutzwürdige Interesse der betroffenen Personen, selbst über die Verwendung ihrer Daten zu bestimmen. Werden die Daten von einem Verantwortlichen an eine Auskunftei übermittelt, ist insoweit bereits die Übermittlung dieser Daten nach Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO regelmäßig unzulässig. Ebenso unzulässig ist die Verarbeitung dieser Daten durch die Auskunftei.
Die DSK hatte nun zu überprüfen, ob für die verbreitete Praxis der Übermittlung und Verarbeitung von Positivdaten zu Verträgen über Mobilfunkdienste und Dauerhandelskonten von Privatpersonen eine andere Bewertung erforderlich ist. Diese Praxis betrifft längerfristige

Verträge, die durch Vorausleistungsverpflichtungen oder Finanzierungs- bzw. Stundungselemente als kreditorische Risiken betrachtet werden, aber keine Vertragsstörungen aufweisen. Sie werden bei der Bildung von Scorewerten der betroffenen Personen, die Handel oder Kreditwirtschaft zur Bonitätsprüfung heranziehen, regelmäßig neben einer Vielzahl weiterer Sachverhalte einbezogen.
Im Rahmen dieser Überprüfung hatten Unternehmen und Verbände bis zum 31. August 2021 Gelegenheit, Stellungnahmen zu den aufgeworfenen Rechtsfragen abzugeben. Nach sorgfältiger Auswertung der eingegangenen Stellungnahmen kommt die DSK zu dem Ergebnis, dass für die Übermittlung der Positivdaten durch die Mobilfunkdiensteanbieter und die Handelsunternehmen zwar berechtigte Interessen bestehen, die Qualität der Bonitätsbewertungen zu verbessern und die beteiligten Wirtschaftsakteure vor kreditorischen Risiken zu schützen. Besondere Umstände, die – wie bei Kreditinstituten insbesondere auf Grund ihrer spezifischen Verpflichtungen nach dem Kreditwesengesetz – entsprechend dem Beschluss der DSK vom 11.06.2018 regelmäßig ein die Interessen, Grundrechte und Grundfreiheiten der betroffenen Person überwiegendes Interesse der Verantwortlichen oder Dritter an der Verarbeitung bestimmter Positivdaten vermitteln würden, konnte die DSK im Rahmen ihrer Überprüfung jedoch nicht feststellen. Eine von der oben genannten Grundregel abweichende Bewertung ist daher nicht begründbar: Auch bei Positivdaten zu Verträgen über Mobilfunkdienste und Dauerhandelskonten kommt den Interessen, Grundrechten und Grundfreiheiten der betroffenen Person, selbst darüber zu bestimmen, ob sie die sie betreffenden Positivdaten für eine Übermittlung durch Mobilfunkdienstleister und Handelsunternehmen und eine Verarbeitung durch Auskunfteien zur Bonitätsbewertung preisgeben will, entscheidende Bedeutung zu. Hierbei fällt besonders ins Gewicht, dass ansonsten unterschiedslos große Datenmengen über übliche Alltagsvorgänge im Wirtschaftsleben erhoben und verarbeitet würden, ohne dass die betroffenen Personen hierzu Anlass gegeben haben. Deshalb können weder Verantwortliche noch Dritte ein überwiegendes Interesse an diesen Verarbeitungen geltend machen.
Eine gegen den Willen der betroffenen Person stattfindende Datenverarbeitung von Positivdaten über Mobilfunkdienstverträge und Dauerhandelskonten durch Vertragspartner und Auskunfteien ist daher unbeschadet anderweitiger Anforderungen nicht nach Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO gerechtfertigt. Ihre datenschutzkonforme

Übermittlung und Verarbeitung ist nur auf der Grundlage einer Einwilligung der betroffenen Person zulässig, für die die allgemeinen Anforderungen gewahrt werden müssen. Insbesondere darf die Erteilung der Einwilligung in die Speicherung des Positivdatums nicht zur Bedingung des betroffenen Vertragsabschlusses gemacht werden.

4.5 Verarbeitungen des Datums „Impfstatus“ von Beschäftigten durch die Arbeitgeberin oder den Arbeitgeber

Beschluss
der Konferenz der unabhängigen Datenschutzaufsichtsbehörden
des Bundes und der Länder
am 19. Oktober 2021

Arbeitgeberinnen und Arbeitgeber dürfen das Datum „Impfstatus“ ihrer Beschäftigten ohne eine ausdrückliche gesetzliche Ermächtigung grundsätzlich nicht verarbeiten – auch nicht im Rahmen der COVID-19-Pandemie.
Als Rechtsgrundlage kommt für die Verarbeitung des Datums „Impfstatus“ von Beschäftigten § 26 Absatz 3 Satz 1 des Bundesdatenschutzgesetzes (BDSG) nicht zum Tragen.
Bei dem Datum „Impfstatus“ handelt es sich um ein Gesundheitsdatum gemäß Artikel 4 Nummer 15 Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung – DS-GVO) und damit um eine besondere Kategorie personenbezogener Daten, Artikel 9 Absatz 1 DS-GVO. Deren Verarbeitung ist grundsätzlich verboten und nur ausnahmsweise erlaubt.
In Einzelfällen ist eine Verarbeitung des Datums „Impfstatus“ auf Grundlage gesetzlicher Regelungen möglich:

- Bestimmte – im Gesetz genannte – Arbeitgeberinnen und Arbeitgeber aus dem Gesundheitsbereich (Krankenhäuser, Arztpraxen usw.) dürfen unter den in §§ 23a, 23 Absatz 3 des Infektionsschutzgesetzes (IfSG) genannten gesetzlichen Voraussetzungen den Impfstatus ihrer Beschäftigten verarbeiten;
- Bestimmte – im Gesetz genannte – Arbeitgeberinnen und Arbeitgeber, zum Beispiel Trägerinnen und Träger von Kindertageseinrichtungen, ambulante Pflegedienste usw., dürfen unter den in § 36 Absatz 3 IfSG genannten Voraussetzungen den Impfstatus ihrer Beschäftigten im Zusammenhang mit COVID-19 verarbeiten;
- Arbeitgeberinnen und Arbeitgeber dürfen den Impfstatus derjenigen Beschäftigten verarbeiten, die ihnen gegenüber einen Anspruch auf Geldentschädigung (Lohnersatz) nach § 56 Absatz 1 IfSG geltend machen. Dessen Voraussetzun-

gen können im Einzelfall auch im Fall einer möglichen Infektion mit CO-VID-19 sowie einer sich anschließenden Quarantäne vorliegen. Anspruchsvoraussetzung ist unter anderem, ob die Möglichkeit einer Schutzimpfung bestand

- Arbeitgeberinnen und Arbeitgeber dürfen den Impfstatus von Beschäftigten auch verarbeiten, soweit dies durch Rechtsverordnungen zur Pandemiebekämpfung auf Basis des IfSG vorgegeben ist.

Die Verarbeitung des Datums „Impfstatus“ von Beschäftigten auf der Grundlage von Einwilligungen ist nur dann möglich, wenn die Einwilligung freiwillig und damit rechtswirksam erteilt worden ist, § 26 Absatz 3 Satz 2 und Absatz 2 BDSG. Aufgrund des zwischen Arbeitgeberinnen und Arbeitgebern sowie ihren Beschäftigten bestehenden Über- und Unterordnungsverhältnisses bestehen regelmäßig Zweifel an der Freiwilligkeit und damit Rechtswirksamkeit der Einwilligung von Beschäftigten.

Im Zusammenhang mit der Abfrage des Datums „Impfstatus“ sind weiter zu beachten:

- Grundsatz der „Datenminimierung“, Artikel 5 Absatz 1 Buchstabe c DS-GVO: Zunächst muss geprüft werden, ob die reine Abfrage des Impfstatus zur Zweckerreichung bereits ausreichend ist. Dann ist keine Speicherung erforderlich. Soll der Impfstatus gespeichert werden, dürfen keine Kopien von Impfausweisen oder vergleichbaren Bescheinigungen (im Original oder als Kopie) in die Personalakte aufgenommen werden. Es ist ausreichend, wenn vermerkt wird, dass diese jeweils vorgelegt worden sind.
- Grundsatz der „Speicherbegrenzung“, Artikel 5 Absatz 1 Buchstabe e DS-GVO, Recht auf Löschung, Artikel 17 DS-GVO: Sobald der Zweck für die Speicherung des Impfstatus entfallen ist, muss dieses personenbezogene Datum gelöscht werden.
- Grundsatz der „Rechenschaftspflicht“, Artikel 5 Absatz 2 DS-GVO: Arbeitgeberinnen und Arbeitgeber müssen – sofern einschlägig – auch die Freiwilligkeit einer Einwilligung nachweisen können, Artikel 7 Absatz 1 DS-GVO.

4.6 Zur Möglichkeit der Nichtanwendung technischer und organisatorischer Maßnahmen nach Art. 32 DSGVO auf ausdrücklichen Wunsch betroffener Personen[2]

Beschluss
der Konferenz der unabhängigen Datenschutzaufsichtsbehörden
des Bundes und der Länder
am 24. November 2021

1. Die vom Verantwortlichen nach Art. 32 DSGVO vorzuhaltenden technischen und organisatorischen Maßnahmen beruhen auf objektiven Rechtspflichten, die nicht zur Disposition der Beteiligten stehen.
2. Ein Verzicht auf die vom Verantwortlichen vorzuhaltenden technischen und organisatorischen Maßnahmen oder die Absenkung des gesetzlich vorgeschriebenen Standards auf der Basis einer Einwilligung nach Art. 6 Abs. 1 UAbs. 1 lit. a DSGVO ist nicht zulässig.
3. Unter Beachtung des Selbstbestimmungsrechts der betroffenen Person und der Rechte weiterer betroffener Personen kann es in zu dokumentierenden Einzelfällen möglich sein, dass der Verantwortliche auf ausdrücklichen, eigeninitiativen Wunsch der informierten betroffenen Person bestimmte vorzuhaltende technische und organisatorische Maßnahmen ihr gegenüber in vertretbarem Umfang nicht anwendet.
4. Kapitel V der DSGVO (Übermittlungen personenbezogener Daten an Drittländer oder an internationale Organisationen) bleibt hiervon unberührt.

[2] Der Beschluss wurde durch die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder gegen die Stimme Sachsens beschlossen.

5. Vorträge und Veranstaltungen

5.1 Vorträge und Veranstaltungen 2021



© Oliver Boehmer - bluedesign®- Schilder Gelb -fotolia.com

Der TLfDI informiert! Der TLfDI ist virtuell unterwegs! –
Das zweite Jahr im Umgang mit der weltweiten Corona-Pandemie hat die Öffentlichkeitsarbeit des TLfDI komplett eingeschränkt. **Großveranstaltungen** gab es daher **keine**. Der TLfDI und das Thüringer Institut für Lehrerfortbildung, Lehrplanentwicklung und Medien (ThILLM) erweiterten ihre Zusammenarbeit im Rahmen des Kooperationsvertrages um eine virtuelle Vortragsreihe zum Thema „Datenschutz beim häuslichen Lernen“. Auch die Vorlesungen des TLfDI an der Rechtsfakultät der Friedrich-Schiller-Universität (FSU) in Jena zur „Einführung in das Datenschutzrecht“ standen den Studierenden wieder virtuell zur Verfügung.

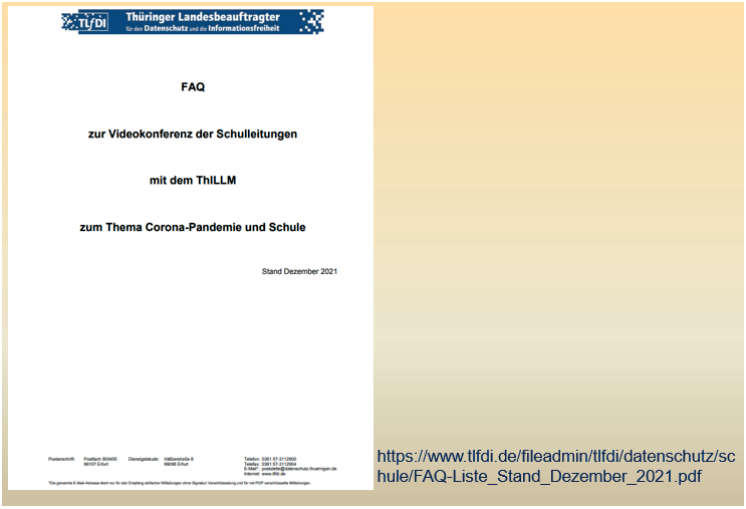
Angeregt durch den gemeinsamen Podcast des Thüringer Instituts für Lehrerfortbildung, Lehrplanentwicklung und Medien (ThILLM) und des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), „Was geht und was darf? Datenschutz im Kontext Schule“ aus dem Jahr 2020 haben beide Institutionen das Thema Datenschutz im schulischen Kontext nunmehr um eine **Videokonferenzreihe** erweitert, um mit diesem **Fortbildungsangebot vor**

allem Schulleitungen zu erreichen Mit diesem Format werden regelmäßig themenbezogene Frage- und Fortbildungsrunden zum Schwerpunkt Datenschutz angeboten. Gestartet ist das Ganze am Safer Internet Day im Februar 2021 mit der Konferenz mit dem Thema „Datensicherheit in der Arbeit mit der Thüringer Schulcloud“. Hier konnten die Teilnehmer:innen ihre Fragen stellen und fachliche Auskunft vom TLfDI als Experten bekommen. Fortsetzungen folgten und folgen! Die Rückmeldungen waren sehr positiv.



Der TLfDI versorgte die Schulleitungen auch mit wichtigen Informationen zur Schulsoftware und dem Datenschutz beim häuslichen Lernen während der Pandemie in Briefform – hier gab es eine große Resonanz, auch außerhalb des Freistaats.

Erstellen von FAQs aufgrund von Videokonferenzen mit den Schulleitungen:


Thüringer Landesbeauftragter
für den Datenschutz und die Informationsfreiheit

FAQ

zur Videokonferenz der Schulleitungen

mit dem ThILLM

zum Thema Corona-Pandemie und Schule

Stand Dezember 2021

https://www.tlfdi.de/fileadmin/tlfdi/datenschutz/schule/FAQ-Liste_Stand_Dezember_2021.pdf

Siehe Link:
https://www.tlfdi.de/fileadmin/tlfdi/datenschutz/schule/FAQ-Liste_Stand_Dezember_2021.pdf

Weiter Informationsschreiben des TLfDI an Schulleitungen:

https://fragdenstaat.de/anfrage/prufungen-und-einschatzungen-zu-an-schulen-verwendeter-anwendungen/640738/anhang/anhang-1-hinweise-zur-thuringer-schulcloud-u-weiterer-software-150121.pdf

https://fragdenstaat.de/anfrage/prufungen-und-einschatzungen-zu-an-schulen-verwendeter-anwendungen/640738/anhang/anhang-2-orientierungshilfe-videokonferenzsysteme.pdf

https://fragdenstaat.de/anfrage/prufungen-und-einschatzungen-zu-an-schulen-verwendeter-anwendungen/640738/anhang/anhang-3-checkliste-ds-in-videokonferenzsystemen.pdf

Die Vorlesungen an der Fakultät der Rechtswissenschaften an der Friedrich-Schiller-Universität in Jena waren ebenfalls wieder online und nur über die Moodle-Lernplattform zu absolvieren.



Der TLfDI folgte einer Einladung der Stiftung Datenschutz zum „DatenTag Online“ nach Berlin:



Link:
https://stiftungdatenschutz.org/veranstaltungen/unsere-veranstaltungen-detailansicht/digitalunterricht-220

Ebenso beteiligte sich der TLfDI wieder als Referent auf dem Forum Bildung der Frankfurter Buchmesse 2021. Das Forum Bildung mit dem Titel „Digitale Bildungsmedien: Wozu braucht es Daten von Lernenden?“ wurde im Rahmen von Frankfurt EDU zum zentralen Treffpunkt für Austausch und Diskussion zu den aktuellen Bildungsthemen in der heutigen Zeit.



News reporter or TV journalist at press conference, holding microphone and writing notes Von wellphoto

Die Presse- und Öffentlichkeitsarbeit beantwortete mehr als **50** Presseanfragen von Journalist:innen. Der TLfDI gab über **20** Interviews und veröffentlichte **24** Pressemitteilungen.

Die Broschüre des TLfDI zu den aktuellen Gesetzen der DS-GVO wurde zum zweiten Mal aufgelegt und aktualisiert.



Link zur Broschüre:
https://www.tlfdi.de/fileadmin/tlfdi/datenschutz/Wir_ueber_uns_-_Musterformulare/Infomaterial/Broschuere_DSGVO_BDSG_DSG_2.Auflage.pdf

Stichwortverzeichnis

3G-Nachweis 2.19
3G-Regel 2.26
Abhilfebefugnisse 1.3
Administrator 1.22
Adoption 3.10
Adoptiveltern 3.10
Akten 1.8
Altersvorsorge, betriebliche 1.9
Amazon 3.16
Amt für Verfassungsschutz 2.4
Amtsarzt 2.7, 1.6
Amtsgericht Erfurt 1.11
Angler 2.9, 2.8
Anhörung 1.11
Anonymisierung 1.23
Anton 1.5
Anwendungshilfe 1.10
Anzeige 3.14
App nora 1.17
Arbeitgeber 3.9, 3.3, 3.1, 2.22, 1.10, 1.1
Arbeitsgericht 3.8
Archiv 2.17
Arzt 3.21, 3.19
Arztwechsel 3.21
Attest 1.6
Attest, ärztliches 3.17
Aufbewahrung 2.17
Aufbewahrungsfrist 3.7, 2.19
Aufbewahrungsrichtlinie für die Behörden des Freistaats Thüringen 2.17
Aufsichtsbehörde, zuständige 2.11
Auftragnehmer 1.13
Auftragsverarbeiter 2.26
Auftragsverarbeitung 1.12, 1.9
Auftragsverarbeitungsvertrag 3.18
Augenblickversagen (Blackout) 3.10

Ausführungsverordnung zum Thüringer Fischereigesetz (ThürFischAVO) 2.9
Auskunftspflicht 2.4
Auskunftsrecht 3.12
Auskunftsverlangen 3.12
Austritt aus der Europäischen Union (EU) 2.1
Ausweis 2.26
Ausweiskopie 2.4
Autohaus 3.13
automatisierter Abruf 1.16
Azubi-Ticket 2.18
Bankdaten 2.18
Beamtengesetz 2.28
Beanstandung 1.3
Beförderungsunternehmen 2.18
Beratung 1.1
berechtigtes Interesse 3.14, 3.13, 3.5, 3.3
Berufsgeheimnis 3.8
Berufsgeheimnisträger 1.18
Beschäftigte 3.24, 3.3, 3.1, 2.28, 1.10, 1.1
Beschäftigtendaten 1.9
Beschäftigungsverhältnis 3.3
Bescheid 3.13
Beschlagnahme 2.3, 1.11
Beschwerde 2.28, 2.27
Beschwerdeverfahren 1.1
Beschwerdeverfahren, strafgerichtliches 2.3
Betriebsvereinbarung 1.10
betroffene Person 2.28, 1.2
Betroffenenrechte 1.17
Beweissicherung 3.11
Bewerberdaten 3.2
Bewerbung 3.6, 3.2
Bilder, Veröffentlichung 3.23
Bilder, Zeitgeschichte 3.23
biometrische Daten 1.16
Bonuszahlung 3.4
Brand- und Katastrophenschutz 1.12
Brexit 2.1
Briefumschlag 3.22

Briefumschlag, verschlossen 2.6
Broschüre 5.1
Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (BfDI) 3.22, 3.8, 1.4
Bundesbehörde 3.8
Bundesgesundheitsministerium (BMG) 1.4
Bürger- und Organisationenpostfach, besonderes elektronisches (eBO) 1.15
Bürgermeister 2.13
Bußgeld 3.14, 3.10, 3.9, 3.6, 3.5, 2.25, 1.11
Bußgeldbescheid 3.8, 1.11
Bußgeldverfahren 1.1
Carsharing-Anbieter 2.3
Chaos-Computer-Club 3.18
Cloud 1.23, 1.7
Cloud-Dienst 1.13
Cloud-Drive 1.13
Corona-Arbeitsschutzverordnung 1.1
Corona-Pandemie 3.20, 3.18, 3.1, 2.26, 2.19, 1.10, 1.8, 1.7, 1.6, 1.4, 1.1
Corona-Test 2.21, 2.20
Coronaverordnung 1.4
Cybersicherheit 1.14
DARFICHREIN 3.18
Data Protection Act 2018 ..... 2.1
Data protection by design 1.14
Dateisystem 2.24
Datendiebstahl 1.22
Datenfeldertabelle 1.4
Datenminimierung 2.17, 2.7, 1.12
Datenschutzbeauftragter 1.12
Datenschutz-Folgeabschätzung 1.12
Datenschutzfolgen-Abschätzung 1.12
Datenschutz-Folgenabschätzung 1.19
Datenschutzniveau, angemessenes 2.1
Datensicherung 3.24
DEHOGA THÜRINGEN e. V. 3.18
Diagnose 1.6
Diagnostik 1.23
Diebstahl 3.11

Dienstplan 2.28
Dienstvorgesetzter 2.28
Digitalisierung 1.7
Digitalkamera 1.23
Diskriminierungsverbot 1.21
Disziplinarverfahren 3.9
Dokumentationspflicht 3.7
Doppeltürprinzip 2.3
Doppelzuständigkeit 3.8
Dritte 3.6, 2.28, 1.9
Drittland 2.1
Drohne 1.12
Duldungsanordnung 3.1
Durchführungsbeschluss 2.1
Durchsuchungs- und Beschlagnahmebeschluss 2.3
EDSA 1.21
EDSB 1.21
Edupage 1.5
Eigentum 3.14
Eingangsbereich 2.14
Einkaufszentrum 3.11
Einschreiben mit Rückschein 3.22
Einspruch 1.11
Einwilligung 3.23, 3.21, 3.15, 3.14, 3.10, 3.7, 3.1, 2.25, 2.15, 2.12, 2.10, 1.12, 1.10, 1.7
Einwilligung, Nachweis der 3.7
Einwohnerantrag 2.13
elektronische Kommunikation 1.15
elektronische Patientenakte 3.21, 3.9
elektronischer Rechtsverkehr 1.15
Eltern 3.10, 3.3, 2.25, 2.22, 2.21, 2.20, 2.19
Elternabend 2.25, 2.19
Elternvertreter 2.25
E-Mail 3.2, 2.22, 2.3, 1.18, 1.11
E-Mail-Account, dienstlicher 2.22
E-Mail-Verteiler 1.2
Erforderlichkeit 2.12, 2.9
Erwerbsminderung 2.16
Erzieher 2.14
Europäische Kommission 1.14

Europäischer Datenschutzausschuss (EDSA) 1.3
Evaluierung 1.3
Exchange-Server 1.22
Exzess 1.11
Fahrdatensätze 2.3
Fahrzeug 3.5
Falschversendung 3.16
Fangbuch 2.8
Fangkarte 2.9
FAQ 5.1
FAQs 1.5
Fassade 3.11
Feuerwehr 2.12, 1.17
Fischerei 2.9
Fischereierlaubnisschein 2.8
Fischereigesetz 2.8
Föderalismus 2.11
Förderrichtlinie 2.10
Forstamt 2.10
Fragebogen über den Kauf von Wohnungseigentum 2.30
Franchise 3.4
Frankfurter Buchmesse 5.1
Freiheitshandels- und Kooperationsabkommen 2.1
Freiwilligkeit 3.15, 3.1, 2.10, 1.12
Friedhofsverwaltung 2.29
Friedrich-Schiller-Universität Jena 5.1
Funkanlagen 1.14
Gastronomie 3.11
Gaststätte 3.20
Geburtsurkunde 3.10
Gefährdungslage 3.11
Gefahrenabwehr 1.12
Gefälligkeitsattest 1.6
Gemeinde 2.13, 2.11
Gemeinderat 2.13
Gericht 2.6
Geschäftszeiten 3.13
Gesetz über das Verfahren bei Einwohnerantrag, Bürgerbegehren und Bürgerentscheid (ThürEBBG) 2.13
Gesundheitsamt 3.18, 1.6, 1.4

Gesundheitsdaten 3.21, 3.19, 3.17, 3.9, 3.1, 2.26, 2.21, 2.20, 2.19, 2.7, 1.10, 1.6, 1.1
Gesundheitsdatum 3.8
GPS-Sender 3.5
Grabstätte 2.29
Grabstätten-Auskunftssystem, digitales 2.29
Großbritannien 2.1
Grundsatz der Verhältnismäßigkeit 1.12
Grundsicherung im Alter 2.16
Grundstück 3.12
Grundstückskauf 2.30
Gutachterausschüsse für Grundstückswerte 2.30
Hacker-Angriffe 1.2
Hafnium 1.22
Händler 3.16
Haushaltsausnahme 3.14
Helmholtz-Zentrum für Infektionsforschung (HZI) 1.4
Hinweisschild 1.12
Hochschule 2.26
hohes Risiko 1.18
Homeoffice 1.8, 1.1
Hotel- und Gaststättengewerbe 3.18
Hygienemaßnahme 3.1
Hygiene-Schutz-Konzept 2.27
Identifikation 2.18, 2.4
Identitätsnachweis 2.26
IGVP (Integrierte Vorgangsbearbeitung Polizei) 1.11
Impfnachweis 3.20, 2.19, 1.10
Impfstatus 3.1
Infektionsschutzgesetz (IfSG) 3.20, 1.10, 1.4
Infektionsschutzgründe 1.1
Informationspflichten 1.12
Initiativbewerbung 3.2
Interessenabwägung 3.11, 1.12
Interessenkonflikt 3.9
Internet 3.1
Intimsphäre 3.9
Jagd 2.10
Jagdbehörde 2.7
JI-Richtlinie 1.3

Jobcenter 2.16
Jugendamt 2.15
Kinder 2.15
Kindergarten 2.14
Klinik 3.24
kommunale Unternehmen 2.5
Kommunalordnung 2.13
Kommune 2.11, 2.5
Kontaktdaten 3.20, 3.18
Kontaktnachverfolgung 3.18, 2.19
Kontoauszug 2.18
Kontoauszug, Vorlage von 2.16
Kopie 3.6, 2.7
Koppelungsverbot 3.4
Kopplungsverbot 3.15
Krankenhaus 3.22, 3.19, 3.9, 1.23, 1.2
Krankenversicherungskarte 3.22
Kultusministerkonferenz (KMK) 1.7
Kundendaten 3.16
Kündigung 3.3
Künstliche Intelligenz (KI) 1.21
Landesamt für Bodenmanagement und Geoinformation (TLBG) 2.30
Landeshaushalt 2.10
Landeshaushaltsordnung 2.5
Landeskriminalamt (LKA) 2.3
Landesregierung 1.3
Landtag 1.3
Lehrer 2.25, 2.24, 2.21, 2.19, 1.5
Leitfaden für die Videoüberwachung durch öffentliche Stellen in Thüringen 1.12
Lichtbild 1.16
Logging 1.22
Löschkonzept 2.17, 1.4
Löschpflicht 2.17
Löschung 3.17, 3.7, 2.2, 1.12
Makler 3.6, 1.9
Maskenpflicht 3.17, 2.19, 1.6
Medieninteresse 3.1
Medizinisches Versorgungszentrum (MVZ) 3.21, 3.19
Meldung nach Art. 33 Abs. 1 DS-GVO 1.11

Meldung nach Art. 33 DS-GVO 3.22, 1.2, 1.1
Microsoft 1.22, 1.7
Microsoft 365 ..... 1.13
Microsoft 365 (bisher Office 365) 1.7
Mieter 3.15
Mieterselbstauskünfte 3.15
Minderjährige 3.10
Minderjähriger 3.3
Missbrauch von Sozialleistungen 2.16
Mitarbeiterexzess 3.8
Monitoring 1.12
Moodle 1.5
Mund-Nasen-Bedeckung 3.1, 2.23
Mundo 1.5
Nachbarn 3.14
Nachstellung 3.5
natürliche Personen 2.29
Netzwerk 1.22
Neugliederung Gebietskörperschaft 2.17
Noten 2.24
Notruf 1.17
Nutzerkonto 1.15
Nutzungsverbot 2.25
Offenbarung 3.16, 2.6
öffentliche Gewalt 1.12
öffentliche Stelle 2.11
öffentlicher Raum 3.14
Office 365 ..... 1.13
Online-Plattformen 1.5
Online-Service-Terms 1.13
Onlinezugangsgesetz (OZG) 1.15
Opportunitätsgrundsatz 1.11
Ordnungsbehörde 1.12
Ordnungswidrigkeit 3.14, 3.8, 3.5, 1.12, 1.11
Ordnungswidrigkeitenanzeige 3.8
Orientierungshilfe 3.15, 1.18
Orientierungshilfe zu Flugdrohnen im öffentlichen Bereich 1.12
Paket 3.16
Papiercontainer 1.11
Pass- und Personalausweisdatenabrufverordnung 1.16

Passregister 1.16
Patienten 3.24
Patientenakte, elektronische 3.19
Patientenakten 1.11
Personalangelegenheiten 1.2
Personalausweis 3.22, 3.15, 3.6
Personalausweiskopie 2.18
Personaldaten 3.3
Personalverwaltung 3.2, 2.28
Personenbezug 1.23
Personensorge 2.15
Personenstammdaten 2.3
Pflegepersonal 3.19
Pilotprojekt 1.7
PKW 2.3
Planen und Spezifizieren 1.19
Polizei 3.14, 2.3, 2.2, 1.17
polizeiliches Informationssystem 2.2
Polizist 1.11
Posteingänge 1.1
Postfach, zentrales 2.27
postmortales Persönlichkeitsrecht 2.29
private Zwecke 3.12, 3.5
Prüfbericht 2.5
Prüffrist 2.2
Psychotherapeut 3.9
Psychotherapeutenkammer 3.9
QR-Code 3.18
Quarantänemaßnahmen 2.21
Ransomware 1.22
Rechnung 3.16
Rechnungs- und Kassenprüfung 2.5
Rechnungshof 2.5
Rettungsdienst 1.17
Risikoabschätzung 1.12
Roboter 1.23
Rollen- und Berechtigungskonzept 1.20
Rollen- und Rechtekonzept 3.19
Rundschreiben 3.8, 2.25, 1.5, 1.1
Sachverhaltsermittlung 3.12

Schrems II 1.7
Schrems II-Urteil des Europäischen Gerichtshofs 1.5
Schulamt 2.24, 1.6
Schulbereich 1.13
Schulcloud 1.5
Schule 2.25, 2.24, 2.23, 2.22, 2.21, 2.20, 1.7, 1.6, 1.5, 1.1
Schüler 2.24, 2.22, 2.21, 2.20, 2.19, 1.5
Schülername 2.23
Schulleitung 5.1
Schulpflicht 1.6
Schulsekretariat 2.23
Schulsoftware 1.7
Schulverwaltungsamt 2.23
Schwärzung 2.16
Schwerbehindertenvertretung 3.8
Schwerbehinderung 3.8
Servicekonto 1.15
sexuelle Belästigung 3.9
Sicherheitsdienst 2.26
Sicherheitslücke 1.22
Social Scoring 1.21
Software zur Kontaktnachverfolgung 1.4
Sorgerecht 3.10
SORMAS 1.4
Sozialhilfeakte 2.17
Sozialsphäre 3.11
Spam-Filter 1.11
Sparkasse 2.27
Speicherbegrenzung 1.12
Speicherdauer 3.17, 3.13
Speicherfrist 2.2
Staatsanwalt 3.5
Staatsanwaltschaft 2.7, 1.11
Stadtrat 2.28
Stadtverwaltung 2.28
Standard-Datenschutzmodell (SDM) 1.20, 1.19
Standesamt 3.10
Standortdaten 3.5
Statistik 1.1
Steckbrief 3.1

Straftat 3.11, 2.2
Strafverfolgung 1.12
Student 2.26
Subunternehmen 3.18
Suchmaschine 2.29
technische und organisatorische Maßnahmen 1.12
Telearbeit 1.8
Thüringer Datenschutz-Anpassungs- und Umsetzungsgesetz EU - ThürDSAnpUG-EU 1.3
Thüringer Gesetz zur Förderung der Teilnahme an Früherkennungsuntersuchungen für Kinder (ThürFKG) 2.15
Thüringer Institut für Lehrerfortbildung, Lehrplanentwicklung und Medien (ThILLM) 5.1
Thüringer Ministerium für Arbeit, Soziales, Gesundheit, Frauen und Familie 3.18, 1.4
Thüringer Ministerium für Bildung, Jugend und Sport 2.25, 2.23, 2.19
Thüringer Ministerium für Infrastruktur und Landwirtschaft 2.10, 2.8
Thüringer Oberverwaltungsgericht 3.12
Thüringer Schulordnung 2.25
Thüringer Verordnung über Prüffristen bei vollzugspolizeilicher Datenspeicherung (ThürPolPrüffristVO) 2.2
Tonband 3.24
Tracking 1.5
Transportverschlüsselung 3.18
Trinkwasserversorgung 2.12
Übermaßverbot 1.12
Überwachung, Telefon 3.24
Umweltimmission 1.12
Unschuldsvermutung 1.11
Unternehmen 3.2
Untersagung 3.11
Unterschriftenliste 2.13
USA 2.25
Veranstaltung 5.1
Verarbeitungsgrundsätze 1.3
Verdienstbescheinigungen 3.15
Verein 2.9
Vereinigtes Königreich 2.1
Verfassungsschutz 2.4

Verfolgungsverjährung 1.11
Vergütungsstruktur 2.5
Verhältnismäßigkeit 3.1
Verletzung des Schutzes personenbezogener Daten 3.16
Vermieter 3.15, 3.6
Veröffentlichung 3.1
Verpixelung 3.13, 1.12
Versammlungsgesetz 1.12
Verschlüsselung 3.18, 2.3, 1.22, 1.18, 1.2
Verstorbene 2.29
Vertrauensperson 3.8, 2.13
Verwaltungsgericht 2.11
Verwarnung 3.23, 2.22, 1.11
Videoaufzeichnung 2.14
Videobeobachtung 2.14
Videokamera 1.12
Videokonferenz 1.5, 1.1
Videoüberwachung 3.14, 3.13, 3.12, 3.11, 2.14, 1.12, 1.1
Vorortkontrolle 3.24
Vor-Ort-Kontrolle 3.19, 3.1
Vorsorgeuntersuchung 2.15
Vorsorgezentrum 2.15
Vortrag 5.1
Vorverfahren 1.11
vorvertragliches Schuldverhältnis 3.15
Wählerliste 3.8
Wahlwerbung 3.23
Web-Plattform einführen 2.29
Web-Portal 3.5
Wegerecht 3.14
Weitergabe 2.27
Werbung 3.4
WhatsApp 2.25
wissenschaftliche Zwecke 1.4
Wohnung 3.6
Wohnungseigentum 2.30
Zeuge 1.11
Zufahrt 3.14
Zugriffsrechte 1.22
Zutrittskontrolle 3.18

Zwangsgeld 3.8
Zweckbindung 2.5
Zweckverband 2.12
Zwischenverfahren 1.11