TLfDI

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



2023

6. Tätigkeitsbericht zum Datenschutz nach der DS-GVO

6. Tätigkeitsbericht zum Datenschutz nach der DS-GVO | 2023

TLfDI

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:	Juni 2024

6. Tätigkeitsbericht zum Datenschutz nach der DS-GVO

des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit

Berichtszeitraum: 1. Januar 2023 bis 31. Dezember 2023
Zitiervorschlag: 6. TB DS-GVO LfDI Thüringen

Der 6. Tätigkeitsbericht DS-GVO steht im Internet unter der Adresse www.tlfdi.de zum Abruf bereit.

Erfurt, im Juni 2024

Tino Melzer

Thüringer Landesbeauftragter für den Datenschutz
und die Informationsfreiheit

Inhaltsverzeichnis

Inhaltsverzeichnis.....2

Vorwort.....6

1. Themengebiete.....25

1.1 Schwerpunkte im Berichtszeitraum einschließlich Statistik25

1.2 EU-Angemessenheitsbeschluss zur Datenübermittlung in die USA vom Juli 2023 – Die „unendliche Geschichte“ wird fortgeschrieben….....27

1.3 ChatGPT und KI 33

1.4 Auftragsverarbeitungsvereinbarung hinsichtlich Microsoft 365.....37

1.5 Umfang und Inhalt des Anspruchs auf Auskunft und Kopie 39

1.6 Gesetz zur Änderung des BDSG.....41

1.7 Kriterien für Souveräne Clouds 43

1.8 Cybersicherheitslage 46

1.9 AK Schulen und Bildungseinrichtungen und AK Datenschutz-/Medienkompetenz.....49

1.10 Handreichung zur „Digitalen Selbstverteidigung“.....52

1.11 Digitalisierung im Gesundheitswesen.....53

1.12 Mögliche Interessenkonflikte eines behördlichen Datenschutzbeauftragten.....56

1.13 Hinweise zur Videoüberwachung im Nachbarschaftsbereich. 61

1.14 Videogaga 2.0: Zur aktuellen Problematik der Videoüberwachung in Thüringer Kommunen.....67

1.15 Nachgefragt – Verbesserungsbedürftige Aspekte beim Amt des kommunalen Datenschutzbeauftragten.....70

1.16 Kleiner Fehler, große Wirkung – Der Versand von E-Mails in „cc“ 71

1.17 Arbeitsunfähig? Was muss man dem Arbeitgeber mitteilen? 73

1.18 Datenschutz kontra Archivwesen: Corona-Impfdaten für die Nachwelt – wen interessiert das? 74

1.19 Wichtige Entscheidungen des EuGH im Berichtszeitraum 76

1.20 Etwas Gutes aus Europa: Die Arbeit des Europäischen Datenschutzausschusses zur einheitlichen Anwendung der Datenschutzregeln 80

2. Fälle öffentlicher Bereich 83

2.1 Müssen Polizisten für den Dienstherrn ständig erreichbar sein? 83

2.2 „Buttersäure-Gate“: Herausgabe von Kundendaten an die Polizei aufgrund eines Durchsuchungsbeschlusses 85

2.3 Übermittlung von Personalaktendaten an den Untersuchungsausschuss 7/4 87

2.4 Kennzeichenerfassung auf dem Parkplatz eines bekannten Thüringer Ausflugszieles 91

2.5 Offenlegung eines Kfz-Kennzeichens auf einem „Knöllchen“ ist zulässig 93

2.6 Geordnete wirtschaftliche Verhältnisse? 95

2.7 Unzulässige Übermittlung einer IBAN durch eine Kommune 99

2.8 Wenn die Beschwerde zulässig, aber in der Sache unbegründet ist 101

2.9 Kita-Apps können viel, dürfen aber nicht alles… Ohne Einwilligung der Eltern müssen Informationen auch auf anderem Weg ausgetauscht werden 103

2.10 Wenn die Einwilligung zur Veröffentlichung von Schülerfotos im Internet fehlt, darf dies nicht zu Nachteilen führen 105

2.11 Abfrage in Schule zu Läusebefall 108

2.12 Unentgeltliche Kopien – ja! Aber in welcher Form? 111

2.13 Anfrage zur Weitergabe von Meldedaten durch eine Stadtverwaltung für das Mammographie-Screening-Programm 113

2.14 Woher, wer und wieso – Transparenz ist alles und ohne Transparenz ist alles nichts, besonders im Datenschutz! .. 116

2.15 Krankheit oder Versagensangst – darf eine Hochschule für den Nachweis der Prüfungsunfähigkeit eine ärztliche Diagnose verlangen? 119

2.16 Beschwerde über Versand von Langzeitstudiengebührenbescheiden an alle Betroffenen durch eine Thüringer Hochschule 122

2.17 Anfrage von Schülern zur Erstellung eines Instagram-Accounts für die Schule im Rahmen einer Seminarfacharbeit 124

3. Fälle nicht-öffentlicher Bereich 127

3.1 Insolvenzverwalter hat Verpächterdaten an die Käuferinnen der Insolvenzschuldnerin weitergegeben 127

3.2 Ausweiskopie bei Blutspende nicht erforderlich 132

3.3 Wenn der Arbeitgeber durch ein arbeitsmedizinisches Tauglichkeitsgutachten mehr erfährt als er sollte 137

3.4 Wenn eine private Auseinandersetzung zu einem Mitarbeiterexzess führt 140

3.5 Nichts ist so, wie es scheint – auch nicht die Patientenquittung 144

3.6 Wer will was und weswegen? – Die Durchsetzung von Rechtsansprüchen im gerichtlichen Verfahren – geht das ohne personenbezogene Daten? 146

3.7 Besteht ein Auskunftsrecht nach Art. 15 der Datenschutz-Grundverordnung zwischen Internetforumsmitgliedern? .. 149

3.8 Wohnmobilstellplatz unter Dauerbeobachtung 151

3.9 Webcamaufnahmen eines öffentlichen Platzes – nicht mit Personenbezug! 155
3.10 Campingplatz Kfz-Kennzeichenerfassung 157
3.11 Waldspaziergang unter Beobachtung 161
3.12 Videoüberwachung in Supermarkt 164

4. Vorträge und Veranstaltungen 168
4.1 Vorträge und Veranstaltungen 168

5. Entschließungen und Beschlüsse 177
5.1 Notwendigkeit spezifischer Regelungen zum Beschäftigtendatenschutz! 177
5.2 Verfassungsrechtliche Anforderungen bei automatisierter Datenanalyse durch Polizei und Nachrichtendienste beachten! 180
5.3 Geplante Chatkontrolle führt zu einer unverhältnismäßigen, anlasslosen Massenüberwachung! 182
5.4 Datenschutz in der Forschung durch einheitliche Maßstäbe stärken 184
5.5 Rahmenbedingungen und Empfehlungen für die gesetzliche Regulierung medizinischer Register 188
5.6 Zur datenschutzrechtlichen Bewertung von Zugriffsmöglichkeiten öffentlicher Stellen von Drittländern auf personenbezogene Daten 194
5.7 Bewertung von Pur-Abo-Modellen auf Websites 198

Stichwortverzeichnis 200

Vorwort

Der Berichtszeitraum des Jahres 2023 unterfällt der Verantwortung meines Amtsvorgängers, Herrn Dr. Lutz Hasse. Das folgende Vorwort hat er für seinen letzten Tätigkeitsbericht vorgesehen und es wird hier nahezu vollständig in der Fassung abgedruckt, die durch ihn gezeichnet wurde.

„Liebe Leserinnen und Leser,

mit dem vorliegenden 6. Tätigkeitsbericht endet die zwölfjährige Amtszeit von Herrn Dr. Hasse. Deshalb sei es erlaubt, an dieser Stelle nicht nur einführende Worte zum aktuellen Berichtszeitraum, sondern auch zu einigen wesentlichen Aktivitäten, die der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) in diesen zwölf Jahren auf den Weg brachte, zu verlieren.
Von Beginn seines Amtes an wurde schnell sichtbar, dass der TLfDI die Durchsetzung des Datenschutzrechts ernst nimmt und seine Datenschutzaufsicht in völliger Unabhängigkeit, ohne äußere Einflussnahme wahrnahm. Mit der Übernahme des nicht-öffentlichen Bereichs Ende 2011 vom bis dahin zuständigen Landesverwaltungsamt stiegen die registrierten Posteingänge beim TLfDI von 4.120 im Jahre 2011 auf 5.757 im Jahre 2013. In diesem Zusammenhang musste die Behörde von da an Ordnungswidrigkeitenverfahren durchführen, ohne dass hier auf Erfahrungen im Datenschutzbereich zurückgegriffen werden konnte. Da zahlreichen Thüringer Unternehmen die datenschutzrechtlichen Regelungen vielfach unbekannt waren, bemühte sich der TLfDI um einen steten und intensiven Austausch mit den in Thüringen vertretenen Industrie- und Handelskammern (IHK), gründete mit der IHK Erfurt einen „Runden Tisch“ und initiierte unter anderem Informationsveranstaltungen auf Unternehmermessen der IHK. Ein weiterer Schwerpunkt der späteren datenschutzrechtlichen Arbeit wurde bereits damals sichtbar: das Problem der Videoüberwachung und die mangelnde Einsicht der Verantwortlichen, dass dies in den meisten Fällen unzulässig ist. Mit Inkrafttreten des Thüringer Informationsfreiheitsgesetzes fiel an den TLfDI auch die Aufgabe des Informationsfreiheitsbeauftragten. Herrn Dr. Hasse gelang es, die wachsende Aufgabenfülle mit der Gewinnung von neuen Stellen beim TLfDI einigermaßen abzufedern.

2012 wurde dem TLfDI aus Medienberichten bekannt, dass das Thüringer Landeskriminalamt (TLKA) seit zwei Jahren versuchte, den Diebstahl von Toilettenpapierrollen aufzuklären. Zum Ergreifen eine/s/r möglichen Täter/s/in hatte das TLKA seit Anfang 2011 verdeckte Videoaufnahmen angefertigt. Es konnte aber kein Täter ermittelt werden. Auch die inzwischen eingeschaltete Staatsanwaltschaft stellte das Verfahren ergebnislos ein. Die datenschutzrechtliche Prüfung des Falls erwies sich für den TLfDI als schwierig, da das TLKA die vom TLfDI geforderten Unterlagen nicht an diesen übermittelte. Diese mangelnde Unterstützung wurde nach der damaligen Rechtslage neben anderen Rechtsverstößen vom TLfDI beanstandet.
Das Jahr 2013 war aus datenschutzrechtlicher Sicht als besonders spannend zu bezeichnen war. Denn 2013 gab es erste Presseberichte darüber, dass ein US-Telefonkonzern der National Security Agency (NSA) detaillierte Verbindungsdaten, wie Rufnummer, Dauer und Uhrzeit, zur Verfügung stellte. Wenig später wurde zusätzlich die Zugriffsmöglichkeit der NSA auf neun Internetfirmen bekannt. Damit überwachte die NSA Audios, Videos, Fotos, E-Mail, Dokumente und Verbindungsdaten, um Kontakte und Bewegungen einer Person nachvollziehen zu können. Diese Informationen stammten von einem Ex-NSA-Beschäftigten mit Namen Edward Snowden. Der TLfDI bewertete als einer der Ersten Snowdens Enthüllungen „als schon heldenhaft, sich gegen solche Organisationen aufzulehnen“. Ohne solche Leute wären wir auf solche Parallelwelten nicht gestoßen. Für den TLfDI bot sich wenig später die Gelegenheit, mit dem von ihm eingeladenen damaligen US-amerikanischen Generalkonsul Mark J. Powell über die NSA-Affäre zu sprechen. Als Lehre aus der Affäre riet der TLfDI dazu, Verschlüsselungsmechanismen bei Dateien und E-Mails und beim Surfen im Internet Anonymisierungsdienste zu verwenden. Auf die Verwendung von Cloud-Computing sollte man verzichten. „Erst die Kopplung all dieser und weiterer Instrumente, von Millionen Usern tagtäglich praktiziert, macht die Auswertung der Daten für die Geheimdienste damit so aufwändig und unerschwinglich, dass hinreichender Datenschutz ‚im Kleinen‘ wieder gewährleistet scheint. ‚Im Großen‘ bleibt die Bundesregierung gefordert, auf politische Lösungen hinzuwirken.“
Wie nicht anders zu erwarten, wuchs der Arbeitsanfall beim TLfDI in den Jahren 2014/2015 weiter an. Dies zeigte sich auch im Umfang des Tätigkeitsberichts, der eine Trennung des Öffentlichen Bereichs und des nicht-öffentlichen Bereichs in zwei Bänden erforderlich machte.

Insgesamt wurden in den beiden genannten Jahren 28.975 Dokumente erstellt, darunter 13.519 Posteingänge. Die Forderung nach einer weiteren Aufstockung des Personals wurde unumgänglich. Thematisch warf die vor der Tür stehende Datenschutz-Grundverordnung (DS-GVO) ihren Schatten voraus. Damit das gemeinsame europäische Datenschutzrecht nicht unter den Standard des in Deutschland bestehenden Datenschutzniveaus fällt, wirkte der TLfDI an Positionspapieren und Entschließungen der Datenschutzkonferenz zur Datenschutz-Grundverordnung mit. Große Unsicherheit machte sich bei der Übermittlung von personenbezogenen Daten aus Europa in die USA breit, als der Europäische Gerichtshof in seiner Entscheidung vom 6. Oktober 2015 (Az.: C-362/14) die „Safe-Harbor"-Entscheidung der EU-Kommission für unwirksam erklärte. Damit konnten ab sofort Übermittlungen personenbezogener Daten aus Europa an Unternehmen in den USA nicht mehr auf den „Safe-Harbor"-Beschluss der Europäischen Kommission gestützt werden. Als Nachfolgeabkommen stand „EU-US Privacy Shield" in den Startlöchern. Aber auch hierzu hagelte es bereits früh Kritik von den Europäischen Datenschutzbeauftragten, da nach deren Auffassung auch die neue Regelung nicht mit dem Europäischen Datenschutzstandard vereinbar war.
Auch die Jahre 2016/2017 zeigten eine weitere Zunahme der Posteingänge um 50 Prozent von 2016 zu 2017. Diese signifikante Erhöhung war sicherlich auf die Datenschutz-Grundverordnung zurückzuführen, die dann ab Mai 2018 ihre Wirkung entfaltete. In diesem Zeitraum wurden viele Kapazitäten des TLfDI durch die Thüringer Polizei gebunden. Wie publik wurde, zeichnete die Polizei auch Telefonate von polizeilichen Telefonapparaten auf, die gar keine Notrufe darstellten. Die Ursache fand sich in einer unzureichend umgesetzten Dienstanweisung sowie darin, dass neue und vorhandene Technik nicht miteinander abgestimmt waren. Eine Beanstandung wurde ausgesprochen. Eine weitere Affäre stellte der Einsatz der Software „Device Watch" dar, mit der man je nach Konfiguration das Verhalten von Mitarbeiterinnen und Mitarbeitern am PC kontrollieren kann. Hier wurden ebenfalls wegen Verstößen gegen das Datenschutzrecht als auch gegen das Personalvertretungsrecht Beanstandungen ausgesprochen. Zur Vertrauensbildung wurden Polizeibeamtinnen und Polizeibeamte an den TLfDI entsandt, um dessen Arbeitsweise und Arbeitsinhalte kennenzulernen. Auch der TLfDI profitierte von dem Gedankenaustausch mit den entsandten Polizeikräften, indem sich ein besseres wechselseitiges

Verständnis entwickelte. Die zur Polizei zurückkehrenden Polizeikräfte wurden als behördliche Datenschutzbeauftragte eingesetzt, sodass auf diesem Wege eine datenschutzrechtliche Nachhaltigkeit erzeugt werden konnte.
Zufrieden war der TLfDI mit der Entwicklung im kommunalen Bereich. Die Kommunen gingen vermehrt dazu über, den TLfDI bereits vor einer Datenverarbeitung zu Rate zu ziehen und nicht erst, wenn das Kind in den Brunnen gefallen war.
Ein vom TLfDI aufgedeckter Aktenskandal erreichte 2017 sein vorläufiges Ende. Bereits 2013 hatte der TLfDI ein herrenloses Hartmetallwerk in Immelborn (Wartburgkreis) durchsucht. Dabei wurde festgestellt, dass circa eine Million Personal- und Firmenakten sowie Unterlagen aus Anwaltskanzleien und Arztpraxen mit teilweise sensiblen Inhalten seit Jahren in den Werkshallen ohne weitere Schutzmaßnahmen lagerten. Der TLfDI prägte damals den Begriff vom „Fukushima für den Datenschutz“. Da die Sicherung und der weitere Umgang mit dieser Aktenmenge die Kräfte der eigenen Behörde weit überschritten hätte, bat der TLfDI die Thüringer Polizei um Amtshilfe bei der „Beseitigung des Chaos“. Die Polizei verweigerte unverständlicherweise mit argumentativer Schützenhilfe durch das Thüringer Innenministerium ihre Unterstützung. Aufgrund der Weigerung des Innenministeriums, dem TLfDI die erbetene Amtshilfe zu leisten, verhärteten sich zwischen beiden Stellen die Fronten. Da sich keine Lösung abzeichnete, reichte der TLfDI beim Verwaltungsgericht Weimar Klage gegen das Innenministerium ein, mit dem Ziel, die Polizei zur Amtshilfe zu verpflichten. Inzwischen wollte die CDU-Fraktion des Thüringer Landtags in einem Untersuchungsausschuss klären lassen, ob der TLfDI die Klage erhoben hätte, um dem Innenminister in seinem Wahlkampf zu schaden […]. Währenddessen hatte der TLfDI in Eigenregie mit Hilfe eines „Sponsors“ Anfang 2015 eine Möglichkeit gefunden, das wilde Aktenlager zu räumen und die Akten innerhalb von zwei Monaten zu vernichten oder den zuständigen Stellen zurückzugeben. Der Zwischen- und Endbericht zum Untersuchungsausschuss zur „Causa Immelborn“ kam dann auch zu dem Ergebnis, dass sowohl das Amtshilfeersuchen des TLfDI an die Polizei als auch sein Vorgehen bei der Auflösung des Aktenlagers rechtmäßig waren. Außerdem hatte sich der von der CDU-Fraktion geäußerte Verdacht, dass der TLfDI mit seiner Klage auf Amtshilfe der Hausleitung des Thüringer Innenministerium angeblich hatte schaden wollen, nicht erhärtet. Es stellte sich schließlich auch heraus, dass die Thüringer Polizei

den TLfDI bei der Bewältigung des Aktenproblems unterstützen wollte, daran aber im September 2013 vom Thüringer Innenministerium gehindert worden war.
Wie in den Jahren zuvor stieg die Zahl der Beschwerden über Videoüberwachung weiter rasant an. Die Beispiele sind unzählig, sei es die Installation von Wildkameras, die Überwachung von Wohnanlagen, die Beobachtung und Aufzeichnung von öffentlichen Plätzen oder die Videoüberwachung von Nachbarn, von Geschäftsräumen, Restaurants, Biergärten, Mitarbeitern, Straßenabschnitten durch Private und so weiter.
Die Geltung und damit Umsetzung der DS-GVO ab dem 25. Mai 2018 stellten für die Unternehmen und Behörden eine Herausforderung dar und führte zu einer weiteren Mehrarbeit beim TLfDI, etwa aufgrund der Flut von Beratungsanfragen und der angefragten Beurteilung von ergriffenen Umsetzungsmaßnahmen. Zusätzlich erarbeitete der TLfDI Informationsmaterialien und zahlreiche Muster, zum Beispiel für die Meldung von Datenpannen oder die Meldung von berufenen Datenschutzbeauftragten. Der Verunsicherung bei den Verantwortlichen versuchte der TLfDI in zahlreichen Schulungen und Informationsveranstaltungen entgegenzuwirken. Das Jahr 2018 war von einem erheblichen Anstieg der Posteingänge von 12.158 im Jahr 2017 auf 22.188 geprägt.
Aufgrund der erforderlichen Anpassung des Thüringer Landesrechts an die DS-GVO arbeitete die Thüringer Landesregierung von Juni 2017 bis Januar 2018 an dem Gesetzentwurf eines neuen Thüringer Datenschutzgesetzes. Der TLfDI war vom Ergebnis enttäuscht. Insbesondere auch deshalb, weil im parlamentarischen Beratungsverfahren längst nicht alle Verbesserungsvorschläge des TLfDI berücksichtigt wurden. Für nicht EU-rechtskonform sah es der TLfDI an, dass bei einem datenschutzrechtlichen Verstoß der TLfDI sowohl den Verantwortlichen als auch die zuständige oberste Landesbehörde und die Aufsichtsbehörde darüber zu unterrichten hat. Eine Verständigung mit den beiden letztgenannten Behörden ist aber in der DS-GVO gar nicht vorgesehen. Zusätzlich wird dem TLfDI keine effektive Befugnis gegenüber öffentlichen Stellen eingeräumt, zur vorübergehenden Beschränkung der Verarbeitung personenbezogener Daten Zwangsmittel gemäß der ThürVwZVG, insbesondere eine Ersatzvornahme, anzuwenden. Kritisiert wurde vom TLfDI, dass dieser bei Datenschutzverstößen, die unter den Anwendungsbereich der JI-Richtlinie fallen, lediglich ein Beanstandungsrecht und keine Befugnis erhält,

Anordnungen oder Verbote zu erlassen. Schließlich schlug der TLfDI eine Ergänzung des Thüringer Sicherheitsüberprüfungsgesetzes vor, wonach die Person des TLfDI sich zur Ausübung ihres Amtes keiner Sicherheitsüberprüfung unterziehen sollte, weil die Person des TLfDI in Anwendung von Art. 51 Abs. 1 DS-GVO in der Ausübung ihres Amtes unabhängig und nur dem Gesetz unterworfen sei. Da der Innen- und Kommunalausschuss des Thüringer Landtags und letztlich die Thüringer Landtagsabgeordneten den Vorschlägen des TLfDI nur bedingt gefolgt waren, ist das neue Thüringer Datenschutzgesetz aus der Sicht des TLfDI daher immer noch verbesserungsbedürftig.
Auch 2019 erreichte die Zahl der Posteingänge mit 20.344 fast das Niveau des Vorjahres, die Anzahl der Meldungen von Datenpannen sowie der Eingang von Beschwerden hatte gegenüber dem letzten Berichtsjahr noch zugenommen.
Das Thema Künstliche Intelligenz wurde von den Datenschutzbeauftragten bereits seit Jahren beobachtet. 2019 hatten sich die Datenschutzaufsichtsbehörden in der „Hambacher Erklärung“ erstmals grundlegend zum Thema Künstliche Intelligenz – KI positioniert. Danach dürfen KI-Systeme nur zu verfassungsrechtlich legitimierten Zwecken eingesetzt werden, müssen transparent, nachvollziehbar und erklärbar sein, müssen Diskriminierung vermeiden, müssen den Grundsatz der Datenminimierung erfüllen, brauchen einen Verantwortlichen, damit die Grundsätze von Art. 5 DS-GVO eingehalten werden und den Hinweispflichten nach Art. 13 DS-GVO nachgekommen werden kann und die Sicherheit der Verarbeitung gemäß Art. 32 DS-GVO eingehalten wird und im Regelfall eine Datenschutz-Folgenabschätzung erfolgt und damit technische und organisatorische Standards eingehalten werden können.
Im darauffolgenden Jahr 2020 übertrafen die Posteingänge mit 22.193 sogar das Jahr 2018. Hierbei waren auch eine weitere Steigerung der Beschwerden als auch der Datenschutzpannenmeldungen zu verzeichnen.
Der Europäische Gerichtshof erklärte in seinem „Schrems II“-Urteil vom 16. Juli 2020 (Rechtssache C-311/18) auch das EU-US Privacy Shield für ungültig, weil der entsprechende Angemessenheitsbeschluss der EU-Kommission kein mit der EU vergleichbares Datenschutzniveau gewährleistet. Der Zugriff auf die personenbezogenen Daten von Nicht-US-Amerikanern wurde nicht beschränkt und die Betroffenen hatten keine durchsetzbaren Rechte gegen etwaige Zu-

griffe. Diese Entscheidung hatte für Verantwortliche in Europa erhebliche Auswirkungen, da diese nunmehr prüfen mussten, ob auf der Grundlage von Standardvertragsklauseln mit etwaigen zusätzlichen Maßnahmen personenbezogene Daten an US-amerikanische Unternehmen übermittelt werden durften. Eine für den Verantwortlichen kaum erfüllbare Aufgabe.
Die seit dem Jahr 2020 flächendeckend grassierende Corona-Pandemie war das große Thema, das den TLfDI in seiner täglichen Arbeit intensiv beschäftigte. Mit dem ersten Lockdown und steigenden Infektionszahlen wurde der TLfDI mit zahlreichen datenschutzrechtlichen Problemen konfrontiert. Dabei ging es schwerpunktmäßig um die Verarbeitung personenbezogener Daten von mit dem Coronavirus infizierten Personen und um Personen in deren Umfeld. Im Polizeibereich hatten die Polizeivollzugbeamten ein massives Interesse an der Information, ob bei Einsätzen in Wohnungen Krankheitsverdächtige oder infizierte Personen angetroffen werden. Der TLfDI kam zur Rechtsauffassung, dass den Einsatzbeamten solche Informationen aus den Gesundheitsämtern im Einzelfall übermittelt werden durften, da dies zur Abwehr erheblicher Nachteile für das Gemeinwohl erforderlich war. Es diente darüber hinaus der Vermeidung von ungehinderter und schneller Weiterverbreitung des Coronavirus in der Bevölkerung. Zusätzlich diente die Übermittlung dieser personenbezogenen Daten an die Polizei dazu, dass die Gesundheit der Polizistinnen und Polizisten, die über den Begriff der subjektiven Rechtsgüter unter den Schutzbereich der öffentlichen Sicherheit fällt, geschützt wird. Im nicht-öffentlichen Bereich ergaben sich Schwierigkeiten aus der Pflicht zur Kontaktdatenerfassung in Restaurants, bei Friseuren, Kosmetikern und so weiter. Der TLfDI musste hier viele Fragen zum Inhalt und zur Aufbewahrungsdauer der Kontaktdaten klären. Häufig wurden fortlaufende Listen zum Ausfüllen ausgelegt, in denen die betroffenen Personen ihre Kontaktdaten jeweils untereinander angeben sollten; in vielen Fällen wurden mehr Daten erhoben, als dies gesetzlich gefordert war. Aufgrund der Häufigkeit dieses unzulässigen Umgangs mit den „Corona-Listen“ wies der TLfDI in solchen Fällen wie auch in mehreren Pressemitteilungen darauf hin, dass die Kontaktdaten datenschutzkonform zu erheben seien. Einige Unternehmen verlangten vor dem Betreten ihres Geschäfts, dass alle Besucher sich einem Fiebermessen unterziehen mussten. Der TLfDI ging in diesem Fall davon aus, dass dies in der Regel mangels Eignung und Erforder-

lichkeit der Messung unzulässig war. Denn eine erhöhte Körpertemperatur konnte nicht zwangsläufig als symptomatisch für eine SARS-CoV-2-Infektion angesehen werden. Schließlich rückte ein weiteres Thema im Zuge der Corona-Pandemie in den Blickpunkt, nämlich die Einführung beziehungsweise Gewährung von Telearbeit und weitere Möglichkeiten der mobilen Arbeitsgestaltung insbesondere in der öffentlichen Verwaltung. Der TLfDI erarbeitete Hinweise, welche datenschutzrechtlichen Anforderungen an das Arbeiten im häuslichen Bereich gestellt werden müssen. Klare gesetzliche Regelungen in diesem Bereich gibt es leider nicht. Aus datenschutzrechtlicher Sicht gilt: Je höher die Sensibilität der Daten ist, desto höher ist auch ihr Schutzbedarf und folglich sind es auch die zu ergreifenden Schutzmaßnahmen in technischer und organisatorischer Hinsicht. Zu berücksichtigen ist, dass der Dienstherr auch bei einer genehmigten Telearbeit oder mobilem Arbeiten grundsätzlich die datenschutzrechtliche Verantwortung für die dienstlich veranlasste Verarbeitung trägt. Alle Datenschutzgrundsätze, insbesondere die vom Dienstherrn und Beschäftigten zu beachtenden Schutzmaßnahmen sowie Kontrollrechte und -pflichten, sollten deshalb in einer Dienstvereinbarung festgeschrieben werden. Bei besonders schützenswerten Daten, wie Gesundheits-, Beschäftigten- oder Sozialdaten, kann der Dienstherr nach Prüfung der erforderlichen Schutzvorkehrungen im Einzelfall auch zum Ergebnis gelangen, dass eine solche Verarbeitung besonders sensibler Daten in Telearbeit beziehungsweise bei mobilen Arbeiten untersagt wird. Dies trifft erst recht zu, wenn der Verantwortliche nicht die erforderlichen technischen (zum Beispiel Zwei-Faktor-Authentifizierung, gesicherter VPN-Zugang, Verschlüsselungstechniken, Anbindung an Remote-Desktop-Lösungen) und organisatorischen Maßnahmen (zum Beispiel Vorhandensein eines separaten Arbeitszimmers im häuslichen Bereich, verschließbare Aufbewahrungsmöglichkeit der Zugangsmittel und lokal gespeicherten Daten) herstellen kann, dies bedeutet das „Aus“ einer Verarbeitung solcher Daten außerhalb der Dienststelle. Die Entscheidung darüber, ob und welche Daten auch außerhalb der Dienststelle wie verarbeitet werden dürfen trifft letztlich der Dienstherr. Mit dem Inkrafttreten der Corona-Arbeitsschutzverordnung wurden die Arbeitgeber dann verpflichtet, ihren Beschäftigten Homeoffice-Möglichkeiten anzubieten, es sei denn, zwingende betriebliche Gründe sprachen dagegen.

Im Jahre 2021 gab es 21.226 Posteingänge beim TLfDI. Davon waren 4.670 Beschwerdeverfahren, was gegenüber dem Vorjahr eine Steigerung von über 50 % bedeutete. Ebenfalls wurden 115 Bußgeldverfahren neu eröffnet und 72 Bußgeldbescheide erlassen, also über 70 % mehr gegenüber dem Vorjahr.
Im Berichtsjahr 2022 war die Corona-Pandemie nicht mehr das alles beherrschende Thema. Vielmehr gewannen wieder andere datenschutzrechtliche Fragen mehr Raum. Es gab im laufenden Jahr 20.592 Posteingänge beim TLfDI. Die Zahl ist damit auf einem annähernd gleich hohen Niveau geblieben.
Microsoft 365 stand als Thema erneut im Mittelpunkt, insbesondere im Schulbereich. Weiterhin legte der EuGH eine Entscheidung zur Vorratsdatenspeicherung vor (Urteil vom 20. September 2022 – C 793/19). Danach waren die deutschen Regelungen zur Vorratsdatenspeicherung nicht mit EU-Recht vereinbar. Dieses stand einer allgemeinen und unterschiedslosen Vorratsdatenspeicherung von Verkehrs- und Standortdaten entgegen. Allerdings räumte der EuGH Spielraum für eine nationale Neuregelung ein. Danach sind Vorratsspeicherungen unter bestimmten, eng begrenzten Bedingungen zulässig, etwa zum Schutz der nationalen Sicherheit, zur Bekämpfung schwerer Kriminalität, zur Verhütung schwerer Bedrohungen. Der TLfDI fasste das Urteil dahingehend zusammen, dass der EuGH als Vorgabe machte, dass eine Vorratsdatenspeicherung entweder flächendeckend, aber nicht anlasslos, oder anlasslos, dann aber nicht flächendeckend sein dürfe. Trotzdem sah der TLfDI in diesem Bereich weiter die Gefahr, dass die Verlockung, die technischen Möglichkeiten zu einer nahezu unbegrenzten Überwachung auch tatsächlich zu nutzen, früher oder später zu weiteren und neuen Vorstößen einer Vorratsspeicherung führen dürfte.
Unter den zahlreichen datenschutzrechtlichen Themen die zu bearbeiten waren, stand der Schul- und Bildungsbereich seit Beginn seiner Amtszeit im März 2012 im Fokus seiner Arbeit. Bereits zuvor war der TLfDI von 2006 bis Anfang 2011 als Referatsleiter beim TLfDI unter anderem für den Bereich Schule und Bildung tätig. Schon zu dieser Zeit entwarf er zum 2. Europäischen Datenschutztag am 28. Januar 2007 eine Broschüre „Kinder-Jugend-Datenschutz“, die eine Materialsammlung zum Datenschutz in der Schule enthielt und viele datenschutzrechtliche Problemfelder aufzeigte, die bis heute nichts an Aktualität verloren haben. Schon in seinem ersten unter eigener Leitung erstellten Tätigkeitsbericht 2012/2013 griff Herr Dr. Hasse die

Problematik der Nutzung von sozialen Netzwerken zu schulischen Zwecken auf und verwies darauf, dass mit den meisten sozialen Netzwerken ein vertraulicher Austausch personenbezogener Daten von Schülern und Lehrern nicht gewährleistet werden kann und damit ein datenschutzrechtlicher Verstoß vorliegt. Zwölf Jahre später muss der TLfDI noch immer Schulen wegen der Nutzung von zum Beispiel WhatsApp zur dienstlichen beziehungsweise schulischen Kommunikation verwarnen. Gleiches gilt auch für die behördlichen Datenschutzbeauftragten (bDSB) der Schulen. Hier mahnte der TLfDI gegenüber dem für Thüringen zuständigen Bildungsministerium an, dass nur ein bDSB in jedem Staatlichen Schulamt, der für alle Schulen im jeweiligen Zuständigkeitsbereich zuständig ist, mit der Aufgabe überfordert ist. Zwölf Jahre später hat sich die Situation nicht nur nicht gebessert, durch die Reduzierung der Staatlichen Schulämter auf fünf sind die bDSB für noch mehr Schulen zuständig als je zuvor. Da dem TLfDI sowohl die Lösung konkreter schulischer Datenschutzprobleme als auch die Vermittlung von Medienkompetenz in Schulen und Hochschulen ein besonderes Anliegen ist, übernahm er eine Arbeitsgruppe Datenschutz und Schule, die vom Arbeitskreis (AK) Datenschutz und Bildung der Datenschutzkonferenz, dem Gremium der unabhängigen deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder gegründet wurde. Wenig später übernahm Herr Dr. Hasse auch den Vorsitz des AK „Datenschutz und Bildung“ vom Datenschutzbeauftragten Rheinland-Pfalz. Zur ersten Sitzung des AK „Datenschutz und Bildung“ hatte Herr Dr. Hasse zum Thema „Medienbildung in der Schule“ mehrere Fachleute eingeladen. In einem Gastvortrag wurde die Erarbeitung einer Strategie der Kultusministerkonferenz zur „Bildung in einer digitalen Welt“ vorgestellt. Darin wurden Vorschläge zur Ergänzung von Lehrplänen erarbeitet, um in der Schule den Schülern mehr Medienkompetenz zu vermitteln. Hierfür soll es eine bundesweite Verständigung über die Anforderungen an die Qualifizierung von Erziehenden und Lehrenden geben. Der TLfDI wurde als Vorsitzender des AK Datenschutz und Bildung nach Abschluss des Koordinierungsprozesses innerhalb des Generalsekretariats der Kultusministerkonferenz (KMK) in die weitere Planung einbezogen. Dies führte zu einer stärkeren Einflussnahme des Datenschutzes auf die Medienbildung in den Schulen. Herr Dr. Hasse setzt sich seitdem dafür ein, dass eine solide Medienbildung auch in den Lehramtsstudiengängen der Hochschulen Eingang findet und musste frühzeitig feststellen, dass hier dicke Bretter gebohrt werden müssen. Der

TLfDI konnte seine Kontakte zur KMK nutzen, um den Schutz der Privatsphäre beziehungsweise den Datenschutz auch in der Lehrerausbildung zu verankern. Das neue Strategiepapier der KMK sieht nunmehr verpflichtende Studieninhalte für angehende Lehrer vor. Der TLfDI erkannte auch früh den Trend in der Schule, Lernstoff digital zu vermitteln. Als eine Reaktion darauf entstand unter Vorsitz von Herrn Dr. Hasse eine Orientierungshilfe der Datenschutzaufsichtsbehörden für Online-Lernplattformen im Schulunterricht. Als weiteres großes Thema rückte vor acht Jahren die Frage nach der Zulässigkeit des schulischen Einsatzes von Microsoft Office 365 (heute: Microsoft 365) in den Mittelpunkt. Sowohl 2021 als auch 2022 stand Microsoft 365 bei der vom TLfDI und der Kultusministerkonferenz gegründeten „Arbeitsgruppe Datenschutz“ auf der Tagesordnung. Als Unterstützungsleistung für ein geplantes Gespräch der KMK mit hochrangigen Vertretern der Fa. Microsoft erarbeitete der TLfDI gemeinsam mit den Mitgliedern seiner beiden Arbeitskreise Schulen und Bildungseinrichtungen sowie Datenschutz-/Medienkompetenz einen Fragenkatalog zu datenschutzrechtlichen Unklarheiten und fehlenden Erläuterungen in den von Microsoft veröffentlichten Unterlagen zu Microsoft 365. Der TLfDI war über den Auftritt von Microsoft bei der KMK in Berlin ebenso enttäuscht wie die KMK. Nach Einschätzung des TLfDI brachte das Gespräch mit Microsoft keine greifbaren Lösungen und auf die vorgetragenen datenschutzrechtlichen Probleme wurde nicht eingegangen. Eine weitere von der Datenschutzkonferenz eingesetzte Arbeitsgruppe „Microsoft Onlinedienste“ hatte sich seit Ende 2020 mit der Microsoft 365 Problematik beschäftigt und dabei 14 Videokonferenzen mit Microsoft durchgeführt. Der unter Berücksichtigung der Gesprächsergebnisse und des von Microsoft bereitgestellten „Datenschutznachtrags vom 15. September 2022“ erstellte Bericht zur datenschutzrechtlichen Beurteilung von Microsoft 365 führte dann zu einer im Wesentlichen vom TLfDI vorbereiteten Festlegung der Datenschutzkonferenz. Darin stellt die Datenschutzkonferenz fest, „dass der Nachweis von Verantwortlichen, Microsoft 365 datenschutzrechtskonform zu betreiben, auf der Grundlage des von Microsoft bereitgestellten „Datenschutznachtrags vom 15. September 2022“ nicht geführt werden kann. Solange insbesondere die notwendige Transparenz über die Verarbeitung personenbezogener Daten aus der Auftragsverarbeitung für Microsofts eigene Zwecke nicht hergestellt und deren Rechtmäßigkeit nicht belegt wird, kann dieser Nachweis nicht erbracht werden.“ Der TLfDI hatte diese Bewertung

allen Thüringer Schulen zur Kenntnis gegeben und darauf hingewiesen, dass bei einer Nutzung von Microsoft 365 für unterrichtliche oder für dienstliche Zwecke die Schulen entgegen der Pflicht nach Art. 5 Abs. 2 DS-GVO nicht die Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten nach Art. 5 Abs. 1 DS-GVO nachweisen und damit nicht ihrer Rechenschaftspflicht nachkommen können. Trotzdem ist davon auszugehen, dass Microsoft 365 in mehreren Schulen trotz des Verbots durch das Ministerium für Bildung, Jugend und Sport (dort zu finden in den FAQs, Pkt. 7.5) noch immer zum Einsatz kommt (https://bildung.thueringen.de/schule/medien/datenschutz-in-schulen).

Bereits Ende 2017 hatte sich der TLfDI an Herrn Minister Holter gewandt und ihm die Durchführung von Fortbildungsveranstaltungen für Schulleitungen zum Inhalt der DS-GVO und deren Bedeutung für die Schulen vorgeschlagen. Nachdem die Initiative des TLfDI zunächst vom Ministerium nicht aufgegriffen wurde, konnten aufgrund der Beharrlichkeit des TLfDI dann doch einige größere „Live"-Veranstaltungen mit Schulleiterinnen und Schulleitern durchgeführt werden. Die Veranstaltungen bestanden aus einem Vortragsteil zum Datenschutz in der Schule unter Geltung der DS-GVO und aus der Möglichkeit für die Schulleitungen, Fragen an den TLfDI zu richten. Die Beantwortung von allen offenen Fragen wurde anschließend auf der Internetseite des TLfDI veröffentlicht.

Die Evaluationsergebnisse des Kurses „Medienkunde" von Herrn Prof. Dr. Wollinger (https://www.db-thueringen.de/receive/dbt_mods_00034913) bestätigten die von Herrn Dr. Hasse zuvor geäußerten Befürchtungen hinsichtlich des untergeordneten Stellenwerts der Vermittlung von Medienkompetenz in der Schule. Der TLfDI hatte zuvor aufgedeckt, dass viele Medienpässe, die von den Schulen ausgestellt waren, sich als Fakes herausstellten. Herr Prof. Wollinger empfiehlt neben einem integrativen Ansatz auch die Einführung eines neuen Unterrichtsfachs „Medienkunde". Außerdem wird in dem Bericht auf die Notwendigkeit hingewiesen, die Lehrkräfte in medienkompetenzbezogenen Aus- und Fortbildungen zu schulen und die Digitalisierung in den Schulen in den Blick zu nehmen. Mit Überlegungen zu einer „Digitalstrategie Thüringer Schulen (DiTS)" hatte das Thüringer Bildungsministerium die Einführung eines Unterrichtsfachs Medienkunde/Informatik angekündigt.

Durch die Umwandlung der AG Datenschutz und Schule zunächst in einen Unterarbeitskreis und dann in einen eigenen Arbeitskreis Schulen und Bildungseinrichtungen sowie die Umbenennung des AK Datenschutz und Bildung in den AK Datenschutz-/Medienkompetenz wurde der TLfDI Vorsitzender von zwei Arbeitskreisen der Datenschutzkonferenz. Als Vorsitzender der beiden Arbeitskreise entschied sich der TLfDI, exemplarisch für die wachsende Anzahl von Online-Lernplattformen, die Entwicklung der HPI-Schulcloud des Hasso-Plattner-Instituts, einem vom Bundesministerium für Bildung und Forschung geförderten Pilotprojekt, aus datenschutzrechtlicher Sicht zu begleiten. Damit initiierte der TLfDI erstmals eine auf längere Zeit ausgerichtete Kooperation zwischen einer Datenschutzaufsichtsbehörde und einem Software-Hersteller. Herr Dr. Hasse verwies bereits bei seiner ersten Einladung zu einer HPI-Schulcloud-Sitzung darauf, dass der Datenschutz zu beachten ist und rote Linien zu definieren sind, die unbedingt eingehalten werden müssen. Der TLfDI forderte zum Beispiel pseudonymisierte Benutzer-Logins auf der Online-Lernplattform, damit die Bildungsmedienanbieter nicht die Klarnamen und E-Mail-Adressen der die Plattform nutzenden Schülerinnen und Schüler erfahren. Viele Probleme, die der TLfDI angesprochen hatte, konnten gelöst werden. Teilweise fehlen aber auch schulische Rechtsvorschriften, die zum Beispiel regeln, ob Schulclouds und andere digitale Anwendungen nur mit Einwilligung der Eltern genutzt werden dürfen, ob die Verwendung von privaten Endgeräten (BYOD – Bring Your Own Device) von der Schule einfach vorausgesetzt werden kann und welche Datensicherheitsaspekte bei der Nutzung zu beachten sind.
Da die Verantwortung für den Inhalt der Lehrerausbildung bei den Hochschulen liegt, wandte sich der TLfDI seit 2019 mehrmals mit Fragen und Vorschlägen zur Einführung von Qualifizierungsmaßnahmen für Lehramtsstudierende im Bereich des Datenschutzes und der Medienbildung sowohl an das für die Hochschulen zuständige Ministerium als auch an die Hochschulen. Dabei erinnerte der TLfDI an die Beschlüsse der KMK vom 16. Mai 2019, die die Ausbildungsstandards für die Lehrerausbildung an Hochschulen neu fassen und damit wichtige Weichenstellungen auch für die Entwicklung medienpädagogischer Kompetenz von angehenden Lehrerinnen und Lehrer gaben. An den vorausgehenden Prozess war auch der Arbeitskreis Datenschutz-/Medienkompetenz unter dem Vorsitz des TLfDI beteiligt. Der TLfDI bat deshalb um Auskunft, wie die Umsetzung der neuen Stan-

dards in Thüringen vorangeht und welche Maßnahmen zur Unterstützung des Prozesses getroffen würden. Aus den Antwortschreiben ergab sich, dass Lehrinhalte zum Datenschutz und zur Medienkunde für die Studierenden nicht verpflichtend waren, sondern vorrangig im Wahlpflichtbereich oder als Zusatzangebot vermittelt wurden. Begründet wurde dies damit, dass eine Aufnahme in das Pflichtcurriculum den Wegfall anderer wichtiger Inhalte bedeuten würde. Trotz der teilweise ausführlichen Antworten der Hochschulen gewann der TLfDI den Eindruck, dass die Hochschulen einer Datenschutzaufsichtsbehörde die Zuständigkeit absprachen, Fragen zur hochschulinternen Medienbildung zu stellen. Seit 2022 wird der TLfDI selbst tätig und bietet eine Vorlesung zum Thema Datenschutz an der Universität Jena an. Er steht im Gespräch mit der Unileitung, dass beim Bestehen der am Ende stehenden Prüfungsklausur sowohl für Juristen als auch insbesondere für Lehramtsstudierende „Creditpoints“ vergeben werden, die sich die Teilnehmer anrechnen lassen können.
Die im Jahre 2020 einsetzende Corona-Pandemie führte im Schulbereich aufgrund des häufigen Ausfalls von Unterricht in der Schule zu einer massiven Belastung hinsichtlich der Vermittlung des Unterrichtsstoffes. Die bereits aus der HPI-Schulcloud entwickelte Thüringer Schulcloud wurde flächendeckend in vielen Thüringer Schulen eingeführt. Es war ein glücklicher Zufall, dass der TLfDI diejenige Online-Lernplattform datenschutzrechtlich begleitete, die nun zur Unterrichtsbewältigung auf Distanz eingesetzt werden konnte und ein Ausweichen auf rechtswidrige Software nicht erforderlich machte. Bis Ende 2020 wurde die Thüringer Schulcloud an 838 Thüringer Schulen und anderen Bildungseinrichtungen eingesetzt. Bei allen Unzulänglichkeiten, die sich bei Beginn im Realbetrieb der Thüringer Schulcloud zeigten, ist sie doch als Erfolgsmodell zu bezeichnen. Als Alternative zum Schulunterricht vor Ort waren während der Corona-Pandemie digitale Treffen über Videokonferenzsysteme das Mittel der Wahl. Der TLfDI legte dem Thüringer Ministerium für Bildung, Jugend und Sport dar, dass der Einsatz eines Videokonferenzsystems zulässig ist, wenn entweder eine Rechtsgrundlage im Schulrecht vorliegt, die die Verarbeitung beim Einsatz eines Videokonferenzsystems erlaubt oder dazu verpflichtet oder aber zuvor von der Schule eine Einwilligung bei den Eltern beziehungsweise volljährigen Schülerinnen und Schülern eingeholt wird. Da keine schulische Rechtsgrundlage den Einsatz von Videokonferenzsystemen erlaubt, blieb den Schulen nur die Einholung der oben genannten Einwilligung. Da die

Schule Verantwortlicher im Sinne von Art. 4 Nr. 7 DS-GVO ist und von der Schulleitung vertreten wird, durfte keine Lehrkraft eigenmächtig ein Videokonferenzsystem einführen, sondern musste dieses zuvor der Schulleitung zur Genehmigung vorlegen. Dabei musste die Schulleitung durch das Ergreifen geeigneter technischer und organisatorischer Maßnahmen sicherstellen, dass die Verarbeitung der personenbezogenen Daten datenschutzkonform erfolgt. Das Fehlen dieser Voraussetzung durfte keinesfalls im Wege der Einwilligung ersetzt werden. Die Einwilligung ersetzt lediglich die sonst fehlende Rechtsgrundlage, kann aber nicht andere Verstöße gegen die DS-GVO legalisieren. Da wie bereits beschrieben 2020 das EU-US Privacy Shield vom EuGH für ungültig erklärt wurde, war die Nutzung von Videokonferenzsystemen der großen und bekannten US-amerikanischen Anbieter als äußerst kritisch anzusehen. Empfohlen werden konnten eher Open-Source-Lösungen, die aber zuvor ebenfalls von der Schulleitung geprüft werden mussten. Eine dieser Lösung steht als Tool bei der Nutzung der Thüringer Schulcloud zur Verfügung. Die Problematik der Nutzung geeigneter Videokonferenzsysteme stellte sich genauso im Hochschulbereich. Aufgrund der hohen Teilnehmerzahlen von Studierenden nutzten die Hochschulen auch einschlägig bekannte US-amerikanische Produkte, die zwar sehr leistungsfähig, aber keinesfalls datenschutzkonform waren. Der TLfDI musste die Hochschulen auf die Unzulässigkeit der Nutzung solcher Systeme hinweisen. Weiterhin wurde das Ablegen von Prüfungen in der Coronazeit zu einem Problem, wenn die zu Prüfenden nicht vor Ort waren, eine Verzögerung der Studierdauer verhindert werden, aber trotzdem eine für alle Prüflinge vergleichbare, chancengerechte Prüfungsleistung erfolgen sollte. Hierzu begleitete der TLfDI eine Hochschule bei der Einführung eines Prüfungsverfahrens, bei dem zwar einige Unzulänglichkeiten festgestellt wurden, letztlich aber keine durchgreifenden datenschutzrechtlichen Bedenken bestanden. Voraussetzung für die Durchführung von Online-Prüfungen ist das Vorliegen einer Rechtsgrundlage, die dies grundsätzlich erlaubt. In Thüringen gab es diese gesetzliche Befugnis seit Mitte 2020. Die konkrete technische Ausgestaltung eines Online-Prüfungsverfahrens musste hingegen auf der Grundlage der Anforderungen des Art. 32 DS-GVO sichergestellt werden.

Auf Initiative des TLfDI wird seit 2021 eine vom Thüringer Institut für Lehrerfortbildung, Lehrplanentwicklung und Medien organisierte „Videokonferenzreihe zum Thema Datenschutz für pädagogische

Führungskräfte“ durchgeführt. Mehrmals jährlich werden interessierte Schulleitungen zu dieser Videokonferenz eingeladen. Die Schulleitungen erhalten dann nach einer schuldatenschutzrechtlichen Einführung die Gelegenheit, datenschutzrechtliche Fragen zu stellen, die entweder direkt beantwortet werden oder aber die Beantwortung erfolgt später schriftlich. Solange Schulleitungen ihren Bedarf anmelden, wird die Veranstaltung fortgeführt werden.
Hoch erfreut konnte der TLfDI feststellen, dass Schulen sich neben dem Funktionalen auch vermehrt darüber Gedanken machten, ob ein bestimmtes Digitaltool auch datenschutzrechtliche Anforderungen erfüllt. Nicht zuletzt die hohe Zahl der Anfragen von Lehrkräften und Schulleitungen, aber auch der Schulaufsichtsbehörden waren sichtbarer Beleg hierfür. Neben den Antworten auf Einzelfragen entstanden beim TLfDI im ersten Halbjahr 2021 insgesamt sieben für die Thüringer Schulen bestimmte Rundschreiben, um mit der notwendigen Reichweite über Schulsoftware aufzuklären. Dabei musste manche Euphorie von Schulen über das eine oder andere Schultool gedämpft werden. Durch Wegfall des „Privacy Shield“ sah der TLfDI bei Tools, die die Datenübermittlung in die USA vorsehen, die dafür notwendigen Garantien für die Einhaltung des europäischen Datenschutzniveaus nicht gewährleistet. Die Durchsetzung der Betroffenenrechte von Schülern, Eltern und Lehrern vor US-amerikanischen Gerichten hielt der TLfDI unter diesen Bedingungen für nicht möglich. Auch der Einsatz von nicht abschaltbaren Trackingmechanismen auf vielen Websites oder die Nutzung von Werbeplattformen machten die Nutzung von Online-Plattformen für den Schulunterricht unmöglich, waren aber besonders bei kostenlosen Angeboten weit verbreitet. Der TLfDI konnte aber bei vielen Angeboten für den schulischen Einsatz nicht selten auch seine datenschutzrechtliche Zustimmung erteilen.
Eine weitere Aufregung während der Pandemie waren Fragen im Zusammenhang mit der Pflicht zum Tragen der Mund-Nasen-Bedeckung und der Form der Nachweisführung zur „Masken-Befreiung“, sodass den TLfDI hierzu regelmäßig Beschwerden erreichten. Es beschwerten sich Eltern über Schulen, die die vorgelegten Atteste zur Befreiung von der Verpflichtung zum Tragen einer medizinischen Mund-Nasen-Bedeckung nicht anerkannten, weil sie entweder keine Diagnose enthielten oder vermutet wurde, dass es sich um ein sogenanntes Gefälligkeitsattest handelte. Außerdem würden Schulen die Atteste zur Prüfung an die zuständigen Schulämter weiterleiten und damit Gesundheitsdaten Dritten zugänglich machen. Besonders problematisch bei

diesen Fällen war der Umstand, dass für die Kinder, sofern sie keine Maske trugen und der Befreiungsgrund –noch – nicht als glaubhaft anerkannt war, trotz Schulpflicht ein Betretungsverbot für die Schule galt. Nach der damals in Thüringen geltenden Verordnung galt die Verpflichtung zur Verwendung einer qualifizierten Gesichtsmaske dann nicht, wenn die Verwendung wegen Behinderung oder aus gesundheitlichen oder anderen Gründen nicht möglich oder unzumutbar war. Dies musste in geeigneter Weise glaubhaft gemacht werden. Nach Auffassung des TLfDI war sicherzustellen, dass ein sogenanntes Gefälligkeitsgutachten ausgeschlossen werden konnte. Dies konnte zum Beispiel dann der Fall sein, wenn Ärzte solche Atteste zugunsten von Personen ausstellten, die in erheblicher Entfernung wohnen und über ihren angestammten Patientenkreis hinausgingen. Der TLfDI sah in dem Verhalten eines Schulleiters, der sich mit einem solchen zweifelhaften Attest an das zuständige staatliche Schulamt wandte und um weitere Prüfung bat, keine unzulässige Übermittlung von Gesundheitsdaten durch die Schule.

Auch das Jahr 2021 bot der Behörde keine Zeit zum Durchatmen, da die Corona-Pandemie weiterhin die Arbeit beim TLfDI bestimmte. Den Verantwortlichen waren oft die notwendigen technischen und organisatorischen Maßnahmen zur Durchführung von Online-Formaten unklar. In den Thüringer Schulen wuchs die Verunsicherung darüber, welche Softwareprodukte im Unterricht datenschutzkonform zum Einsatz kommen durften. Obwohl dies vorrangig Aufgabe des Dienstherrn gewesen wäre, bot sich der TLfDI als erster Ansprechpartner an und beriet die Schulleiter in Form von mehreren Rundschreiben und den bereits genannten Videokonferenzen für Schulleitungen. Ziel des TLfDI war es, auch in der Pandemie Datenverarbeitungen in der Schule rechtskonform zu gestalten.

Der TLfDI hatte in den vergangenen Jahren immer wieder Videofilme für Kinder und Jugendliche erstellt, um auf unterhaltsame Weise datenschutzrechtliche Sachverhalte darzustellen. Zuletzt erfolgte dies in einem gemeinsamen Projekt mit dem Berufsverband der Datenschutzbeauftragten e. V. (BvD), bei dem drei Videofilme gedreht wurden, an denen der TLfDI mitwirkte. Aktuell wird mit dem BvD erneut das Drehen von weiteren Videofilmen vorbereitet.

Seit 2021 begleitet der TLfDI mit seinem AK Schulen und Bildungseinrichtungen auf Bitte des Medieninstituts der 16 Länder – FWU das Projekt „VIDIS-Vermittlungsdienst für das digitale Identitätsmanagement in Schulen“ aus datenschutzrechtlicher Sicht. Die Kernaufgabe

von VIDIS ist die Schaffung einer einheitlichen Anbindung aller teilnehmenden Schulportale der Länder an die Online-Produkte der Bildungsmedienanbieter als „Single Sign-on“. Dies hat den Vorteil, dass die Schülerinnen und Schüler sich nur einmal mit einem Passwort anmelden müssen und dann Zugriff auf alle Online-Angebote erhalten, für die die Schule eine Freigabe erteilt hat. Darüber hinaus erfolgen die Zugriffe der Lernenden in pseudonymisierter Form, sodass der Bildungsmedienanbieter keine Klardaten zur Kenntnis erhält. Darüber hinaus hat VIDIS vorerst eine datenschutzrechtliche Vorprüfung von allen Online-Bildungsangeboten übernommen, die an VIDIS teilnehmen wollen. Der TLfDI hat gemeinsam mit dem AK Schulen und Bildungseinrichtungen zahlreiche Hinweise zum datenschutzkonformen Betrieb von VIDIS gegeben. Perspektivisch soll die Prüfung mit dem Verfahren eduCheck, ebenfalls vom FWU, durchgeführt werden. Auch hier ist abzusehen, dass eine datenschutzrechtliche Begleitung durch den TLfDI und Mitglieder des AK Schulen und Bildungseinrichtungen erfolgen wird. Die digitalen Bildungsangebote, die sich von eduCheck einer technischen und rechtlichen Prüfung unterziehen, können bei Erfüllung aller Kriterien ein eduCheck-Gütesiegel erhalten, welches die Schulleitungen bei der Auswahl von für den Unterricht geeigneten Tools unterstützt. Umgekehrt können auch die Bildungsmedienanbieter zum Beispiel Verlage feststellen, welche Mindestanforderungen diese zu erfüllen haben, um den Schulen ein datenschutzkonformes Produkt anbieten zu können. Letztlich behalten sich die Datenschutzaufsichtsbehörden aber im Einzelfall vor, die datenschutzrechtliche Zulässigkeit von Bildungsmedienangeboten, die im Unterricht zum Einsatz kommen sollen, zu beurteilen. Ein hierzu bereits bestehender Dialog mit den Verlagen gestaltet sich indes schwierig. Parallel zu eduCheck wird mit dem Forschungsprojekt „DIRECTIONS“ seit 2022 eine Datenschutzzertifizierung von Informationssystemen im Bildungssektor entwickelt. Ziel des Projekts liegt ebenfalls in der Entwicklung eines Zertifikats, welches Bildungsmedienanbieter nutzen können, um die Einhaltung der datenschutzrechtlichen Vorgaben nachzuweisen. Der TLfDI hat aufgrund seines großen Interesses daran, dass die Schulen ausschließlich digitale Bildungsmedien im Unterricht nutzen, die allen datenschutzrechtlichen Vorschriften genügen und so die Schülerinnen und Schüler schützen, auch dieses Verfahren von Anfang an begleitet und hat hier eine tragende Rolle übernommen. Ziel ist es, eine Zertifizierung zu entwickeln, die nahe an eine Zertifizierung nach Art. 42 DS-GVO heranreicht, denn diese

Norm erlaubt lediglich die Zertifizierung von konkreten Datenverarbeitungsvorgängen, nicht aber von Produkten.
Das waren im Schnelldurchlauf zwölf Jahre Datenschutz in Thüringen. Rasante tatsächliche und technische Entwicklungen, die mit den Produkten der Künstlichen Intelligenz vorläufig ihren Höhepunkt erreicht haben. Der TLfDI steht in direktem Kontakt mit der Anbieter-Firma OpenAI und wartet auf Beantwortung seiner vielen Fragen.
Solange der TLfDI etwa zu ChatGPT kein grünes Licht gegeben hat, sollten insbesondere Schulen mit der Verwendung von Kinder-Daten äußerst vorsichtig sein und zumindest einen Daten-Treuhänder zwischenschalten oder Offline-Produkte nutzen.
Auch dieses Beispiel zeigt, dass der Datenschutz in Thüringen ganz vorne mit dabei ist, um angesichts der immer intensiver werdenden Bedrohungen des Grundrechts der informationellen Selbstbestimmung dessen Schutz zu gewährleisten. Vielleicht findet die massiv zunehmende Bedeutung dieses Grundrechts irgendwann Ausdruck in einer ebenso massiven politisch-finanziellen-Unterstützung des TLfDI.
Meinem Nachfolger Tino Melzer wünsche ich eine glückliche Hand!

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

1. Themengebiete



© Cevahir - Datenaustausch - fotolia.com

1.1 Schwerpunkte im Berichtszeitraum einschließlich Statistik

Der Datenschutz muss auch in Thüringen immer europäischer gedacht werden. Es gab wichtige Entscheidungen des Europäischen Datenschutzausschusses und auch des Europäischen Gerichtshofes. Digitalisierung und KI gewinnen immer mehr an Bedeutung und datenschutzrechtliche Probleme tauchten in allen Lebensbereichen auf.

In der Datenschutzaufsicht gewinnt die Perspektive nach Europa immer größere Bedeutung. Die EU-Kommission hat am 10. Juli 2023 einen Angemessenheitsbeschluss für den Transfer personenbezogener Daten in die USA getroffen (sogenanntes Data Privacy Framework). Es galt, seine Reichweite für Übermittlungen an die USA zu beleuchten sowie den Umfang und die Durchsetzung von Rechten betroffener Personen gegenüber Stellen in den USA (siehe dazu Beitrag Nr. 1.2). Auch sonst gab es einige wichtige Entscheidungen des Europäischen Datenschutzausschusses (siehe Beitrag Nr. 1.20). Ende des Jahres traf der Europäische Gerichtshof richtungsweisende Entscheidungen (siehe Beitrag Nr. 1.19).

Das Potenzial von künstlicher Intelligenz (KI) begeistert viele und erhält Einzug in immer mehr Lebensbereiche und Big Data. Sie versprechen, unser Leben grundlegend zu verändern. Besonders die Entwicklung von KI-basierten Chatbots, allen voran ChatGPT, stellt Verantwortliche vor besonderen Herausforderungen, das System datenschutzkonform zu betreiben (siehe dazu Beitrag Nr. 1.3).
Die Digitalisierung der Gesellschaft ist in allen Lebensbereichen weiterhin auf dem Vormarsch und stellt die Aufsichtsbehörden vor die Herausforderung, diese Entwicklung datenschutzrechtlich zu begleiten (Beiträge Nr. 1.7, 1.8, 1.10, 1.11).
Auch in diesem Berichtsjahr war die Frage, ob Microsoft 365 datenschutzrechtskonform betrieben werden kann weiterhin Thema (vergleiche Beitrag Nr. 1.4).
Schwerpunkt der Tätigkeit des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) ist nach wie vor der Bereich Schulen und Bildung. Hier wurden innerhalb der beiden Arbeitskreise Schulen und Bildungseinrichtungen sowie Datenschutz-/Medienkompetenz wieder zahlreiche aktuelle Themen länderübergreifend diskutiert (vergleiche Beitrag Nr. 1.9).
Daneben gab es viele Einzelfälle aus unterschiedlichen Problemfeldern, von denen im Bericht einige exemplarisch dargestellt sind. Bei den Beschwerden nimmt die datenschutzrechtliche Prüfung von Videoüberwachung in verschiedensten Zusammenhängen einen gewissen Schwerpunkt ein.

Einige statistische Angaben:
Im Jahr 2023 gab es 21.334 Posteingänge beim TLfDI, womit eine Steigerung gegenüber dem Vorjahr zu verzeichnen ist.
Es wurden im Berichtsjahr 115 Bußgeldverfahren eröffnet, etwas mehr als im Vorjahr. Davon endeten bereits zehn Bußgeldverfahren mit einem Bußgeldbescheid. Insgesamt wurden im Jahr 2023 beim TLfDI 32 Bußgeldbescheide erlassen, wovon 24 bis zum Ende des Berichtszeitraumes Rechtskraft erlangten. Die Höhe der insgesamt festgesetzten Bußgelder lag etwa auf dem Vorjahresniveau und betrug 31.490 Euro. Der TLfDI erließ zwei Bußgeldbescheide nach Art. 83 Abs. 4 Datenschutz-Grundverordnung (DS-GVO). Weiterhin wurden 28 Bußgeldbescheide nach Art. 83 Abs. 5 DS-GVO erlassen. Der Trend der Vorjahre, wonach sich der überwiegende Teil der Bußgeldbescheide gegen die Betreiber unbefugter Videoüberwachung rich-

tete, setzte sich auch im aktuellen Berichtszeitraum fort. Gleichbleibend mit fünf Bußgeldbescheiden war auch die verhältnismäßig geringe Anzahl von Verstößen im Polizeibereich. Dagegen war eine Zunahme von Bußgeldbescheiden zu verzeichnen, in denen sonstige Beamte und Beschäftige des öffentlichen Dienstes unbefugt auf die ihnen zur Verfügung gestellten IT-Systeme zugegriffen hatten. Auch wurden vermehrt Fälle geahndet, in denen in unzulässiger Weise die Standortdaten von Personen mit Hilfe von GPS-Trackern überwacht worden waren.
Insgesamt gab es 300 Meldungen der Verletzung des Schutzes personenbezogener Daten nach Art. 33 DS-GVO. Dies stellt eine Steigerung im Vergleich zum Vorjahr um rund 6 % dar. Im Berichtszeitraum gingen 415 Beschwerden nach Art. 77 Abs. 1 DS-GVO ein, also Eingaben von Personen, die sich gegen eine sie betreffende Datenverarbeitung durch Thüringer Stellen wandten, 106 davon im öffentlichen Bereich und 309 im nicht-öffentlichen Bereich.
Im Berichtszeitraum wurden insgesamt 109 Maßnahmen nach Art. 58 Abs. 2 DS-GVO ergriffen. Hiervon betrafen 17 Maßnahmen den öffentlichen Bereich und 92 den nicht-öffentlichen Bereich. In zwei Fällen wurden die Verantwortlichen gewarnt, dass beabsichtigte Verarbeitungsvorgänge voraussichtlich gegen diese Verordnung verstoßen (Art. 58 Abs. 2 Buchstabe a) DS-GVO). 88 Verantwortliche wurden nach Art. 58 Abs. 2 Buchstabe b) DS-GVO verwarnt, da diese mit Verarbeitungsvorgängen gegen diese Verordnung verstoßen hatten. Sieben Verantwortliche wurden im Berichtszeitraum nach Buchstabe d) angewiesen, Verarbeitungsvorgänge auf eine bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit dieser Verordnung zu bringen. Eine vorrübergehende oder endgültige Beschränkung der Verarbeitung, einschließlich eines Verbots nach Buchstabe f), wurde gegenüber sechs Verantwortlichen verhängt. Bei sechs Verantwortlichen wurden Maßnahmen nach Buchstabe d) und f) in Kombination ergriffen.

1.2 EU-Angemessenheitsbeschluss zur Datenübermittlung in die USA vom Juli 2023 – Die „unendliche Geschichte“ wird fortgeschrieben …

Wie lange gilt der neue EU-US Datenschutzrahmen (EU-US Data Privacy Framework – EU-US DPF) den die EU-Kommission am 10. Juli 2023 mittels Angemessenheitsbeschluss als Grundlage für die

Datenübermittlung in die USA verabschiedet hat? Diese nicht nur für Datenschützerinnen und Datenschützer spannende und elementare Rechtsfrage wird am Ende wohl wieder vom Europäischen Gerichtshof (EuGH) entschieden werden müssen, wenn der Datenschutzaktivist Max Schrems oder ein anderer kritischer Verteidiger des Grundrechts auf informationelle Selbstbestimmung dieses Gericht angerufen hat und für Klarheit sorgen wird. Gründe hätte der EuGH genug, um auch das EU-US DPF für unwirksam zu erklären, wie der folgende Beitrag zeigt.

Rückblende in den Sommer 2020: In seinem Urteil vom 16. Juli 2020 (Rechtssache C-311/18 „Schrems II“) erklärte der Europäische Gerichtshof (EuGH) das damalige EU-US Privacy Shield-Abkommen für unwirksam, weil das durch die EuGH-Richter bewertete damalige US-Recht kein Datenschutzniveau bot, das dem in der Europäischen Union (EU) im Wesentlichen gleichwertig war (siehe dazu ausführlich den Beitrag 2.1 Privacy-Shield durch Schrems II gekippt: Wie geht’s weiter bei der Datenübermittlung in die USA?, 3. Tätigkeitsbericht zum Datenschutz nach der DS-GVO 2020).
Aufgrund des EuGH-Urteils musste die EU-Kommission zum nunmehr dritten Mal mit der US-Administration ein neues Datenschutzabkommen auf der Grundlage von Art. 45 Datenschutz-Grundverordnung (DS-GVO) aushandeln. Voraussetzung dafür war natürlich, dass zuvor im US-Recht Änderungen vorgenommen wurden, die den datenschutzrechtlichen Bedenken des EuGH-Urteils Rechnung trugen. Deshalb erließ US-Präsident Joe Biden am 7. Oktober 2022 die Executive Ordner No. 1486 („Enhancing Safeguards for United States Signals Intelligence Activities“, also: Verbesserung der Sicherheitsvorkehrungen für nachrichtendienstliche Tätigkeiten der Vereinigten Staaten), die die folgenden zwei wesentlichen Neuerungen vorsah: Zum einen wurde der Zugriff auf personenbezogene Daten von EU-Bürgerinnen und Bürgern für US-Nachrichtendienste unter dem Gesichtspunkt der Verhältnismäßigkeit beschränkt. Zum anderen wurde ein neues US-Datenschutzprüfungsgericht („Data Protection Review Court“) im Rahmen eines zweistufigen Prüfungsverfahrens eingesetzt.
Nicht zuletzt wegen dieser Rechtsänderungen hat die EU-Kommission dann am 10. Juli 2023 einen Angemessenheitsbeschluss verabschiedet und darin festgestellt, dass für die Übermittlung personenbezogener Daten unter dem neuen EU-US-Datenschutzrahmen (EU-US

Data Privacy Framework, abgekürzt: EU-US DPF) ein angemessenes Datenschutzniveau im Vergleich zur DS-GVO bestehe, wenn die Datenübermittlung an selbstzertifizierte US-Unternehmen erfolge (siehe dazu den Angemessenheitsbeschluss der EU-Kommission vom 10. Juli 2023 in englischer Fassung unter: https://commission.europa.eu/system/files/2023-07/Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework_en.pdf.
Die Datenschutzkonferenz (DSK) verabschiedete zum EU-US DPF am 4. September 2023 eine 32-seitige Ausarbeitung mit dem Titel „Übermittlung personenbezogener Daten aus Europa an die USA – Anwendungshinweise zum Angemessenheitsbeschluss der Europäischen Kommission zum Datenschutzrahmen EU-USA (EU-US Data Privacy Framework) vom 10. Juli 2023“ (siehe unter: https://datenschutzkonferenz-online.de/media/ah/230904_DSK_Ah_EU_US.pdf). Unter anderem wird in den Anwendungshinweisen erklärt, welche US-Organisationen sich wie zertifizieren lassen können und dass das US-Department of Commerce eine „Data Privacy Framework List“ (DPF-Liste) unterhält und veröffentlicht, die all diejenigen US-Organisationen auflistet, welche ihre Selbstzertifizierung unter dem EU-US Data Privacy Framework abgeschlossen haben.
Kritik oder rechtliche Unsicherheiten, die zum Inhalt des Angemessenheitsbeschlusses vor und nach seiner Veröffentlichung geäußert wurden, enthalten die Anwendungshinweise allerdings nicht – obwohl der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) ihre Aufnahme im Abstimmungsverfahren der Anwendungshinweise explizit gefordert hatte. Deshalb konnte der TLfDI der Annahme der DSK-Anwendungshinweise letztlich auch nicht zustimmen. Wesentlich war für ihn Folgendes, worauf er in seiner Pressemitteilung vom 4. September 2023 (siehe dazu: https://tlfdi.de/fileadmin/tlfdi/presse/Pressemitteilungen_2023/230904_PM_DPF.pdf) hinwies:
„*Die Menge an Kritikpunkten ist signifikant, weshalb der TLfDI der Auffassung ist, dass Datenexporteure, welche sich auf das Data Privacy Framework berufen wollen, sich der Kritikpunkte und damit dem Risiko des Widerrufs des Angemessenheitsbeschlusses bewusst sein sollten.*“
Folgende Kritikpunkte des Europäischen Datenschutzausschusses (EDSA) am EU-US DPF (siehe dazu: https://edpb.europa.eu/news/news/2023/edpb-welcomes-improvements-under-eu-

us-data-privacy-framework-concerns-remain_en) benannte der TLfDI in seiner Pressemitteilung vom 4. September 2023 ausdrücklich:

- Weiterbestehende **Ausnahmen für das Recht auf Auskunft von Betroffenen** bleiben bestehen (laut Annex I des Angemessenheitsbeschlusses, Section III „supplemental principles", Nr. 15, Buchstabe d insbesondere für öffentlich verfügbare Daten, aber zum Beispiel auch für Daten zu Forschungszwecken – Details findet man in Erwägungsgrund 31 des Angemessenheitsbeschlusses und dessen Fußnote 45). Das heißt, die Auskunft kann verweigert werden, wenn der Datenimporteur sich zum Beispiel hinter Daten zu Forschungszwecken „verstecken" kann.
- **Unspezifische Regelungen**, wann der **Anwendungsbereich des EU-US DPF** überhaupt **eröffnet ist**. Das heißt, es ist unklar, wann das DPF angewendet werden kann und welche Voraussetzungen in den Einzelfällen zum Beispiel bei Beschwerden, aber auch bei einer Auskunft eigentlich erfüllt sein müssen. Annex I, Section III, Nr. 8 a ii des Angemessenheitsbeschlusses erlaubt zum Beispiel das Recht auf Auskunft gegenüber Unternehmen ohne Vorbedingungen. Für das gleiche Recht (nur zu Zwecken der „nationalen Sicherheit" der USA) muss laut Erwägungsgrund 178 des Angemessenheitsbeschlusses die Betroffenheit nachgewiesen werden. Gelingt dieser Nachweis in dem einen Fall nicht, wird das Privacy Framework nicht angewendet. Weiterhin gibt es Ausnahmeregelungen zum Beispiel zu Journalisten (Annex I, Section III, Nr. 2), welche jegliche Recherchedaten vom DPF ausnehmen.
- **Fehlende Definition zentraler Begriffe** (und damit weiterbestehende Unklarheit bezüglich der Auslegung dieser Begriffe). Dies ist zum Beispiel dann problematisch, wenn entschieden werden muss, ob eine Datenerfassung „verhältnismäßig", also geeignet, erforderlich und angemessen ist. Die Begriffe werden im Angemessenheitsbeschluss und dessen Anhängen zwar durchgehend benutzt, aber nicht definiert. Damit kann jede Seite diese Begriffe unterschiedlich auslegen – und im Zweifel wird dies von den Aufsichtsstellen in den USA ausgelegt. Gleiches gilt für die Prüfung der „Notwendigkeit" (Erforderlichkeit), aber auch der „Betroffenheit" oder wann die Risiken für ein Individuum die Interessen der US-Organisation überwiegen (wie recht pauschal in Erwägungsgrund 31 aufgezählt).

- **Fehlende Klarheit**, **wie Verantwortliche die Prinzipien des EU-US DPF durchsetzen sollen**. Annex I Section III, Nr. 9 Buchstabe d erklärt zum Beispiel im Angestelltenverhältnis den Arbeitgeber zur primären Beschwerdestelle (und erst im Nachgang können weitere Stellen eingeschaltet werden). Weitere Anlaufstellen für Beschwerden wären je nach Beschwerdegegner das „Department of Commerce“ (DoC), das „Department of Transportation“ (DoT), die „Federal Trade Commision“ (FTC), die Datenschutzaufsichtsbehörden der EU, die zertifizierte US-Organisation, eine unklare Menge an Behörden, welche für Kriminalitätsbekämpfung zuständig sind (siehe Erwägungsgrund 107 und Fußnote 190 des Angemessenheitsbeschlusses sowie Erwägungsgrund 108 desselbigen), ein „Inspector General“, das „Privacy and Civil Liberties Oversight Board“ (PCLOB), der „Foreign Intelligence Surveillance Court“ (FISC), der „Civil Liberties Protection Officer of the Director of National Intelligence“ (ODNI CLPO) sowie der „Data Protection Review Court“ DPRC). Die Rolle einiger Stellen wird in den Anwendungshinweisen der DSK erklärt. **Die Wege zu diesen Beschwerdestellen sind ganz unterschiedlich gestaltet und für Betroffene ohne fundierte rechtliche Beratung schwer zu bewältigen.**
- **Vollständig fehlende Regelungen zu Profiling und zur automatisierten Entscheidungsfindung.**
- **Unklare Regelungen zur Massendatenerfassung für Zwecke der nationalen Sicherheit sowie deren Datenspeicherdauer und praktische Umsetzung der vereinbarten Regelungen**. Hier spielt primär Erwägungsgrund 141 die Hauptrolle. Dieser erlaubt Massendatenerfassung der Geheimdienste (wie Edward Snowden 2013 offenlegte), wenn eine gezielte Datensammlung nicht möglich ist und zweitens die „Notwendigkeit“ der Maßnahme begründet werden kann. Ist dies der Fall, soll die Massendatenerfassung auf das notwendige Minimum reduziert werden. Zur Begründung der „Notwendigkeit“ und was das „notwendige Minimum“ ist, werden keine Festlegungen getroffen. Eine mit der EU-Rechtsprechung vergleichbare Auslegung ist auch hier nicht garantiert.
- **Fehlende Autorisierung zur Massendatenerfassung durch eine unabhängige Stelle**, stattdessen nur nachträgliche Prüfmöglichkeit im Fall von zugelassenen Beschwerden.

- **Nachträgliche Prüfung** wird **nicht durchgängig durch vom Geheimdienst unabhängige Stellen gewährleistet**. Vielmehr ist der hierfür eingerichtete „Foreign Intelligence Surveillance Court“ (FISC) zwar ein unabhängiges Gericht, ist jedoch an die Geheimdienste der USA angegliedert. Außerdem ist dessen Tätigkeit von außen nicht weiter überprüfbar (siehe Annex VII des Angemessenheitsbeschlusses).
- Der **Status der Prüfung** bei einer **Beschwerde gegen geheimdienstliches Handeln ist nach wie vor zu intransparent**, das heißt, es ist unklar, ob die Beschwerde überhaupt angenommen wurde, ob Maßnahmen getroffen wurden und welche Maßnahmen dies überhaupt sind. So wurde früher nur mitgeteilt: „Ohne zu bestätigen oder zu leugnen, dass der Beschwerdeführer Gegenstand von Aktivitäten des US-Signalnachrichtendienstes war, wurden bei der Überprüfung entweder keine erfassten Verstöße festgestellt, oder das Datenschutzüberprüfungsgericht hat eine Feststellung getroffen, die angemessene Abhilfemaßnahmen erfordert.“ In Erwägungsgrund 183 wird dieser Satz bereits als Zitat wieder aufgegriffen. Diese Mitteilung kann nun vom Betroffenen pauschal angegriffen werden, woraufhin ein ausgewählter Jurist den Beschwerdeführer vertritt.

Aufgrund all dieser berechtigten Einwände des EDSA wies Dr. Lutz Hasse am Ende der Pressemitteilung vom 4. September 2023 auf Folgendes hin: *„Unternehmen etwa sollten vor diesem Hintergrund abwägen, ob sie sensible Daten – auch Kundendaten – in die USA transferieren oder bis zur Entscheidung des EuGHs vorsorglich nicht. Denn die Wahrscheinlichkeit, dass der Europäische Gerichtshof den Adäquanzbeschluss aufheben wird, ist danach recht hoch.“*

In diesem Zusammenhang sei noch auf eine Entscheidung des Oberlandesgerichts Köln hingewiesen (OLG Köln, Urteil vom 3. November 2023, Aktenzeichen:6 U 58/23), die am Ende des Jahres 2023 für Beachtung, aber auch für gewisse Irritationen sorgte. In ihrem Urteilsspruch, in dem es um die Deutsche Telekom ging, die beim Aufruf ihrer Internetseite personenbezogene Daten an das Unternehmen Google LLC. in die USA übermittelte, gingen die Kölner Richter auch auf den neuen Angemessenheitsbeschluss, den EU-US DPF, ein und stellten dazu unter anderem Folgendes fest: „*Doch auch beim Vorliegen des neuen Angemessenheitsbeschlusses müssen die übrigen Anforderungen an eine zulässige Datenverarbeitung erfüllt sein, wozu unter anderem das Erfordernis der Einwilligung gehört.“*

Mit diesem Hinweis wollte das OLG Köln mitnichten den EU-US DPF rechtlich bewerten (was es auch gar nicht dürfte), sondern lediglich darauf hinweisen, dass neben der rechtlichen Befugnis für Übermittlungen von personenbezogenen Daten in Drittländer, wie zum Beispiel die USA, auch die übrigen Voraussetzungen für eine rechtmäßige Datenverarbeitung beachtet und erfüllt sein müssen.

1.3 ChatGPT und KI

Aufgrund der massentauglichen Nutzbarkeit von insbesondere ChatGPT und gleichzeitig der vielen offenen Fragen, welche sich aus der Nutzung dieser Technologie ergeben, untersucht der TLfDI zurzeit die datenschutzrechtlichen Risiken und Anforderungen von ChatGPT. Nutzer sollten sich vor der Nutzung sehr gut über die bisher bekannten Risiken und Grenzen des Systems erkundigen und keinesfalls sensible Informationen an das System preisgeben. Aufgrund des Neuheitswertes dieser Technologie wird eine abschließende Bewertung noch einige Zeit in Anspruch nehmen. Daher sollte die Technologie, wenn personenbezogene Chat-Inhalte betroffen sein könnten, nur sehr vorsichtig, wenn überhaupt, genutzt werden.

Ende des Jahres 2022 hatte eine bis dahin in der breiten Öffentlichkeit unbekannte Firma OpenAI LLC ein Chatprogramm veröffentlicht, bei dem jedermann Fragen und Aufgaben stellen kann und eine integrierte „Künstliche Intelligenz (KI)“ die Antwort kreiert – genannt ChatGPT. Das Kürzel ChatGPT steht dabei für die englische Bezeichnung „***Chat****bot* ***G****enerative* ***P****re-trained* ***T****ransformer“*.
In Fachkreisen war die Firma OpenAI LLC, ein US-amerikanisches Unternehmen, natürlich nicht unbekannt, sondern vielmehr ein Vorreiter in der Entwicklung „generativer KI“ – und dies bereits seit dem Jahr 2018. Bisher wurde KI zum Klassifizieren von Mustern (wie Autos, Nummernschilder, Gesichter und so weiter in Bildern) genutzt. Generative KI hingegen kann Bilder von zum Beispiel Autos, Nummernschildern, Gesichtern erzeugen – und das bereits seit den ersten Arbeiten von Google im Jahr 2015. Bis dahin waren die Fähigkeiten der generativen KI nur Forschern und Programmierern zugänglich.
In das Bewusstsein der breiten Bevölkerung gelangte diese Technik erst im Berichtszeitraum, als das Programm ChatGPT eine solche generative KI durch eine einfache „Software zur Konversation“ nutzbar

machte. Was kann ChatGPT? Nicht viel mehr, als auf natürlich formulierte Texte wie zum Beispiel Fragen oder Aufgaben genauso natürlich zu antworten wie ein Gesprächspartner dies tun würde. Diese Texte können Fragen sein, Aufgaben (auch aus dem Unterricht), die Ausformulierung von Ideen, Gedichte und vieles mehr. Tatsächlich sind der Fantasie der Nutzer hier keine Grenzen gesetzt. Seit Anfang 2023 erweitern sich die Fähigkeiten von ChatGPT auch kontinuierlich weiter. Nach dem ursprünglichen Modell in Version 3.5 wurde das Modell 4.0 nutzbar gemacht (als Bezahlversion von ChatGPT), welches neben Text auch Bilder ausgeben kann und sehr viel akkurater und „gutmütiger" ist. Dies bedeutet, dass ChatGPT weniger Fakten erfindet und auf Fragen, deren Beantwortung anderen Personen potentiell schaden könnte, keine Antwort gibt. So werden zum Beispiel Fragen nach Anleitungen zu Sprengstoffherstellung oder wie Personen am besten ausspioniert werden könnten, nur ausweichend beantwortet. Seit Oktober 2023 versteht Modell 4 nicht nur Text als Eingabe, sondern auch Bilder. Damit sind Aufgaben möglich wie: „Zeige mir dieses Bild als Foto mit einem Strand und Palmen" oder „Entwirf eine Website mit folgender Oberfläche". Insgesamt steht somit ein sehr mächtiges Werkzeug zur Verfügung, um lästige, sich wiederholende Aufgaben einer bisher nicht-automatisierbaren Art von einer Maschine bewältigen zu lassen.

Doch warum interessiert dies die unabhängigen deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder? Die Antworten auf diese Frage sind vielfältig.

Erstens basieren die Fähigkeiten von ChatGPT auf sehr großen Datenmengen, welche zum Training des dahinterliegenden Modells genutzt wurden. Für die Version 3.5 wurden circa 570 Gigabyte Text an Daten genutzt – die Datenmenge der nachfolgenden Modelle ist unbekannt, aber mit hoher Sicherheit mehr als 570 Gigabyte.

Die Textquellen für die Antworten sind offen verfügbare Informationen aus dem Internet, welche von CommonCrawl.org frei zur Verfügung gestellt wurden. Darunter sind auch offen verfügbare Forenbeiträge, Posts in sozialen Netzwerken und öffentlich zugängliche Zeitungsartikel. Mit anderen Worten sind diese Quellen durchsetzt von personenbezogenen Daten, welche alle zum Trainingszeitpunkt auch in das Sprachmodell wanderten. Nun funktioniert ein Sprachmodell nicht wie eine Datenbank und man kann auch nicht bestimmte Informationen an bestimmten Stellen im Modell wiederfinden. Vielmehr

sind die Informationen nur implizit durch Netzwerkgewichte im Modell repräsentiert, das heißt auf Milliarden von Bruchstücken verteilt, die nur durch gemeinsames Zusammenwirken wieder eine bestimmte Information erzeugen. Es ist der Forschung momentan noch gar nicht klar, wie ein so großer Informationsbestand an Text durch bestimmte Anfragen beziehungsweise „Unterhaltungen“ mit dem Modell beeinflussbar ist. Neben den vielen nützlichen Eigenschaften von ChatGPT sind daher die Risiken der im Modell kodierten Informationen über gespeicherte Personen nur im Ansatz verstanden. Gerade, wenn Nutzerinputs zum Nachtraining des Modells genutzt werden, ist zurzeit unklar, wie gut Sicherheitsmechanismen wirken, dass solche Daten nicht im Nachgang einfach erfragt werden können oder gar nicht im Modell enthalten sind. Weiterhin gibt OpenAI auch offen zu, die Unterhaltungen mit dem Modell auch als Trainingsdaten zu nutzen (dem können Nutzer aber explizit widersprechen, siehe Link https://openai.com/blog/new-ways-to-manage-your-data-in-chatgpt).
Weitere Daten werden laut OpenAI zu Analysezwecken genutzt. Zur Anmeldung sind eine E-Mail-Adresse und eine Telefonnummer erforderlich. Es wird nicht verhindert, dass Nutzer personenbezogene Daten Dritter in den Chatverlauf eintragen. ChatGPT kann sogar aufgefordert werden, Schlussfolgerungen über eine solche Person auszugeben, wie zum Beispiel: „Ich habe über eine Person folgende Informationen gefunden: [Informationen …] Welche Partei Deutschlands würde diese Person wahrscheinlich wählen?“ Andere (potentielle) Schwachstellen des Modells sind zum Beispiel, dass es Informationen frei erfinden kann, wie dies Menschen auch können. Dies ist bei Ideenfindung von Vorteil, aber an anderen Stellen von Nachteil. Es handelt sich bei ChatGPT nicht um eine Suchmaschine, und dies muss vom Nutzer verstanden werden.
Aus Sicht der deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder gilt es, auch bei der Anwendung in Deutschland, die Datenschutz-Grundverordnung (DS-GVO) einzuhalten. Also für die Verarbeitungsprozesse von personenbezogenen Daten die Transparenz, Kontrolle und bestimmte Rechte von betroffenen Personen zu gewährleisten. Hier sind Konflikte sichtbar: auf der einen Seite ein Modell mit einem schwer beeinflussbaren Speicherschema, Unmengen an personenbezogenen Daten und noch einer völlig unklaren Lage, wie Nutzer dem System eventuell private Informationen entlocken können. Auf der anderen Seite stehen die gesetzlichen Regelungen zu Klarheit bei der Verarbeitung, Sicherheit von Systemen und

bestimmten Betroffenenrechten. Grund genug für den Thüringer Landesbeauftragten für Datenschutz und die Informationsfreiheit (TLfDI) gegen OpenAI von Amts wegen aktiv zu werden und in erster Stufe Klarheit zu den oben genannten Eckpunkten zu verlangen. Gleichartige Verfahren starteten parallel auch andere Datenschutzbeauftragte der Mitgliedstaaten der Europäischen Union und auch viele andere deutsche Datenschutzaufsichtsbehörden. Bisher konnte OpenAI noch keine zufriedenstellenden Antworten gegenüber dem TLfDI liefern – was auch der Tatsache geschuldet ist, dass ChatGPT aus deren Sicht eigentlich eine experimentale Software ist.
Jedem Nutzer sollten daher die Schwachstellen von ChatGPT bewusst sein (tendiert zum Fantasieren, manchmal auch zur emotionalen Beeinflussung) und momentan rät der TLfDI bei der privaten Nutzung strikt davon ab, jegliche Art von sensiblen Daten (zum Beispiel zu Fragen der Gesundheit, zum psychologischen Zustand, über Geldnöte, politische Äußerungen) in Unterhaltungen mit ChatGPT zu nutzen. Gleiches gilt für Microsoft-Dienste, die dieses Modell auch schon nutzen (wie Microsoft Bing-Chat oder Microsoft Copilot). Insbesondere die öffentliche Verwaltung muss vor Einsatz solcher Produkte die Einhaltung der DS-GVO prüfen.
Bereits 2019 hatte die Datenschutzkonferenz (DSK), das Gremium der unabhängigen deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder ein *„Positionspapier der DSK zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen“* veröffentlicht (https://www.datenschutzkonferenz-online.de/media/en/20191106_positionspapier_kuenstliche_intelligenz.pdf).
Als erste Aufsichtsbehörde in Europa hatte 2023 die italienische Datenschutzbehörde der Firma OpenAI untersagt, personenbezogene Daten von italienischen Bürgerinnen und Bürgern im Rahmen der Anwendung ChatGPT zu verarbeiten. Dieses Verbot wurde später jedoch wieder aufgehoben. Der TLfDI nahm dies zum Anlass, am 14. April 2023 in einer entsprechenden Pressemitteilung darauf hinzuweisen, siehe https://tlfdi.de/presse/pressemitteilungen/chatgpt-auf-dem-pruefstand/. Der TLfDI wird sich weiter an der rechtlichen und technischen Prüfung von ChatGPT beteiligen und die Untersuchungen weiter vorantreiben. Diesbezüglich ist er nun auch in verschiedenen Gremien aktiv. Eine abschließende Bewertung ist aber in nächster Zeit nicht zu erwarten. Der TLfDI wird bei neuen Erkenntnissen informieren.

1.4 Auftragsverarbeitungsvereinbarung hinsichtlich Microsoft 365

Mit Stand 24. August 2023 haben einige deutsche Datenschutzaufsichtsbehörden eine *Handreichung für die Verantwortlichen zum Abschluss einer Auftragsverarbeitungsvereinbarung gemäß Art. 28 Abs. 3 DS-GVO mit Microsoft für den Einsatz von Microsoft 365* veröffentlicht. Der TLfDI war an der Erstellung der Handreichung beteiligt. Die Handreichung versetzt Verantwortliche nun in die Lage, Microsoft entsprechende Nachfragen zu stellen und Vertragsänderungen vorzuschlagen.

Auch im Berichtszeitraum 2023 gab es Entwicklungen zum Thema Microsoft 365. Zur Erinnerung: Die Datenschutzkonferenz (DSK), das Gremium der unabhängigen deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder, nahm am 24. November 2022 den Bericht der Arbeitsgruppe DSK „Microsoft-Onlinedienste“ und dessen Zusammenfassung zur Kenntnis. Die DSK stellte damals fest, dass zum Beispiel aufgrund fehlender Transparenz bei der Datenverarbeitung ein Verantwortlicher nicht in der Lage ist, die Anforderungen an die Rechenschaftspflicht gegenüber Nutzern (das heißt Betroffenen) zu erfüllen: „Solange insbesondere die notwendige Transparenz über die Verarbeitung personenbezogener Daten aus der Auftragsverarbeitung für Microsofts eigene Zwecke nicht hergestellt und deren Rechtmäßigkeit nicht belegt wird, kann dieser Nachweis nicht erbracht werden.“ Zu diesem Kritikpunkt kommen noch weitere Kritikpunkte hinzu, zum Beispiel zu eigenen Verarbeitungszwecken Microsofts, zur Löschung von personenbezogenen Daten, mögliche Zugriffe von Drittstaaten auf Server Microsofts und die Einbeziehung von Unterauftraggebern. Details sind im umfangreichen Bericht unter https://datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365.pdf und https://www.datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365_abschlussbericht.pdf zu finden. Die Kritik bezieht sich dabei ausschließlich auf die Online-Dienste Microsofts sowie Datenflüsse, die diese Online-Dienste mit Daten versorgen, und nicht, wie irrtümlich manchmal behauptet, pauschal auf jede Microsoft Software.
Am 10. Juli 2023 hat die Europäische Kommission den Angemessenheitsbeschluss für das EU-U.S. Data Privacy Framework (Nachfolger

des „Privacy Shields“) angenommen. Der Angemessenheitsbeschluss kann nunmehr als Grundlage für Datenübermittlungen an zertifizierte Organisationen in den USA dienen (https://www.bfdi.bund.de/SharedDocs/Kurzmeldungen/DE/2023/17_Angemessenheitsbeschluss-EU-US-DPF.html). Somit wurden einige Kritikpunkte der Untersuchung zumindest entschärft, aber die Hauptkritikpunkte zu mangelnder Transparenz (auch der *eigenen Verarbeitungszwecke* Microsofts) bleiben bestehen. Da dies vor allen Dingen ein Problem der Verantwortlichen ist – also der Auftraggeber gegenüber Microsoft – haben sich einige deutsche Datenschutzaufsichtsbehörden in einer Arbeitsgruppe zusammengefunden, um eine Handreichung für die Verantwortlichen zum Abschluss einer Auftragsverarbeitungsvereinbarung gemäß Art. 28 Abs. 3 Datenschutz-Grundverordnung (DS-GVO) mit Microsoft für den Einsatz von „Microsoft 365“ zu entwickeln. Die Auftragsverarbeitung mit Microsoft wird über das „Products and Services Data Processing Addendum“ (DPA) geschlossen und wird von Microsoft vorgegeben (siehe https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA). Es ist jedoch nicht unveränderbar. Die Handreichung greift die Kritikpunkte der DSK wieder auf und zeigt mögliche Lösungsansätze, um Verantwortlichen Handlungsvorschläge zu unterbreiten, welche *Vertragsänderungen im DPA* mit Microsoft angestrebt werden sollten oder welche Fragestellungen zur Datenverarbeitung mit Microsoft geklärt werden müssen.

Wichtig zu wissen ist, dass bloße vertragliche Zusicherungen von Microsoft, etwa dergestalt, dass personenbezogene Daten nicht mehr zu eigenen Zwecken verarbeitet werden, für den Verantwortlichen nicht ausreichen, um Datenschutzkonformität nachzuweisen. Vielmehr sind insoweit aktive Kontrolltätigkeiten des Verantwortlichen erforderlich (Roßnagel in Simitis, DSGVO-Kommentar, Art. 5 Rn. 174, 181 ff.).

Wenn dem Verantwortlichen klar ist, welche Daten zu welchen Zwecken verarbeitet werden, so ist es eine wichtige Aufgabe des Verantwortlichen, zu den Zwecken eine Rechtsgrundlage zur Verarbeitung nachzuweisen. Dies kann durch Microsoft als Auftragsdatenverarbeiter nicht geschehen. Auch hier hilft die Handreichung weiter und weist auf die Textstellen im Microsoft-Vertragswerk hin, in welchem Verarbeitungszwecke festgelegt werden.

Auch der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit ist an der Erstellung dieser Handreichung beteiligt gewesen. Federführend wurde diese durch den Datenschutzbeauftragten für den Datenschutz Niedersachsen koordiniert und mit Stand 24. August 2023 veröffentlicht (siehe https://www.lfd.niedersachsen.de/download/199434).

1.5 Umfang und Inhalt des Anspruchs auf Auskunft und Kopie

Nach Art. 15 Abs. 3 DS-GVO hat der Verantwortliche der betroffenen Person auf Antrag unentgeltlich eine vollständige und originalgetreue Zusammenstellung ihrer personenbezogenen Daten zur Verfügung zu stellen. Lassen sich die verarbeiteten Daten nur im Kontext erschließen, hat der Betroffene darüber hinaus einen Anspruch auf Kopie des Dokuments, in dem seine personenbezogenen Daten enthalten sind. Dies gilt namentlich für Befunde und andere Dokumente, die sich in der Patientenakte der betroffenen Person befinden.

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichten wiederholt Anfragen, die sich auf Umfang und Inhalt der nach Art. 15 Abs. 3 Datenschutz-Grundverordnung (DS-GVO) bereitzustellenden Kopie personenbezogener Daten und die Kosten für eine Abschrift oder Kopie der Patientenakte bezogen.
Lange Zeit wurde die Frage nach der Reichweite des Rechts auf Erhalt einer Kopie personenbezogener Daten kontrovers diskutiert und auch in der Rechtsprechung nicht einheitlich beantwortet. Nunmehr hat der Europäische Gerichtshof (EuGH) in einer Leitentscheidung eine grundsätzliche Klärung herbeigeführt (EuGH, Urteil vom 4. Mai 2023, C-487/21) und die dabei entwickelten Grundsätze im Hinblick auf die in der Patientenakte enthaltenen Gesundheitsdaten konkretisiert (EuGH, Urteil vom 26. Oktober 2023, C-307/22).
Wie das Gericht feststellt, bezieht sich der Begriff der „Kopie“ nicht auf ein Dokument als solches, sondern auf die personenbezogenen Daten, die es enthält und die vollständig sein müssen. Als besonderer Form der Auskunftserteilung wird daher dem Anspruch auf Erhalt einer Kopie regelmäßig Rechnung getragen, wenn dem Antragsteller zunächst eine vollständige und verständliche Zusammenstellung seiner personenbezogenen Daten zur Verfügung gestellt wird, die Gegenstand der Verarbeitung sind. Dabei muss es sich allerdings um eine

originalgetreue Reproduktion der personenbezogenen Daten handeln, sodass eine bloße Auflistung oder allgemeine Beschreibung der verarbeiteten Daten (Adresse, Geburtsdatum et cetera) nicht genügt. Da die betroffene Person nicht verpflichtet ist, ihren Antrag zu begründen, ist es auch unerheblich, welchen Zweck sie mit der Datenkopie verfolgt.
Auch wenn dies nicht der primäre Gegenstand des Auskunftsrechts ist, kann sich darüber hinaus die Bereitstellung von Dokumenten oder Dateien als unerlässlich erweisen, wenn der Kontext der verarbeiteten Daten erforderlich ist, um ihre Verständlichkeit zu gewährleisten und der betroffenen Person die wirksame Ausübung ihrer Rechte zu ermöglichen.
Dies ist etwa der Fall, wenn die Daten nicht bei der Person selbst erhoben, sondern aus anderen Daten generiert werden. Gleiches gilt, wenn sich die Daten nicht aus den Quelldokumenten isolieren lassen, ohne dass damit ihr Aussagegehalt verkürzt oder verfälscht wird. Hiervon ist regelmäßig bei Dokumenten auszugehen, die sich gemäß § 630f Abs. 2 Bürgerliches Gesetzbuch (BGB) in der Patientenakte befinden und bei denen die Gefahr besteht, dass bei einer einfachen Zusammenstellung relevante Daten ausgelassen oder unrichtig wiedergegeben werden.
Die Reproduktion von Auszügen aus Dokumenten oder Dateien, die personenbezogene Daten enthalten, kann sich als unerlässlich erweisen, wenn der (medizinische) Zusammenhang, in dem die personenbezogenen Daten verarbeitet wurden, erforderlich ist, um ihre Verständlichkeit zu gewährleisten und der betroffenen Person die wirksame Ausübung ihrer Rechte zu ermöglichen. In Bezug auf die Gesundheitsdaten der betroffenen Person ist hiervon bei Dokumenten auszugehen, die sich in der Patientenakte befinden und bei denen die Gefahr besteht, dass bei einer einfachen Zusammenfassung oder Zusammenstellung relevante Daten ausgelassen oder unrichtig wiedergegeben werden. Hierzu zählt Erwägungsgrund 63 Satz 2 DS-GVO Informationen wie beispielsweise Diagnosen, Untersuchungsergebnisse, Befunde der behandelnden Ärzte und Angaben zu Behandlungen oder Eingriffen. Diese entsprechen im Wesentlichen den dokumentationspflichtigen Unterlagen nach § 630f Abs. 2 BGB (vergleiche Wagner, Münchner Kommentar zum BGB, § 630f RN 7 ff.), sodass der betroffenen Person im Zweifelsfall die in der Patientenakte enthaltenen Dokumente unentgeltlich zur Verfügung zu stellen sind,

sofern nicht therapeutische Gründe oder Rechte Dritter entgegenstehen (§ 630g Abs. 1 BGB).
Somit hat der Verantwortliche aufgrund des Anwendungsvorrangs des Unionsrechts gemäß Art. 15 Abs. 3 Satz 2 DS-GVO in aller Regel eine kostenfreie Erstkopie der Patientenakte zur Verfügung zu stellen.
Mit Schreiben vom 7. Dezember 2023 hat der TLfDI die Landesärztekammer Thüringen über diese Auslegung von Art. 15 Abs. 3 DS-GVO unter Berücksichtigung von § 630g Abs. 2 Satz 2 BGB informiert.
Wenngleich der Anspruch auf Kopie isoliert geltend gemacht werden kann, ist eine strukturierte, an den Details der Verarbeitung orientierte Zusammenstellung angebracht, um auch dem Anspruch auf Auskunft nach Art. 15 Abs. 1 DS-GVO gerecht zu werden. Dabei sind dem Betroffenen neben dem Zweck und der Dauer der Datenverarbeitung die konkreten Empfänger seiner Daten und nicht nur Empfängerkategorien (mitbehandelnde Ärzte, Krankenkassen et cetera) mitzuteilen, es sei denn, es ist nicht möglich, die Empfänger zu identifizieren (EuGH, Urteil vom 12. Januar 2023, C-154/21).

1.6 Gesetz zur Änderung des BDSG

Das Bundesdatenschutzgesetz soll im Ergebnis der durchgeführten Evaluierung und in Umsetzung des Koalitionsvertrages angepasst werden. Die geplanten Änderungen haben auch Auswirkungen auf die Arbeit des TLfDI.

Mit der Datenschutz-Grundverordnung (DS-GVO) wurde das Datenschutzrecht in der Europäischen Union (EU) weitgehend einheitlich geregelt. Vor diesem Hintergrund wurde auf Bundesebene das Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und Umsetzungsgesetz EU – DSAnpUG-EU) erlassen. Das in Deutschland bis dahin geltende Bundesdatenschutzgesetz (BDSG) wurde mit dem Geltungsbeginn der DS-GVO am 25. Mai 2018 in weiten Teilen unanwendbar. Mit dem DSAnpUG-EU wurden die im Hinblick auf die DS-GVO erforderlichen gesetzlichen Anpassungen in einem neuen Bundesdatenschutzgesetz vorgenommen. Das DSAnpUG-EU ist nach der Gesetzesbegründung spätestens

drei Jahre nach seinem Inkrafttreten zu evaluieren. Das Bundesministerium des Innern, für Bau und Heimat (BMI) führte die Evaluierung durch. Der Evaluationsbericht findet sich unter https://www.bmi.bund.de/SharedDocs/evaluierung-von-gesetzen/downloads/berichte/evaluierung-bdsg.pdf?__blob=publicationFile&v=5. Im Ergebnis der Evaluation wurden einige Änderungsbedarfe am BDSG festgestellt.
Auch der Koalitionsvertrag zwischen SPD, BÜNDNIS 90/DIE GRÜNEN und FDP enthält unter dem Punkt „Digitale Innovation und digitale Infrastruktur“ Vorhaben, die Datenschutzbezug haben (https://www.bundesregierung.de/resource/blob/974430/1990812/93bd8d9b17717c351633635f9d7fba09/2021-12-10-koav2021-data.pdf?download=1). So soll zur besseren Durchsetzung und Kohärenz des Datenschutzes die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) im BDSG institutionalisiert werden und es soll ihr rechtlich ermöglicht werden, verbindliche Beschlüsse zu fassen.
Das BMI legte einen Referentenentwurf eines „Ersten Gesetzes zur Änderung des Bundesdatenschutzgesetzes“ vor, der die Vereinbarungen des Koalitionsvertrags aufgreifen sowie die Ergebnisse der Evaluation umsetzen soll (https://www.bmi.bund.de/SharedDocs/downloads/DE/gesetzestexte/gesetzesentwuerfe/entwurf_aendG_bdsg.pdf;jsessionid=0C66B63FA4B109168E87201E2420AD37.live872?__blob=publicationFile&v=4).
Zur DSK, der auch der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit angehört, findet sich eine Regelung im Gesetz, allerdings wird eine Regelung zur rechtlichen Verbindlichkeit von Beschlüssen der DSK mit der Begründung nicht getroffen, dass damit gegen das Verbot der Mischverwaltung verstoßen werde.
Die DSK nahm zu dem Gesetzentwurf Stellung (https://www.datenschutzkonferenz-online.de/media/st/23_09_06_DSK_Stellungnahme_BDSG.pdf).
Darin weisen die Mitglieder der DSK auf die Notwendigkeit und Schwierigkeit der einheitlichen Rechtsanwendung hin. Vor diesem Hintergrund wird die vorgesehene Institutionalisierung der DSK grundsätzlich begrüßt. Die vorgesehene gesetzliche Bestimmung umschreibt die DSK allerdings unzutreffend. Die DSK soll durch den oder die Bundesbeauftragten/Bundesbeauftragte für den Datenschutz

und die Informationsfreiheit sowie die Aufsichtsbehörden der Länder im Sinne des § 40 BDSG gebildet werden. Damit werden nur die nach Landesrecht für die Datenschutzaufsicht im nicht-öffentlichen Sektor zuständigen Behörden erfasst und der Bayerische Landesbeauftragte für den Datenschutz wäre aus der DSK ausgeschlossen. Dies bedarf einer klarstellenden Änderung.
Die DSK bekräftigt die Notwendigkeit der Errichtung einer Geschäftsstelle, die im Gesetzentwurf nicht vorgesehen war. Eine ständige Geschäftsstelle bringt einen Gewinn an Professionalität und eine Steigerung der Kontinuität im Handeln der DSK.
Es bleibt abzuwarten, ob die DSK den Gesetzgeber von der Notwendigkeit der Errichtung einer Geschäftsstelle der DSK überzeugen kann. Der TLfDI wird sich hierfür im Rahmen der DSK einsetzen. Die notwendigen Harmonisierungsmaßnahmen der DSK, wie eine konsistente Datenschutzaufsicht, die Verantwortlichen, Auftragsverarbeitern und betroffenen Personen Rechtssicherheit bietet, abgestimmte Stellungnahmen zu Gesetzentwürfen oder Praxisfragen der Verarbeitung in Deutschland und Europa, können angesichts der fortschreitenden Digitalisierung verlässlich nur weiter gewährleistet werden, wenn sie die notwendige organisatorische Unterstützung durch eine Geschäftsstelle erfahren. Dies ist in besonderem Maße für personell nicht so gut aufgestellte Aufsichtsbehörden unerlässlich.

1.7 Kriterien für Souveräne Clouds

Verantwortliche, welche Datenverarbeitungen in Cloud-Systemen beauftragen, stehen bisher häufig vor datenschutzrechtlichen Problemen. Die DSK hat daher Anforderungen und Erwartungen an souveräne Clouds formuliert, welche dem Verantwortlichen die nötigen Kontrollmöglichkeiten aufzeigen und dem Anbieter die nötigen Kriterien an die Hand geben, um echte Souveränität zu erreichen. Eine „Souveräne Cloud“ verdient diesen Namen nur, wenn sie es dem Verantwortlichen ermöglicht, seinen datenschutzrechtlichen Pflichten effektiv, nachprüfbar und dauerhaft nachzukommen, diese also selbstständig, selbstbestimmt und sicher ausüben zu können.

In den letzten Jahren war der deutliche Trend bei Unternehmen, Privatanwendern und öffentlichen Stellen zu erkennen, immer mehr Datenverarbeitungen in „die Cloud“ auszulagern. Gemeint sind hier

große Rechenzentren, welche Dienste wie Datenspeicherung, Backups, Webserver, Anwendungen oder ganze Funktionsblöcke betreiben können (Warenhaltung und Management, Personalverwaltung und so weiter). So sind Cloud-Nutzer heutzutage vor allen Dingen bei Cloud-Systemen von Microsoft, Apple, Amazon, Oracle und Adobe verortet. Die Kunden sind dabei meist die datenschutzrechtlich Verantwortlichen und die Cloud-Anbieter selber „nur“ als Auftragsverarbeiter eingebunden.
Mit Inkrafttreten der Datenschutz-Grundverordnung (DS-GVO) kamen sowohl auf Auftragnehmer (Cloud-Anbieter) als auch auf Verantwortliche (Kunden) zusätzliche Transparenzpflichten hinzu. Auch regelt nun Art. 20 DS-GVO das Recht auf Datenportabilität, das heißt das Recht auf Datenübertragbarkeit. In der Praxis werden die Transparenzpflichten sowohl vom Auftragnehmer als auch vom Auftraggeber oft nicht erfüllt. Art. 5 Abs. 1 Buchstabe a) DS-GVO schreibt aber fest, dass jede Verarbeitung personenbezogener Daten in einer für die Betroffenen nachvollziehbaren Weise zu erfolgen hat (Transparenzgrundsatz). Dieser Grundsatz wird insbesondere durch die Informations- und Auskunftspflichten gemäß Art. 12 ff. DS-GVO konkretisiert.
Verantwortliche, die Cloud-Dienste einsetzen, müssen nach Art. 5 Abs. 2 und Art. 24 Abs. 1 DS-GVO zudem sicherstellen, dass die mit diesen Diensten erfolgende Verarbeitung personenbezogener Daten gemäß den Vorgaben der DS-GVO erfolgt und hierfür den Nachweis erbringen (Rechenschaftspflicht). Verantwortliche Anwendende müssen ihrerseits über hinreichende Informationen verfügen, um ihrer Rechenschaftspflicht nachzukommen und ihre Pflichten gegenüber den Betroffenen umsetzen zu können. Soweit regelt die DS-GVO alle Anforderungen an eine Datenverarbeitung. Doch wozu veröffentlicht die Datenschutzkonferenz (DSK) eine Stellungnahme zu diesem Thema? Dazu aus der Stellungnahme: „Digitale Souveränität umfasst dabei mehr als die bloße Einhaltung der Datenschutzanforderungen. Digitale Souveränität ist nur erfüllt, wenn sie dazu beiträgt, das dargestellte Umsetzungsproblem [der datenschutzgerechten Umsetzung der Verarbeitung, Erg. der Redaktion] grundlegend und nachhaltig zu lösen. Dementsprechend erfordert der Schritt von einer datenschutzkonformen Cloud hin zu einer souveränen Cloud auch die Erfüllung begleitender Kriterien, die die Einhaltung der datenschutzrechtlichen Pflichten effektiv, nachprüfbar und dauerhaft sicherstellen.“

Teil der Souveränität ist auch die Vermeidung potentieller Drittstaatentransfers von personenbezogenen Daten sowie eventuell mögliche Zugriffe von Drittstaaten auf Server in der der Europäischen Union (EU). *Drittstaaten* sind Staaten, die kein Mitglied der Europäischen Union sind. Aufgrund dieser entstehenden Verschiebung der tatsächlichen Verfügungsgewalt kommt der Gewährleistung der Rechtsdurchsetzung besondere Bedeutung zu.
Die DSK, das Gremium der unabhängigen deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder, ist deshalb der Ansicht, dass eine Kontrollierbarkeit voraussetzt, dass die Cloud nur von in der EU ansässigen Anbietenden betrieben wird. Hiervon umfasst ist, dass sich sowohl der Unternehmenssitz des Anbietenden, als auch der Standort der Rechenzentren in der EU befinden (siehe Kriterium 2.4), weil dort die Einhaltung und notfalls gerichtliche Durchsetzbarkeit des Datenschutzniveaus langfristig sichergestellt ist. Es ist nicht ausreichend, dass der entsprechende Server von einer in der EU ansässigen Gesellschaft betrieben wird, die ihrerseits Teil eines Drittstaaten-Konzerns ist, da dieser seinerseits rechtlichen Bindungen des Drittstaates unterliegen kann. Als souveräne Cloud kann daher nur der Betrieb eines vollständig in der EU ansässigen Anbietenden gelten.
Ebenso weist die DSK in ihrem Papier daraufhin, dass bei Auslagerung umfangreicher Datenverarbeitungen in die Cloud ein Wechsel des Systems häufig nur sehr schwer möglich ist. Stellt sich im Nachgang heraus, dass ein Angebot nicht datenschutzkonform eingesetzt werden kann, ist ein Wechsel häufig unmöglich bis sehr schwierig und teuer. Souveräne Cloud-Angebote müssen ihren Anwendenden einen möglichst einfachen Ersatz ermöglichen. Hierzu müssen Anbietende geeignete Möglichkeiten zum Export aller relevanten Daten bereitstellen. In Abhängigkeit vom Cloud-Angebot sollten auch weitere Objekte möglichst einfach in eine neue Umgebung überführbar sein, zum Beispiel virtuelle Rechner, Konfigurationen virtueller Umgebungen oder Eigenentwicklungen.
Aus diesen Gründen hatte die 103. Konferenz der DSK beschlossen, eine Task-Force zu gründen, mit den Aufgaben: Abgrenzung des Begriffs „Souveräne Cloud“ von anderen Cloud-Angeboten, Formulierung von Anforderungen an „Souveräne Clouds“, um einen datenschutzrechtlich tragfähigen Betrieb zu ermöglichen und Berücksichtigung von generischen und sektoralen Anforderungen.

Mit einer Stellungnahme der DSK vom 11. Mai 2023 veröffentlichte dann die DSK die Kriterien für „Souveräne Clouds“ als Positionspapier: https://www.datenschutzkonferenz-online.de/media/weitere_dokumente/2023-05-11_DSK-Positionspapier_Kritierien-Souv-Clouds.pdf.
Neben einer ausreichenden Transparenz, Unabhängigkeit von Drittstaatenzugriffen werden dabei auch offene Standards, Open-Source-Software, Schnittstellen und eine ausreichende Transparenz der Datenverarbeitungsvorgänge thematisiert. Ziel ist es, Anbieter von Cloud-Lösungen in die Lage zu versetzen, solche Angebote zu machen, die Kunden wirklich unabhängig werden lässt und auch um Verantwortliche endlich in die Lage zu versetzen, zu verstehen, welche Verarbeitungen in der Cloud tatsächlich stattfinden.

1.8 Cybersicherheitslage

Jährlich wird vom BSI zur Lage der IT-Sicherheit in Deutschland ein Bericht veröffentlicht. Der Bericht für 2023 liegt seit Mitte November 2023 mit Stand 2. November 2023 vor. Verantwortliche von IT-Systemen sollten entsprechend den dort analysierten Risiken ihre eigene IT überprüfen. Auch der 3. Bericht „Branchenlagebild Automotive 2022/2023“ vom BSI gibt einen Überblick über die Cybersicherheitslage in der Automobilindustrie und im Straßenverkehr für den Berichtszeitraum Juli 2022 bis Juni 2023.

Bericht „Die Lage der IT-Sicherheit in Deutschland 2023“
Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist die Cyber-Sicherheitsbehörde des Bundes. Es veröffentlicht jährlich einen umfassenden Bericht zur Lage der IT-Sicherheit in Deutschland. Der Bericht „Die Lage der IT-Sicherheit in Deutschland 2023“ liegt mit Stand 2. November 2023 vor. Im Bericht für das Jahr 2023 kommt das BSI zum Ergebnis: *„Die Bedrohung im Cyberraum ist so hoch wie nie zuvor“*. Nach Angaben des BSI beobachtet es bei Cyberangriffen mit Ransomware zudem eine Verlagerung der Attacken: *„Nicht mehr nur große, zahlungskräftige Unternehmen stehen im Mittelpunkt, sondern zunehmend auch kleine und mittlere Organisationen sowie staatliche Institutionen und Kommunen. Insbesondere von erfolgreichen Cyberangriffen auf Kommunalverwaltungen und kommunale Betriebe sind die Bürgerinnen und Bürger unseres Landes oft auch unmittelbar*

betroffen: So kann es dazu kommen, dass bürgernahe Dienstleistungen eine Zeit lang nicht zur Verfügung stehen oder persönliche Daten in die Hände Krimineller gelangen."
„Daneben rücken Cyberangriffe auf Lieferketten weiter in den Mittelpunkt. Sie können die Cybersicherheit ganzer Branchen gefährden."
Aber, so das BSI, auch die rasante Entwicklung im Bereich der Künstlichen Intelligenz (KI) zeigt, wie schnell technische Neuerungen fortschreiten können. Dies bringt neben großen Chancen für die Digitalisierung auch ein hohes Bedrohungspotenzial mit sich. Das BSI: *„Mit ChatGPT, Bard und LlaMa sowie einer Vielzahl weiterer Tools ist Künstliche Intelligenz in einer breiten, auch wenig technikaffinen Öffentlichkeit angekommen. Diese Tools sind einfach zu bedienen und liefern eine hohe Qualität. Dabei können sie auch für kriminelle Zwecke missbraucht werden. So können sie dafür sorgen, dass sogenannte Deepfakes – manipulierte Bilder, Videos und Stimmen – immer authentischer werden und dadurch immer schwerer zu entlarven sind. Auch kann KI Phishing-Mails glaubwürdiger machen, im Social Web zu Desinformationskampagnen beitragen oder selbst Schadcode generieren – und das wesentlich schneller und zum Teil wesentlich besser als menschliche* Cyberkriminelle*. KI kann auch selbst zur Schwachstelle werden. Sie kann gehackt und missbräuchlich eingesetzt werden. Das stellt das Schwachstellenmanagement in Unternehmen und Behörden vor noch nie dagewesene Herausforderungen."*
Nähere Ausführungen dazu sind im Kapitel „Herausgehobene Trends in der Sicherheit" unter Punkt 10 zu finden.
Den gesamten Bericht „Die Lage der IT-Sicherheit in Deutschland 2023" finden Sie unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.pdf?__blob=publicationFile&v=7#%5B%7B%22num%22%3A292%2C%22gen%22%3A0%7D%2C%7B%22name%22%3A%22FitR%22%7D%2C0%2C595%2C842%5D.

Bericht „Branchenlagebild Automotive 2022/2023"

Seit 2021 gibt das BSI auch einen Bericht „Branchenlagebild Automotive" heraus. Schon im ersten Bericht lieferte hierzu das BSI einen branchenspezifischen Überblick zur Lage der Cyber-Sicherheit, sowohl hinsichtlich der Produktion als auch der Fahrzeuge selbst.
Jetzt liegt der 3. Bericht mit Stand 1. September 2023 vor.
Was hat das mit Datenschutz zu tun? Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) wies

schon in seinem 2. Tätigkeitsbericht 2014/2015 unter Punkt 12.2 darauf hin, dass auch Fahrzeuge, die (partiell) computergesteuert sind, real von Hacker-Angriffen bedroht sind. Schon aus damaliger Sicht des TLfDI können Hacker-Angriffe eines Tages auch irgendwann dazu führen, dass ganz konkret bestimmte Autos manipuliert oder ausspioniert, Daten verfälscht werden oder bewusst beispielsweise das Auto einem Unfall zugeführt wird und so Leib und Leben der Fahrzeuginsassen in Gefahr geraten. Es besteht sogar aufgrund der hochausgereiften Computertechnik irgendwann die Gefahr, dass beispielsweise gleichzeitig hunderte Autos zu einem gleichen Zeitpunkt per Hacker-Angriff manipuliert werden. So lässt sich dann beispielsweise eine ganze Stadt lahmlegen oder bei einem Terroranschlag werden zuvor sämtliche Autos von Hilfs- und Rettungseinheiten destabilisiert (https://tlfdi.de/fileadmin/tlfdi/datenschutz/Wir_ueber_uns/Taetigkeitsberichte_ab_2020/Archiv/2_taetigkeitsbericht.pdf).
Umso mehr sind die entsprechenden Lageberichte des BSI zu diesem Thema von Interesse.
Selbst das BSI schätzt nun durch seine entsprechenden Lageberichte ein, wie wichtig diese Aufgabe ist und dass die Herausforderungen vielfältig und komplex sind. Mit dem vorliegenden „Branchenlagebild Automotive 2022/2023“ wird ein Überblick über die Cybersicherheitslage in der Automobilindustrie und im Straßenverkehr für den Berichtszeitraum Juli 2022 bis Juni 2023 gegeben. Nach Angaben des BSI werden unter anderem die Bereiche Cyber-Kriminalität, IT-Sicherheit der Lieferketten und Produktionsprozesse, Schwachstellen von digitalen Komponenten im Straßenverkehr und neue gesetzliche Regelungen beleuchtet. Auch hier, so das BSI, stellen im Hinblick auf die operative Cyber-Sicherheit in den Betrieben Ransomware-Angriffe aus Sicht des BSI aktuell die größte Bedrohung dar.
Den gesamten Bericht „Branchenlagebild Automotive 2022/2023“ finden Sie unter:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Branchenlagebild/branchenlagebild-automotive-2021_2022.pdf?__blob=publicationFile&v=9.
Der TLfDI bleibt am Thema dran und wird Sie wie immer über den aktuellen Stand informieren.

1.9 AK Schulen und Bildungseinrichtungen und AK Datenschutz-/Medienkompetenz

So viel geballte Datenschutzkompetenz in Sachen Bildung gibt es nur selten: Die Datenschutzkonferenz entsendet die Vertreter ihrer Arbeitskreise „Schulen und Bildungseinrichtungen“ sowie „Datenschutz- und Medienkompetenz“ einmal im Jahr zum TLfDI nach Erfurt. Mit dabei waren 2023 in einer weiteren Sonderkonferenz zeitweise auch Vertreter der Kultusministerkonferenz. Von KI-Anwendungen im Unterricht, dem Einsatz digitaler Schulbücher, einem gemeinsamen Stand auf der Bildungsmesse „didacta“ bis zur Frage, wie Apple Tablets datenschutzkonform in „iPad-Klassen“ eingesetzt werden können – die Bandbreite der Themen und der Gesprächsbedarf waren groß.

Nach zwei „corona-bedingten“ Jahren per Videokonferenz tagten die beiden oben genannten Arbeitskreise erstmals wieder in Präsenz beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) in Erfurt. Vertreter aller Datenschutzaufsichtsbehörden der Länder waren Ende November 2023 angereist oder per Videokonferenz zugeschaltet, um drei Tage intensiv über datenschutzrechtliche Probleme und deren Lösungen im Bildungsbereich zu diskutieren. Herausforderungen gibt es in diesem Bereich reichlich. Bei dem sich rasant entwickelnden Einsatz von Tablets in der Schule, der Anwendung von Künstlicher Intelligenz (KI), deren Einsatz kaum noch nachgewiesen werden, kann und der oft mangelnden Ausbildung der Lehrkräfte im Fach Medienkompetenz sind die Datenschützer ein wichtiges Korrektiv, um auf Gefahren und Missstände aufmerksam zu machen und die Rechte der Betroffenen zu schützen.
Der Arbeitskreis Schulen und Bildungseinrichtungen beschäftigte sich unter anderem mit dem von Schülerinnen und Schülern geliebten Chatbot „ChatGPT“. Während andernorts die pädagogische Frage geklärt werden muss, wie man Haus- und Seminarfacharbeiten noch bewerten kann, wenn der Einsatz dieses Programms bei der Erstellung nicht ausgeschlossen werden kann, beschäftigt die Datenschützer vor allen Dingen, wie sichergestellt werden kann, dass das System nicht mit den personenbezogenen Daten der Schülerinnen und Schüler lernt und arbeitet. Eine Reihe von Fragen wurde daher bereits im Vorfeld der AK-Sitzung erarbeitet und an OpenAI, das US-amerikanische Unternehmen, welches ChatGPT entwickelt hat und betreibt, gesendet.

Die Antworten des US-amerikanischen Softwareunternehmens reichten den deutschen Datenschutzaufsichtsbehörden jedoch noch nicht aus, sodass in der Sitzung entschieden wurde, weitere, detaillierte Auskünfte von OpenAI einzuholen. Die Nutzung von ChatGPT im Unterricht oder zu schulischen Zwecken zu verbieten, ist dabei nicht das Anliegen der Datenschützer, vielmehr soll ermöglicht werden, ein Anmeldeverfahren und eine Anwendung zu etablieren, die keine Rückschlüsse auf die personenbezogenen Daten der Schülerinnen und Schüler erlauben.
Ebenso wurden die Antworten des Apple-Konzerns ausgewertet, dessen Tablets mittlerweile bereits unter dem Begriff „iPad-Klasse“ an zahlreichen Schulen zum Einsatz kommen. Die Geräte, die überwiegend durch die Eltern privat angeschafft werden, müssen mit einer sogenannten Mobile Device Management-Software die schulische von der privaten Nutzung trennen können. Auch hier ergaben sich zahlreiche weitere Nachfragen aus den ersten Antworten des Apple-Konzerns auf den Fragenkatalog des Arbeitskreises Schule und Bildungseinrichtungen. Dieses Thema wird den AK voraussichtlich noch länger beschäftigen.
Die von der Kultusministerkonferenz (KMK) geplante Einführung eines Bildungsverlaufsregisters wurde ebenfalls diskutiert. Bereits jetzt führen einige Länder Statistiken; außerdem werden Bildungsverläufe in zahlreichen, groß angelegten und über die Ländergrenzen hinwegreichenden wissenschaftlichen Studien untersucht, ausgewertet und der Politik die Ergebnisse zur gesetzgeberischen Steuerung zur Verfügung gestellt. Welchen zusätzlichen Nutzen ein bundesweit einheitliches Bildungsverlaufsregister für die in Länderhoheit liegende Bildungspolitik haben soll, ist neben zahlreichen weiteren offenen Fragen, zum Beispiel zur Verschlüsselung, Anonymisierung und Speicherung, der wichtigste Punkt, den die Datenschützer an die KMK herantragen werden.
Gemeinsam mit Vertretern der KMK wurde im Rahmen der AG Datenschutz der KMK und der Datenschutzkonferenz in zwei Unterarbeitsgruppen nach Lösungen gesucht, wie im schulischen Bereich der Einsatz von schülereigenen Geräten („bring your own device“, BYOD), datenschutzgerecht erfolgen kann. Grundsätzlich ist es so, dass zwar viele Schulen aufgrund der Anschaffungen mit Mitteln aus dem Digitalpakt bereits über Klassensätze an schulischen Endgeräten verfügen, aber hier das Problem besteht, dass diese grundsätzlich in der Schule verbleiben. Deswegen soll es ebenfalls möglich sein, dass

Schüler eigenfinanzierte Geräte, die den Vorgaben der Schule entsprechen, selbst anschaffen und dann zu schulischen Zwecken nutzen. Selbstverständlich stehen diese Geräte aber auch der privaten Nutzung der Schüler zur Verfügung. Die Trennung der Nutzungen wird durch ein auf dem Gerät installiertes Mobile Device Management gewährleistet. Diese Problemstellung des BYOD besteht in allen Bundesländern gleichermaßen und so auch in Thüringen. Hier ist jedoch die Schule beziehungsweise die Schulleitung verantwortlich für die Verarbeitung der personenbezogenen Daten der Schülerschaft, dies gilt dann nicht nur beim Einsatz verschiedener Software-Produkte, Apps und Internetseiten, sondern auch bei der Frage der Betriebssysteme und Provider. Diese umfangreiche Problematik wurde daher zusätzlich in eine zweite Unterarbeitsgruppe verwiesen, in der Best-Practice-Beispiele beim Einsatz von Software und Lernanwendungen im schulischen Bereich dargestellt und so aufbereitet werden sollen, dass die Schulen diese unmittelbar anwenden können.
Der Arbeitskreis Datenschutz-/Medienkompetenz beschäftigte sich folgerichtig dann auch mit der Frage der Vermittlung von Medienkunde in den Schulen. Wenngleich die Datenschutzaufsichtsbehörden umfangreiche Fort- und Weiterbildungsangebote für Lehrkräfte im Portfolio haben, fehlt es in vielen Ländern bereits in den Hochschulen an einem entsprechenden Angebot, die angehenden Pädagogen auf ihre Aufgaben in diesem Bereich ausreichend vorzubereiten. Das, was in vielen Ländern in den Lehrplänen an medienkundlichem Unterricht vermittelt werden soll, findet im Schulalltag noch nicht überall in ausreichendem Maße statt. Während einige Länder mittlerweile eigene Fächer dafür eingeführt haben oder dies in Planung ist, sind in anderen Ländern lediglich wenige Zusatz- oder Klassenleiterstunden dafür vorgesehen – ein Umfang, der der Bedeutung von Kompetenz im Umgang mit digitalen Medien in der heutigen Zeit nicht gerecht wird. Hier werden sich die Datenschutzaufsichtsbehörden weiter mit der Politik ins Benehmen setzen, um für flächendeckende Aufklärung und Ausbildung von Schülerschaft und Lehrkörper für die mediale Informationsgesellschaft zu werben. So wird es auf Initiative des TLfDI künftig möglich sein, dass Lehramtsstudierende der Friedrich-Schiller-Universität Jena Credit-Points für ihr Examen erwerben können, wenn sie entsprechende Rechtsvorlesungen des TLfDI belegen. Die Möglichkeit der Anrechnung der Credit-Points für diese juristischen Vorlesungen war bis dato den Jura-Studierenden vorbehalten.

Ein weiterer Baustein, um für einen sorgfältigen Umgang mit dem Recht auf informationelle Selbstbestimmung zu werben, wird ein Gemeinschaftsstand der Datenschützer aus Thüringen, Berlin, Baden-Württemberg und Hessen auf der Bildungsmesse didacta im Februar 2024 sein. Hier sollen insbesondere Lehrkräfte die Gelegenheit haben, im direkten Gespräch ihren zum Teil nachvollziehbaren Frust über die datenschutzrechtlichen Einschränkungen bei der Nutzung bestimmter digitaler Anwendungen loszuwerden und sich die rechtlichen Hintergründe erklären und Alternativen aufzeigen zu lassen. Außerdem wird dies ein weiterer Anlass sein, für das Jugendportal www.youngdata.de zu werben. Die von den Mitgliedern der Datenschutzkonferenz gemeinsam betriebene Internetseite ist seit Herbst 2023 inhaltlich und gestalterisch an die Informationsbedürfnisse junger Menschen angepasst und liefert verständlich und unterhaltsam alles Wichtige, was man als Jugendlicher im Umgang mit sozialen Netzwerken, Foto- und Drohnenaufnahmen, Cybermobbing, Künstlicher Intelligenz und vielem anderen wissen muss.
Die drei eng bestückten Konferenztage haben den Teilnehmern nicht nur viele Informationen und einen länderübergreifenden kollegialen Austausch ermöglicht, sondern auch Anregungen gegeben und Vereinbarungen zu neuen Projekten geschaffen.

1.10 Handreichung zur „Digitalen Selbstverteidigung“

Der TLfDI hat seine „Handreichung zur digitalen Selbstverteidigung“ Anfang 2023 aktualisiert und um die Tipps zur smarten Haustechnik ergänzt. Nunmehr liegt also die 8. Auflage vor.

Die seit Jahren veröffentlichte Broschüre „Handreichung zur digitalen Selbstverteidigung“ des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) richtet sich insbesondere an Kinder, Jugendliche, Erwachsene, Eltern und Senioren und erfährt weiterhin großes Interesse.
Der TLfDI nahm dies deshalb erneut zum Anlass, die Broschüre zu überarbeiten und zu aktualisieren, die 8. Auflage liegt seit Anfang 2023 vor. Die Broschüre weist wie immer nach kurzen Hinweisen auf die aktuelle Gefahrenlage bei der Nutzung digitaler Medien hin. Sie werden mit Hinweisen versorgt, wie Sie Ihren digitalen Schutz erhöhen können. Mit weiterführenden Links können Sie sich tiefgreifender informieren.

Bei der Veröffentlichung der 8. Auflage, mahnte der TLfDI in seiner Pressemitteilung am 6. Februar 2023 nochmals eindringlich: „Minimieren Sie Ihre Daten im Netz – Ihre Daten werden genutzt, um Profile über Sie zu erstellen, ohne dass Sie es wissen. Und diese Profile werden wiederum genutzt, um Feststellungen oder Prognosen über Sie zu treffen. Diese müssen nicht stimmen, werden aber gleichwohl verwendet. Von wem und zu welchem Zweck – unbekannt!“
Die aktuelle 8. Auflage der „Handreichung zur digitalen Selbstverteidigung“ des TLfDI ist abrufbar unter:
https://tlfdi.de/fileadmin/tlfdi/datenschutz/Wir_ueber_uns/Infomaterial/Digitale_Selbstverteidigung_8.Auflage.pdf

1.11 Digitalisierung im Gesundheitswesen

Im Berichtsjahr wurden zwei Gesetze beschlossen, die wichtige Regelungen für die Digitalisierung im Gesundheitswesen enthalten: das Digital-Gesetz und das Gesundheitsdatennutzungsgesetz. Die Digitalisierung bringt viele Vorteile mit sich, enthält aber aus datenschutzrechtlicher Sicht durchaus einige Fallstricke.

Die Digitalisierung erhält in viele Bereiche des gesellschaftlichen Lebens immer mehr Einzug. Im Bereich der Gesundheitsversorgung verspricht sie schnellere Kommunikation und effizientere Verwaltungsabläufe als Voraussetzung für eine gute und wirksame Behandlung. Außerdem soll sie die systematische Auswertung von medizinischen Daten, die Erkennung von Krankheiten und individuell ausgerichtete Therapien ermöglichen. Mobile Anwendungen versprechen, die Behandlungsabläufe zu optimieren. Der deutsche Gesetzgeber hat im Berichtszeitraum mit zwei Gesetzgebungsvorhaben die Digitalisierung im Gesundheitswesen neu geregelt.

1. Digital-Gesetz

Der Deutsche Bundestag hat am 14. Dezember 2023 das „Gesetz zur Beschleunigung der Digitalisierung des Gesundheitswesens“ (Digital-Gesetz – DigiG) beschlossen. Ziel des Gesetzes ist, mit digitalen Lösungen wie der elektronischen Patientenakte und dem elektronischen Rezept (E-Rezept) als verbindlichem Standard den Versorgungsalltag in Deutschland zu verbessern. Die elektronische Patientenakte wird Anfang des Jahres 2025 für alle gesetzlich Versicherten eingerichtet werden und soll den Austausch und die Nutzung von Gesundheitsda-

ten vorantreiben und die Versorgung von Patienten gezielt unterstützen. Wer sie nicht nutzen möchte, kann dem widersprechen (Opt-Out). Privaten Krankenversicherungen wird die Möglichkeit eröffnet, elektronische Patientenakten zu führen, die gesetzlichen Regelungen sind in diesem Fall entsprechend anzuwenden. Die elektronische Patientenakte enthält eine vollständige, weitestgehend automatisch erstellte, digitale Medikationsübersicht. Digitale Gesundheitsanwendungen werden in die Versorgungsprozesse integriert und ihr Einsatz soll transparent gemacht werden. Ein Digitalbeirat der unter anderem mit Vertretern des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) und des Bundesamts für Sicherheit in der Informationstechnik (BSI) besetzt wird, soll künftig die gematik laufend bei all ihren Festlegungen mit ausgewogenen Empfehlungen zu Fragen des Datenschutzes, der Datensicherheit, der Datennutzung und der Anwenderfreundlichkeit beraten. Die gematik wurde von den Spitzenorganisationen des deutschen Gesundheitswesens gegründet, um gemäß dem gesetzlichen Auftrag die Einführung, Pflege und Weiterentwicklung der elektronischen Gesundheitskarte und ihrer Infrastruktur in Deutschland voranzutreiben und zu koordinieren.

Der BfDI hat den Gesetzentwurf kritisiert (https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Stellungnahmen/2023/StgN_Beschleunigung-DigiG-Kurzversion.pdf?__blob=publicationFile&v=4). Er warnte davor, dass ein umfassender zusätzlicher Bestand an Daten die Informationen über den Gesundheitszustand einer Person in bisher nicht gekanntem Ausmaß erschließt und mit voranschreitendem Ausbau der elektronischen Patientenakte die Erstellung eines nahezu vollständigen Gesundheitsprofils ermöglicht. Er forderte, die Befüllungsbefugnis der Leistungserbringer konkreter zu regeln. Seine in einer Formulierungshilfe gemachten Vorschläge wurden nur zum Teil aufgegriffen.

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) wird im Rahmen seiner Aufgabenwahrnehmung darauf achten, dass in der Praxis eine eindeutige Zuordnung der elektronischen Patientenakte zu den Versicherten sichergestellt wird und es keine doppelten Bereitstellungen gibt. Auch die konsequente Beachtung von Widersprüchen gilt es zu kontrollieren.

2. Gesundheitsdatennutzungsgesetz

Ebenfalls am 14. Dezember 2023 hat der Deutsche Bundestag das „Gesetz zur verbesserten Nutzung von Gesundheitsdaten“ (Gesund-

heitsdatennutzungsgesetz – GDNG) beschlossen. Mit dem GDNG sollen künftig Gesundheitsdaten für Forschung und Entwicklung besser erschlossen werden und damit zu einer besseren Versorgung beitragen. Kern des Gesetzes ist die erleichterte Nutzbarkeit von Gesundheitsdaten für gemeinwohlorientierte Zwecke. Dazu wird unter anderem eine dezentrale Gesundheitsdateninfrastruktur mit einer zentralen Datenzugangs- und Koordinierungsstelle für die Nutzung von Gesundheitsdaten aufgebaut. Die Datenhaltung soll weiterhin dezentral erfolgen, indem die Daten am bisherigen Ort gespeichert bleiben und lediglich spezifisch für den jeweiligen Forschungsantrag in einer sicheren Verarbeitungsumgebung zugänglich gemacht werden sollen.
Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK), der auch der TLfDI angehört, nahm am 14. August 2023 zu dem Gesetzentwurf Stellung (https://www.datenschutzkonferenz-online.de/media/st/23_08_14_DSK_Stellungnahme_GDNG-E.pdf). Aus ihrer Sicht war der Referentenentwurf aus datenschutzrechtlicher Sicht an einigen Stellen dringend anzupassen. Soweit die Verknüpfung von pseudonymisierten Daten des Forschungsdatenzentrums Gesundheit nach § 303d des Fünften Buches Sozialgesetzbuch mit pseudonymisierten Daten der klinischen Krebsregister der Länder nach § 65c des Fünften Buches Sozialgesetzbuch zugelassen werden sollte, müssten bereits im Gesetz angemessene Maßnahmen zum Schutz der Rechte und Freiheiten der betroffenen Personen im Sinne des Art. 89 Abs. 1 Datenschutz-Grundverordnung (DS-GVO) getroffen werden. Der Gesetzentwurf wurde daraufhin angepasst. Ob die vorgesehenen Maßnahmen ausreichend sind, wird sich in der Praxis zeigen.
Der Referentenentwurf des Bundesministeriums für Gesundheit zum Gesetz sah vor, dass dem BfDI alleine die Aufsicht über Stellen übertragen wird, soweit sie Sozialdaten im Sinne des § 67 Zehntes Buch Sozialgesetzbuch verarbeiten, die unter die Definition der Gesundheitsdaten gemäß Art. 4 Nr. 15 DS-GVO fallen. In diesem Bereich ist nun, wie bisher, die jeweilige Landesdatenschutzaufsichtsbehörde zuständig. Die federführende Datenschutzaufsicht für länderübergreifende Forschungsvorhaben wird auf alle Gesundheitsdaten ausgeweitet. Die datenschutzrechtliche Aufsicht für länderübergreifende Forschungsvorhaben im Gesundheitswesen wird durch eine/n Landesdatenschutzbeauftragte/n koordiniert.
In Bezug auf die Eigenforschung von Leistungserbringern wurde eine klare Definition des Anwendungsbereichs, sowie eine Klarstellung

gefordert, dass betroffene Personen nach Art. 13 Abs. 1 Buchstabe c) DS-GVO über die Zwecke der Verarbeitung zu informieren sind. Diese Klarstellung erfolgte leider nicht explizit.
Die Kranken- und Pflegekassen sollten datengestützte Auswertungen zum individuellen Gesundheitsschutz ihrer Versicherten, zur Verbesserung der Versorgung und zur Verbesserung der Patientensicherheit vornehmen und insoweit ihre Versicherten individuell ansprechen und Auswertungen ohne Einwilligung vornehmen dürfen. Dieses Risiko des „gläsernen Versicherten“ war noch mit hohen Beeinflussungs- und Diskriminierungsrisiken verbunden und in der im Entwurf enthaltenen Form datenschutzrechtlich unzulässig. Die entsprechende Regelung wurde aus datenschutzrechtlicher Sicht marginal überarbeitet.
Es wurde, wie von der DSK gefordert, klargestellt, dass für die Datenverarbeitungen beim Forschungsdatenzentrum Gesundheit das Sozialgeheimnis gilt.
Durch das Gesetz wird ein Forschungsgeheimnis bei der Nutzung von Gesundheitsdaten eingeführt. Das bedeutet, dass Forschende Gesundheitsdaten nur wie gesetzlich gestattet nutzen und weitergeben dürfen und die Daten geheim zu halten haben. Bei Verletzung dieser Geheimhaltungspflichten gilt künftig eine Strafnorm.
Das kritisierte Opt-Out-Verfahren für die Datenfreigabe aus der elektronischen Patientenakte wurde beibehalten. Diese undifferenzierte grundsätzliche Freigabe für alle nach § 303e Abs. 2 des Sozialgesetzbuches Fünftes Buch (Entwurf) denkbaren Nutzungszwecke nimmt nicht angemessen auf den Schutzbedarf der betroffenen personenbezogenen Daten Rücksicht. Eine derartige Weiterleitung der Daten ist nach Auffassung der Datenschutzaufsichtsbehörden nur zu Zwecken der wissenschaftlichen Forschung im Gemeinwohlinteresse zulässig.
Für den TLfDI ist erfreulich, dass es bei seiner Zuständigkeit als Datenschutzaufsichtsbehörde für die Verarbeitung von Sozialdaten bleibt, die sich in der Vergangenheit bewährt hat.

1.12 Mögliche Interessenkonflikte eines behördlichen Datenschutzbeauftragten

Ein behördlicher Datenschutzbeauftragter darf neben seiner Tätigkeit in dieser Funktion innerhalb der öffentlichen Stelle auch andere Aufgaben und Pflichten wahrnehmen. Hierbei darf es aber zu keinem Konflikt mit dem Amt als behördlichem Datenschutzbeauftragten kommen, da nach Art. 38 Abs. 6 Satz 2 DS-GVO in Verbindung mit

§ 14 Abs. 7 Satz 2 ThürDSG durch die öffentliche Stelle sichergestellt werden muss, dass ein Interessenkonflikt durch andere Aufgaben und Pflichten nicht entsteht. Ein solcher Interessenkonflikt ist etwa für den Fall anzunehmen, dass ein behördlicher Datenschutzbeauftragter gleichzeitig die Funktion eines Geheimschutzbeauftragten innerhalb der öffentlichen Stelle wahrnehmen soll.

Öffentliche Stellen in Thüringen müssen verpflichtend einen Datenschutzbeauftragten bestellen, was sich aus Art. 37 Abs. 1 Buchstabe a) Datenschutz-Grundverordnung (DS-GVO) in Verbindung mit § 13 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) ergibt. Grundsätzlich gestattet Art. 38 Abs. 6 Satz 1 DS-GVO in Verbindung mit § 14 Abs. 7 Satz 1 ThürDSG, dass ein Datenschutzbeauftragter einer öffentlichen Stelle noch „andere Aufgaben und Pflichten“ übernehmen darf, beziehungsweise dass diesem durch den Verantwortlichen noch weitere Aufgaben übertragen werden dürfen, soweit dies nicht zu einem Interessenkonflikt führt. Die Vermeidung von Interessenkonflikten ist dabei eine rechtliche Organisationspflicht des Verantwortlichen beziehungsweise des Auftragsverarbeiters (Baumgartner/Hansch: Der betriebliche Datenschutzbeauftragte, ZD 2019, 102). Den Verantwortlichen beziehungsweise Auftragsverarbeiter trifft damit die Rechtspflicht, Interessenkonflikte des/der bei ihm bestellen Datenschutzbeauftragten zu vermeiden.
Aus der Praxis ist dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) indes bekannt, dass es bei den öffentlichen Stellen im Freistaat bei der Übertragung von anderen Aufgaben und Pflichten auf die Datenschutzbeauftragten regelmäßig zu Unsicherheiten dahingehend kommt, ob die zusätzlichen Aufgaben und Pflichten in Bezug auf die Funktion des/der Datenschutzbeauftragten zu einem Interessenkonflikt führen. So erreichte den TLfDI im Berichtszeitraum zu dieser Thematik unter anderem die Anfrage eines behördlichen Datenschutzbeauftragten, dem innerhalb einer Stadtverwaltung die Position eines Geheimschutzbeauftragten übertragen werden sollte. In Anbetracht eines möglichen Interessenkonflikts bei dieser zusätzlichen Aufgabenübertragung, der die Wahrnehmung der beiden Funktionen in Personalunion nach datenschutzrechtlichen Bestimmungen ausschließen würde, wurde der TLfDI um eine entsprechende Bewertung hierzu gebeten.
Aus Sicht des anfragenden Datenschutzbeauftragen wäre die Übernahme der Rolle des Geheimschutzbeauftragten zulässig gewesen.

Der TLfDI musste dem Datenschutzbeauftragten nach Prüfung der Anfrage jedoch mitteilen, dass bei der Übertragung der Aufgaben eines Geheimschutzbeauftragten auf den behördlichen Datenschutzbeauftragten eine Inkompatibilität der beiden Aufgabenkomplexe und somit ein Interessenkonflikt, mithin eine Unvereinbarkeit im Sinne von Art. 38 Abs. 6 Satz 2 DS-GVO in Verbindung mit § 14 Abs. 7 Satz 2 ThürDSG vorliegt.
Innerhalb einer öffentlichen Stelle gibt es diverse Funktionen, für die grundsätzlich Unvereinbarkeiten mit der Funktion des Datenschutzbeauftragten bestehen. Hierzu zählt auch die Funktion eines Geheimschutzbeauftragten.
Beispielhaft für einen möglichen Interessenkonflikt bei der Übertragung von anderen Aufgaben und Pflichten auf den (behördlichen) Datenschutzbeauftragten soll daher im Folgenden erläutert werden, weshalb eine personelle Trennung der Funktionen „behördlicher Datenschutzbeauftragter“ und „Geheimschutzbeauftragter“ zwingend geboten ist.
Durch die DS-GVO wie auch das ThürDSG werden keine Aussagen dazu getroffen, in welchen konkreten Fällen eine Interessenkollision bei der Übertragung zusätzlicher Aufgaben auf den Datenschutzbeauftragten vorliegt. Art. 38 Abs. 6 DS-GVO und § 14 Abs. 7 ThürDSG ist aber zu entnehmen, dass sich Interessenkonflikte durch die Aufgaben und Pflichten eines Datenschutzbeauftragten ergeben können, sodass für die Prüfung eines möglichen Interessenkonflikts durch Aufgabenübertragung grundsätzlich an die gesetzlich normierten Aufgaben des Datenschutzbeauftragten (Art. 39 DS-GVO in Verbindung mit § 15 ThürDSG) anzuknüpfen ist. Ein Interessenkonflikt nach den datenschutzrechtlichen Bestimmungen liegt insbesondere dann vor, wenn ein (behördlicher) Datenschutzbeauftragter durch anderweitige Aufgaben und Pflichten, die er zusätzlich erfüllen soll, in seiner Aufgabenwahrnehmung nach Art. 39 DS-GVO in Verbindung mit § 15 ThürDSG derart eingeschränkt wäre, dass keine objektive Aufgabenwahrnehmung mehr vorliegt, er mithin die eigenständig vorgenommenen oder veranlassten Datenverarbeitungstätigkeiten selbst kontrollieren müsste. Maßgeblich für die Beurteilung, ob eine Interessenskollision vorliegt, wenn ein Datenschutzbeauftragter einer öffentlichen Stelle zusätzlich die Aufgaben eines Geheimschutzbeauftragten wahrnehmen würde, ist daher die grundsätzlich notwendige Einzelfallbetrachtung dahingehend, in welchem Umfang der Datenschutzbe-

auftragte in seiner Funktion als Geheimschutzbeauftragter personenbezogene Daten verarbeiten würde, ob und in welchem Maße ihm nach der Aufgabenübertragung Entscheidungsbefugnisse über Zweck und Mittel der Verarbeitung personenbezogener Daten im Rahmen der Tätigkeit als Geheimschutzbeauftragter obliegen würden. Die Aufgaben, die ein Geheimschutzbeauftragter im Bereich des personellen und materiellen Geheimschutzes übernimmt, sind vielfältig. Unter anderem obliegt einem Geheimschutzbeauftragten als personelle Maßnahme die Auswahl des zu Geheimnissen zugangsberechtigten Personenkreises durch sogenannte Sicherheitsüberprüfungen. Somit ist die Tätigkeit eines Geheimschutzbeauftragten verbunden mit der Durchführung von umfassenden, auch sensitive personenbezogene Daten betreffenden, teils stark risikobehafteten Verarbeitungsvorgängen mit entsprechenden Entscheidungskompetenzen im Hinblick auf die Verarbeitung personenbezogener Daten aufgrund der Sonderstellung in der Behördenorganisation. Insoweit ist hier die innerbehördliche Kontrolle durch den Datenschutzbeauftragten dringend geboten.
Wenn die Funktionen des behördlichen Datenschutzbeauftragten sowie des Geheimschutzbeauftragten in Personalunion wahrgenommen werden würden, wäre eine erhebliche Spannungslage mit Interessendivergenzen aufgrund von Rollenkonflikten zwischen den beiden Funktionen grundsätzlich nicht vermeidbar. Denn dem behördlichen Datenschutzbeauftragten obliegt unter anderem die Kontrolle der Einhaltung der datenschutzrechtlichen Bestimmungen innerhalb der öffentlichen Stelle. Würde der Datenschutzbeauftragte nun zusätzlich die Funktion eines Geheimschutzbeauftragten ausfüllen, müsste er sich bei dieser Arbeit, die in nicht unerheblicher Weise mit der Verarbeitung personenbezogener Daten verbunden ist, durch seine Funktion als behördlicher Datenschutzbeauftragter faktisch selbst kontrollieren. Eine effektive Kontrolle mit der notwendigen Distanz gegenüber der zu kontrollierenden Stelle wäre dabei aufgrund der Rollenvermischung – auch wenn die Rollen funktional getrennt sind – nicht gegeben; der Datenschutzbeauftragte wäre einer Interessenkollision ausgesetzt. Eine Unvereinbarkeit der Position des Geheimschutzbeauftragten mit der Funktion des behördlichen Datenschutzbeauftragten wird auch von anderen Datenschutz-Aufsichtsbehörden festgestellt (siehe etwa LfDI Baden-Württemberg: 34. Datenschutz-Tätigkeitsbericht des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg 2018, abrufbar unter:

https://www.zaftda.de/tb-bundeslaender/baden-wuerttemberg/landesdatenschutzbeauftragter/691-34-tb-lfd-baden-wuerttemberg-2018-16-5000-vom-04-02-2019/file, S. 29).
Die diesbezügliche Bewertung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit lässt sich der Broschüre „Die Datenschutzbeauftragten in Behörden und Betrieben“ (abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Broschueren/INFO4.pdf?__blob=publicationFile&v=15, S. 14) entnehmen. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit weist hier zutreffend darauf hin, dass auch für die Position eines Geheimschutzbeauftragten gilt, Interessenkonflikte bei der Aufgabenwahrnehmung zu vermeiden (für die Bundesebene verbietet gar § 3 Abs. 1a Sicherheitsüberprüfungsgesetz, dass Aufgaben des personellen Geheimschutzes von behördlichen Datenschutzbeauftragten wahrgenommen werden).
Auch in der Literatur wird davon ausgegangen, dass die Wahrnehmung von Aufgaben im Datenschutz und in Geheimschutzfragen in Personalunion unzulässig sind (so etwa Franck: Behördliche Datenschutzbeauftragte und personeller Geheimschutz nach dem Sicherheitsüberprüfungsgesetz, NVwZ 2021, 430 ff.; Gola: Spezifika bei der Benennung behördlicher Datenschutzbeauftragter, ZD 2019, 389; Bergt in: Kühling/Buchner, DS-GVO/BDSG, 3. Auflage 2020, DS-GVO Art. 38 Rn. 42).
Es ist grundsätzlich zu beachten, dass vor einer Übertragung von zusätzlichen Aufgaben auf (behördliche) Datenschutzbeauftragte durch den Verantwortlichen oder Auftragsverarbeiter stets im Einzelfall zu prüfen ist, ob hierdurch ein Interessenkonflikt entstehen würde. Wie bereits angeführt, gibt es innerhalb der Organisationsstruktur öffentlicher Stellen aber verschiedene Positionen, die aufgrund von Interessenkonflikten in der Regel beziehungsweise grundsätzlich nicht mit Datenschutzbeauftragten besetzt werden dürfen. Neben der Funktion des Geheimschutzbeauftragten, die aus erläuterten Gründen nicht durch den Datenschutzbeauftragten wahrgenommen werden darf, betrifft dies etwa die Leitungsebene einer öffentlichen Stelle, entscheidungsbefugte Positionen im Bereich der IT und auch Leitungsfunktionen im Personalbereich. Ein Datenschutzbeauftragter einer öffentlichen Stelle darf zudem nicht zugleich Geldwäschebeauftragter oder IT-Sicherheitsbeauftragter sein.

Öffentliche Stellen in Thüringen dürfen bei der Übertragung von Aufgaben und Pflichten auf ihre Datenschutzbeauftragten indes nicht unberücksichtigt lassen, dass nicht nur die Entstehung von Interessekonflikten auszuschließen ist. Es muss bei der Übertragung von anderen Aufgaben und Pflichten vielmehr auch sichergestellt werden, dass dem/der Datenschutzbeauftragten hinreichend Arbeitszeit verbleibt, um seine/ihre Aufgaben erfüllen zu können. Dies ergibt sich als Pflicht für die öffentlichen Stellen aus § 14 Abs. 7 Satz 2 ThürDSG.

1.13 Hinweise zur Videoüberwachung im Nachbarschaftsbereich

Eine Videoüberwachung durch private Personen unterliegt regelmäßig den Vorgaben der DS-GVO. Ob eine Videoüberwachung im Nachbarschaftsbereich den datenschutzrechtlichen Vorgaben entspricht, kann mit der hier beschriebenen Checkliste geprüft werden.

Den Thüringer Landesbeauftragen für den Datenschutz und die Informationsfreiheit (TLfDI) erreichen eine Vielzahl von Anfragen und Beschwerden von Bürgern zur Videoüberwachung durch private Personen. Bei der Prüfung dieser Fälle zeigt sich, dass sich viele Betreiber von Videoüberwachungsanlagen der umfassenden datenschutzrechtlichen Dimension ihres Vorhabens nicht bewusst sind. Ein einfaches Kamerasystem ist bereits für wenig Geld zu erwerben und kann mit geringem Aufwand installiert werden. Dies darf jedoch nicht darüber hinwegtäuschen, dass mit einer Videoüberwachung oftmals eine Verarbeitung von personenbezogenen Daten betroffener Personen einhergeht. Werden dabei nicht nur der Verantwortliche selbst und seine engsten Familienangehörigen erfasst, so greift der Anwendungsbereich der Datenschutz-Grundverordnung (DS-GVO). Der Betreiber der Videokamera tritt dabei als sogenannter Verantwortlicher auf und ist für die Datenverarbeitung nach Art. 5 Abs. 2 DS-GVO rechenschaftspflichtig. Er muss also die Einhaltung der datenschutzrechtlichen Vorgaben nachweisen können. Die Datenschutzkonferenz (DSK) hat hierzu eine im Internet frei zugängliche „Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen“ (abrufbar unter: https://www.datenschutzkonferenz-online.de/media/oh/20200903_oh_v%C3%BC_dsk.pdf), sowie das Kurzpapier Nr. 15 „Videoüberwachung nach der Datenschutz-Grundverordnung“ (abrufbar unter: https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_15.pdf) bereitgestellt.

Im Folgenden möchte der TLfDI die wichtigsten Punkte herausarbeiten, um insbesondere den Verantwortlichen eine Checkliste zum datenschutzkonformen Betrieb ihrer Videoüberwachung an die Hand zu geben. Diese Liste hat keinen Anspruch auf Vollständigkeit und dient dazu, einen Überblick zu häufigen Problemfeldern der privaten Videoüberwachung im Nachbarschaftsbereich zu geben. Sind alle Punkte erfüllt, führt dies nicht automatisch zur Zulässigkeit der Videoüberwachung. Haben Sie zu dem Betrieb einer Videoüberwachungsanlage konkrete Fragen, können Sie sich gerne an den TLfDI wenden.

Die Vorschriften der DS-GVO müssen eingehalten werden,

- □ wenn Dritte (Art. 4 Nr. 10 DS-GVO) auf den Aufnahmen in irgendeiner Weise zu identifizieren sind, und
- □ wenn öffentlich zugängliche Bereiche oder Bereiche außerhalb des eigenen Grundstücks überwacht werden.
- □ Dies gilt auch bei Live-Überwachung ohne Speicherung der Aufnahmen.

Ist die DS-GVO nicht anwendbar, müssen ihre Vorgaben für die Videoüberwachung nicht eingehalten werden. Der TLfDI ist in diesen Fällen nicht weiter zuständig.

Rechtmäßigkeit der Überwachung – Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO

Findet die DS-GVO Anwendung, so hat der Verantwortliche für die von ihm betriebene Videoüberwachung die Grundsätze der Datenverarbeitung gemäß Art. 5 Abs. 1 DS-GVO einzuhalten. Auch wenn auf Hinweisschildern immer wieder ein Verweis auf § 4 Abs. 1 Bundesdatenschutzgesetz als Rechtsgrundlage für eine Videoüberwachung zu finden ist, hat das Bundesverwaltungsgericht in seinem Urteil vom 27. März 2019 (BVerwG 6 C 2.18) entschieden, dass diese Norm als europarechtswidrig nicht anwendbar ist. Die private Videoüberwachung unterliegt demnach ausschließlich den gesetzlichen Vorgaben der DS-GVO. Da eine Einwilligung aller potentiell von der Videoüberwachung betroffenen Personen in der Regel ausscheidet, ist die Zulässigkeit der Datenverarbeitung nach Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO zu prüfen. Diese Norm verlangt Folgendes:

- □ Die Überwachung dient der Wahrung der berechtigten Interessen des Verantwortlichen (zum Beispiel der Wahrung des Hausrechts).

- □ Die Überwachung ist für das Erreichen dieses Zwecks erforderlich, das heißt es ist kein milderes Mittel möglich um den Zweck zu erreichen.
- □ Die Interessen des Verantwortlichen an der Videoüberwachung überwiegen die Interessen oder Grundrechte der von der Überwachung betroffenen Personen.

Die Interessen sind immer anhand des konkreten Einzelfalles abzuwägen. Ob die Interessen der Betroffenen im Einzelfall schutzwürdiger sind, entscheidet die Intensität des Eingriffs. Diese bestimmt sich unter anderem anhand des betroffenen Personenkreises, der Art und des Umfangs der erfassten Informationen und der Art und Weise der Datenverarbeitung. In diesem Zusammenhang sind folgende Punkte zu beachten:

- □ Es wird ausschließlich das eigene Grundstück und/oder der Zugangsbereich zum eigenen Haus/zur eigenen Wohnung bis zur Grundstücksgrenze überwacht.
- □ Es werden keine Tonaufnahmen angefertigt.
- □ Allein der Verantwortliche hat Zugriff auf die Aufnahmen.
- □ Die Aufnahmen werden maximal 72 Stunden gespeichert.
- □ Nach Möglichkeit sollten die Aufnahmen nicht in einer Cloud gespeichert oder über eine App aufgerufen werden.

Sonderfall Tür- und Klingelkameras

Wenn eine Tür- und Klingelkamera den öffentlichen Raum erfasst, muss durch technische Maßnahmen sichergestellt werden, dass eine Bildübertragung erst nach Betätigung der Klingel erfolgt, die Übertragung nach einigen Sekunden automatisch wieder endet, räumlich nicht mehr abgebildet wird als ein Blick durch einen Türspion gewähren würde, und dass die Aufnahmen nicht dauerhaft gespeichert werden.

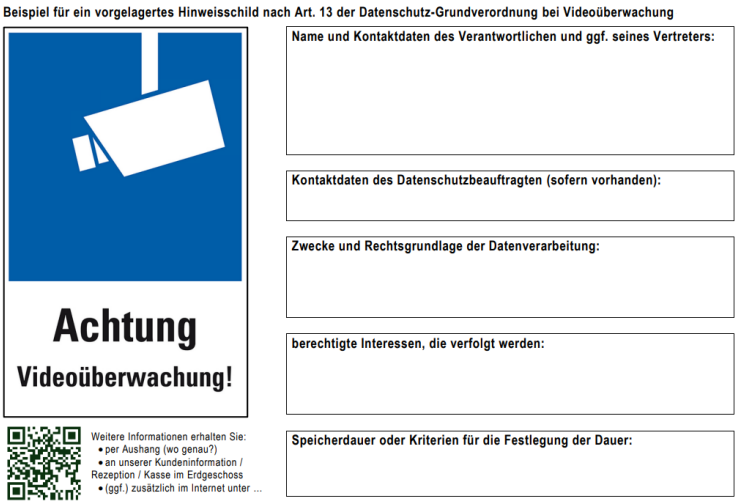
Sonderfall Drohnen

Der Einsatz von Drohnen mit Videokameras durch Privatpersonen in städtischen Gebieten ist grundsätzlich nicht erlaubt. Erfasst eine Drohne mit einer Kamera personenbezogene Daten im öffentlichen Raum, handelt es sich in der Regel um eine Datenverarbeitung im Anwendungsbereich der DS-GVO. Deren datenschutzrechtliche Vorgaben können beim Einsatz einer Drohne kaum eingehalten werden. In den meisten Fällen dürften bereits die Voraussetzungen des Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO, insbesondere hinsichtlich der Erforderlichkeit der Überwachung und dem überwiegenden Interesse des Verantwortlichen, nicht erfüllt sein. Zudem ist es fast unmöglich,

als Verantwortlicher den nachstehenden Hinweispflichten gemäß Art. 12, 13 DS-GVO nachzukommen. Zu beachten sind außerdem diverse andere Rechtsvorschriften, wie etwa die Luftverkehrs-Verordnung, die die Nutzung von Drohnen reglementieren. Weitere Informationen finden Sie im „Positionspapier zur Nutzung von Kameradrohnen durch nicht-öffentliche Stellen“ der DSK (abrufbar unter: https://www.datenschutzkonferenz-online.de/media/oh/20190116_oh_positionspapier_kameradrohnen.pdf).

Hinweispflichten – Art. 12, 13 DS-GVO

□ Auf die Überwachung wird mit einem vorgelagerten Hinweisschild hingewiesen (ein Muster stellt der TLfDI auf seiner Internetseite zur Verfügung).







- □ Das Hinweisschild enthält Angaben zum Verantwortlichen und seinen berechtigten Interessen an der Überwachung, den Zwecken und der Rechtsgrundlage der Datenverarbeitung, sowie der Speicherdauer.
- □ Das Hinweisschild ist gut sichtbar vor dem Aufnahmebereich angebracht.
- □ Ein ausführliches Info-Blatt nach Art. 13 DS-GVO wird vom Verantwortlichen für Nachfragen bereitgehalten (ein Muster stellt der TLfDI auf seiner Internetseite zur Verfügung).

Beispiel für ein vollständiges Informationsblatt (Aushang) nach Art. 13 der Datenschutz-Grundverordnung bei Videoüberwachung[1]



Sie finden diese Informationen zusätzlich im Internet unter ...

Name und Kontaktdaten des Verantwortlichen und ggf. seines Vertreters:

Kontaktdaten des Datenschutzbeauftragten (sofern vorhanden):

Zwecke und Rechtsgrundlage der Datenverarbeitung:

berechtigte Interessen, die verfolgt werden:

Speicherdauer oder Kriterien für die Festlegung der Dauer:

Empfänger oder Kategorien von Empfänger der Daten (sofern Datenübermittlung stattfindet):

bei Absicht des Verantwortlichen, die personenbezogenen Daten **an ein Drittland oder eine internationale Organisation zu übermitteln**: Informationen über Angemessenheitsbeschluss der Kommission bzw. geeignete oder angemessene Garantien:

Hinweise auf die Rechte der Betroffenen

Die betroffene Person hat das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden; ist dies der Fall, so hat sie ein **Recht auf Auskunft** über diese personenbezogenen Daten und auf die in Art. 15 DSGVO im einzelnen aufgeführten Informationen.

Die betroffene Person hat das Recht, von dem Verantwortlichen unverzüglich die **Berichtigung** sie betreffender unrichtiger personenbezogener Daten und ggf. die **Vervollständigung** unvollständiger personenbezogener Daten zu verlangen (Art. 16 DSGVO).

Die betroffene Person hat das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden, sofern einer der in Art. 17 DSGVO im einzelnen aufgeführten Gründe zutrifft, z. B. wenn die Daten für die verfolgten Zwecke nicht mehr benötigt werden (**Recht auf Löschung**).

Die betroffene Person hat das Recht, von dem Verantwortlichen die **Einschränkung der Verarbeitung** zu verlangen, wenn eine der in Art. 18 DSGVO aufgeführten Voraussetzungen gegeben ist, z. B. wenn die betroffene Person Widerspruch gegen die Verarbeitung eingelegt hat, für die Dauer der Prüfung durch den Verantwortlichen.

Die betroffene Person hat das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung sie betreffender personenbezogener Daten **Widerspruch** einzulegen. Der Verantwortliche verarbeitet die personenbezogenen Daten dann nicht mehr, es sei denn, er kann zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen (Art. 21 DSGVO).

Jede betroffene Person hat unbeschadet eines anderweitigen verwaltungsrechtlichen oder gerichtlichen Rechtsbehelfs das **Recht auf Beschwerde bei einer Aufsichtsbehörde**, wenn die betroffene Person der Ansicht ist, dass die Verarbeitung der sie betreffenden personenbezogenen Daten gegen die DSGVO verstößt (Art. 77 DSGVO). Die betroffene Person kann dieses Recht bei einer Aufsichtsbehörde in dem Mitgliedstaat ihres Aufenthaltsorts, ihres Arbeitsplatzes oder des Orts des mutmaßlichen Verstoßes geltend machen. In (Bundesland) ist die zuständige Aufsichtsbehörde: ...

[1] *Hinweis: Die Informationen sind unentgeltlich in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache bereitzustellen. Sie können in Kombination mit standardisierten Bildsymbolen bereitgestellt werden (vgl. Art. 12 DSGVO). Um Lesbarkeit zu erreichen, sollte der Ausdruck mindestens in DIN A3 erfolgen.*

1.14 Videogaga 2.0: Zur aktuellen Problematik der Videoüberwachung in Thüringer Kommunen

Zahlreiche große und auch kleinere Kommunen in Thüringen führten im Berichtszeitraum neue Videoüberwachungen ein oder planen in naher Zukunft deren Einführung. Dabei wird regelmäßig gegen die rechtlichen Grundlagen sowie in der Ausführung gegen wesentliche Datenschutzvorschriften verstoßen. Die Zusammenarbeit mit dem TLfDI gestaltet sich dabei manchmal als verbesserungsbedürftig.

Im abgelaufenen Jahr 2023 beobachtete der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) eine deutliche Zunahme sowohl von geplanten als auch von bereits angelaufenen kommunalen Videoüberwachungsmaßnahmen. Teilweise wurden – geradezu exzessiv – an zahlreichen Standorten innerhalb einer Stadt oder Ortschaft die Bürgerinnen und Bürger einer Überwachung mit teilweise neuester Videotechnik ausgesetzt. Dabei wurden der TLfDI oder sogar der/die eigene Datenschutzbeauftragte der Kommune nicht beteiligt.
Eine Südthüringer Kommune mit nicht einmal 25.000 Einwohnern überwachte zum Beispiel acht Standorte mit teilweise bis zu vier Kameras. Trotz mehrerer Nachfragen und Hinweise des TLfDI erfolgte der notwendige Nachweis, dass die Überwachung datenschutzrechtlich zulässig ist, bislang für keinen der überwachten Orte.
Ein weiteres, unrühmliches Beispiel: Am nördlichen Rand des Thüringer Waldes hat eine Kommune, trotz ausführlicher Beratung und ausdrücklicher Hinweise des TLfDI zur rechtlichen Unzulässigkeit im Vorfeld, eine Videoüberwachungsanlage in Betrieb genommen. Dies erfolgte, ohne den TLfDI über den Beginn der Videoüberwachung zu informieren, obwohl dieser extra zuvor darum gebeten hatte. Nachdem der TLfDI über die Medien von der Videoüberwachung Kenntnis erlangt hatte, wurde die Stadt zur Stellungnahme und Beantwortung von Fragen des TLfDI unter Hinweis auf ihre Mitwirkungspflicht aufgefordert. Die Stadt bat daraufhin um Fristverlängerung, welche vom TLfDI auch gewährt wurde. Die dann beim TLfDI eingegangene Mitteilung hatte den Inhalt, dass die Mitwirkungspflicht nach § 7 Abs. 1 Thüringer Datenschutzgesetz in Verbindung mit Art. 58 Abs. 1 a) Datenschutz-Grundverordnung (DS-GVO) durch die Stadt selbst nicht angezweifelt werde. Eine Stellungnahme oder gar Beantwortung der

Fragen erfolgte von ihr dennoch nicht. Nachdem der TLfDI die Kommune auf ihre Mitwirkungspflicht nochmals eindringlich hingewiesen hatte, folgte nach einer weiteren Fristverlängerung die Antwort, dass man jetzt Rücksprache mit dem eigenen Datenschutzbeauftragen halten und dann die Fragen ausführlich beantworten werde. Fortsetzung folgt – der TLfDI lässt hier garantiert nicht locker.
Noch interessanter stellt sich der Sachverhalt einer Überwachung durch eine Ostthüringer Stadt dar. Auch hier erfuhren die zuständigen Mitarbeiter des TLfDI von der tatsächlichen Durchführung der Videoüberwachungsmaßnahmen, unter anderem an einer Toilettenanlage, nicht von der Kommune selbst. Auf die Aufforderung des TLfDI zur Stellungnahme kam nach einer gewährten Fristverlängerung die Antwort von der Stadt, dass man die Videoüberwachungsanlagen einer eigenen Verhältnismäßigkeitsüberprüfung unterzogen habe und eine Beantwortung der einzelnen Fragen des TLfDI daher entbehrlich sei. Der TLfDI hätte seine Fragen ja schließlich nur mit dem Angebot einer Unterstützung verknüpft. Durch die eigene Prüfung der Stadt habe sich daher die mit der TLfDI-Anfrage verbundene Fristsetzung erledigt. Es liegt auf der Hand, dass sich der TLfDI mit dieser Antwort nicht begnügt und den Sachverhalt weiterhin genau überprüft hat.
An dieser Stelle möchte der TLfDI auf Folgendes hinweisen: Selbstverständlich werden Anfragen und Anhörungen des TLfDI, dem Gebot der Höflichkeit entsprechend, regelmäßig in Form einer Bitte und mit dem Angebot der Unterstützung verfasst. Gleichzeitig erfolgt aber auch in aller Regel, so auch in den vorgestellten Fällen, der ausdrückliche schriftliche Hinweis auf die bestehende Mitwirkungs- und Auskunftspflicht der öffentlichen Stellen gemäß § 6 Abs. 3 Thüringer Datenschutzgesetz. Ein Ermessen der Kommunen, ob Anfragen des TLfDI zu beantworten sind, besteht daher nicht!
Zum vierten Beispiel: Eine Mittelthüringer Landgemeinde unterzog der TLfDI im Rahmen der Bearbeitung einer Beschwerde einer Kontrolle ihres Freibades. Dabei stellte der TLfDI vor Ort fest, dass fast das gesamte Freibad-Gelände, auch das Kinderspielbecken und die Zugänge zu den Umkleiden, mit mehr als einem Dutzend Kameras überwacht wird. Die Gemeinde benannte unter anderem den Schutz vor unberechtigten Schadenersatzansprüchen der Besucherinnen und Besucher und die Sicherheit der Gäste als Gründe für diese übermäßige Überwachung. Auf Nachfrage konnte dem TLfDI bis zum Zeitpunkt des Redaktionsschlusses für diesen Tätigkeitsbericht kein tat-

sächlich für die datenschutzrechtliche Prüfung auch nur entfernt relevanter Vorfall benannt werden, bei dem die Videoüberwachung zur Erreichung der von der Gemeinde angegebenen Zwecke geholfen hätte.
Der TLfDI möchte hier betonen, dass eine Videoüberwachung von einer Kommune grundsätzlich nicht präventiv eingesetzt werden kann. Wenn vor Ort noch nie etwas Relevantes vorgefallen ist, fehlt im Allgemeinen eine rechtliche Grundlage für solche in das Grundrecht auf informationelle Selbstbestimmung der betroffenen Bürgerinnen und Bürger erheblich eingreifende Maßnahmen einer Videoüberwachung. Der TLfDI wird darüber hinaus bei Anhörungen regelmäßig mit den Argumenten konfrontiert, dass sich noch nie jemand über die Kameras beschwert habe und im Übrigen durch die Überwachung das Sicherheitsgefühl der Bürgerinnen und Bürger verstärkt werde. Beide Argumente sind auch für den TLfDI durchaus nachvollziehbar. Es fehlen jedoch – nicht nur im Freistaat Thüringen – Rechtsvorschriften, die solche Zwecke mit in die Voraussetzungen der Zulässigkeit von Videoüberwachungen einbeziehen!
In allen oben genannten Fällen folgten somit, von den gesetzlichen Grundlagen einmal abgesehen, auch im Rahmen der Durchführung der Videoüberwachung wesentliche Verstöße. **Diese wird der TLfDI – soweit noch nicht geschehen – entsprechend Art. 58 Abs. 2 DS-GVO ahnden!** Bei bislang keiner der beispielhaft aufgeführten Kommunen konnte der TLfDI überdies eine datenschutzkonforme Ausgestaltung der nach Art. 13 DS-GVO notwendigen Hinweise auf die Videoüberwachung feststellen. Dies erstaunt umso mehr, als dass seit Geltung der DS-GVO auf der Internetseite des TLfDI entsprechende, regelmäßig aktualisierte Muster mit den dazugehörigen Aufstellhinweisen zu finden sind, siehe dazu: https://www.tlfdi.de/fileadmin/tlfdi/datenschutz/video/anlage2_vollst_information_final.pdf und https://www.tlfdi.de/fileadmin/tlfdi/datenschutz/video/anlage1_hinweisschild_final.pdf.
Aber es gibt auch positive Entwicklungen zu berichten: Im vergangenen Jahr haben sich mehrere Kommunen bereits in frühen Stadien der Planung solcher Videoüberwachungsmaßnahmen an den TLfDI gewandt. Der TLfDI begrüßt dies ausdrücklich. Durch die Hilfe und aktive Unterstützung des TLfDI können Fehler und unnötige Kosten bei den Städten und Gemeinden vermieden werden. Der TLfDI wird daher auch im kommenden Jahr bestrebt sein, alle Anfragen der öffentlichen Stellen zum Einsatz von Videoüberwachungstechnik so gut wie

möglich zu beantworten – auch wenn es manchmal aufgrund der hohen Anzahl der Anfragen und der geringen Anzahl der einzusetzenden Mitarbeitenden beim TLfDI ein wenig länger dauern kann!

1.15 Nachgefragt – Verbesserungsbedürftige Aspekte beim Amt des kommunalen Datenschutzbeauftragten

Eine vom TLfDI im Berichtszeitraum durchgeführte Umfrage bei den Mitgliedern des Arbeitskreises der kommunalen Datenschutzbeauftragten ergab, dass für viele Amtsinhaber ein höherer Zeitanteil und eine bessere Vergütung für die Bewältigung ihrer Aufgaben wünschenswert wären.

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) führte im Berichtszeitraum im Rahmen des Arbeitskreises der kommunalen Datenschutzbeauftragten eine freiwillige und anonyme Umfrage durch. Hintergrund dieser Umfrage war die im Arbeitskreis aufgekommene Thematik zur Eingruppierung der kommunalen Datenschutzbeauftragten und deren Zeitanteilen. Aus den 35 eingegangenen Antworten dieser Umfrage ergab sich folgendes Bild:
40 Prozent der angefragten kommunalen Datenschutzbeauftragten bezifferten ihre Zeitanteile in der Woche für die Aufgabe als Datenschutzbeauftragte(r) mit fünf bis zehn Stunden, 26 Prozent mit elf bis 20 Stunden und jeweils 14 Prozent mit 21 bis 30 Stunden sowie 31 bis 40 Stunden. Für die Mehrzahl der befragten Datenschutzbeauftragten (63 Prozent) reichten die Zeitanteile für die Wahrnehmung der Aufgaben als Datenschutzbeauftragte(r) nicht aus. Lediglich 34 Prozent der Befragten sahen ihre Zeitanteile als genügend für die Bewältigung der Aufgaben an.
Weiterhin ergab sich aus der Umfrage, dass die Mehrheit der angefragten kommunalen Datenschutzbeauftragten im gehobenen Dienst tätig ist. Für 60 Prozent wäre eine Anhebung der Zeitanteile sowie eine höhere Eingruppierung wünschenswert.
Der TLfDI weiß, dass die kommunalen Datenschutzbeauftragten ein wichtiges Amt innehaben. Bereits im letzten Tätigkeitsbericht (unter Punkt 1.4. „Die kommunalen Datenschutzbeauftragten – unverzichtbar“) widmete sich der TLfDI in einem Beitrag den kommunalen Datenschutzbeauftragten und ihrer Arbeit.

Zu den Aufgaben eines behördlichen Datenschutzbeauftragten gehören unter anderem die Überwachung der Einhaltung der Datenschutz-Grundverordnung (DS-GVO), des Thüringer Datenschutzgesetzes (ThürDSG) und anderer datenschutzrechtlicher Bestimmungen (siehe § 15 Abs. 1 ThürDSG) sowie der auf Grundlage der JI-Richtlinie erlassenen Rechtsvorschriften (dazu insbesondere § 15 Abs. 3 ThürDSG), die Unterrichtung und die Beratung des Verantwortlichen und der Beschäftigten, die Verarbeitungen personenbezogener Daten durchführen, Schulungen zum Datenschutz, die Zusammenarbeit mit der Aufsichtsbehörde und Anlaufstelle für diese zu sein. Zudem ist den behördlichen Datenschutzbeauftragten vor der erstmaligen Inbetriebnahme einer Verarbeitungstätigkeit das dafür erforderliche Verzeichnis mit der Gelegenheit zur Stellungnahme vorzulegen. Schließlich sind die behördlichen Datenschutzbeauftragten bei einer Datenschutz-Folgenabschätzung einzubeziehen.
Schon im bereits erwähnten 5. Tätigkeitsbericht nach der DS-GVO wies der TLfDI darauf hin, dass sich die Arbeit der kommunalen Datenschutzbeauftragten in einer angemessenen Vergütung widerspiegeln sollte und die öffentliche Stelle sicherzustellen hat, dass für sie/ihn hinreichende Arbeitszeit verbleibt, um diese verantwortungsvolle Aufgabe wahrzunehmen.
Diese Einschätzung deckt sich nun auch mit den Ergebnissen dieser Umfrage. Es wäre wünschenswert, dass die verantwortlichen öffentlichen Stellen dies bei der Einrichtung des Amtes des behördlichen kommunalen Datenschutzbeauftragten berücksichtigen.

1.16 Kleiner Fehler, große Wirkung – Der Versand von E-Mails in „cc“

Der TLfDI hat immer wieder mit Fällen zu tun, bei denen eine E-Mail anstatt in „bcc“ (blind-copy-carbon = Blindkopie) in „cc (carbon-copy = Kopie) an einen großen Empfängerkreis gesendet wird. Das mag banal klingen, ist es aber nicht. Der große Unterschied zwischen „cc“ und „bcc“ liegt darin, dass „cc“ ein offener Empfängerkreis bedeutet, sodass jeder Empfänger die jeweils anderen Empfänger und deren private E-Mail-Adressen sehen kann.

E-Mail schreiben, alle Empfänger mit deren privaten E-Mail-Adressen einfügen, losschicken. Das passiert jeden Tag unzählige Male. Doch selbst bei einer so banalen Tätigkeit ist daran zu denken, wie

eine E-Mail mit großem Empfängerkreis datenschutzkonform zu verschicken ist.

Gemäß Art. 5 Abs. 1 Buchstabe f) Datenschutz-Grundverordnung (DS-GVO) müssen personenbezogene Daten in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit"). Unter Berücksichtigung des Stands der Technik trifft der Verantwortliche geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen gemäß Art. 32 Abs. 1 Buchstabe b) DS-GVO die Vertraulichkeit mit ein.

Bei der Übermittlung einer E-Mail an einen offenen Empfängerkreis, bei der ein oder mehrere Empfänger mit ihren privaten E-Mail-Adressen für anderer Empfänger sichtbar sind, ist grundsätzlich die Vertraulichkeit gefährdet, da die Gefahr besteht, dass unbefugte Personen einen Zugriff auf die personenbezogenen Daten (Name und private E-Mail-Adresse) erhalten können.

Von einer konkludenten Einwilligung der betroffenen Person sollte der Verantwortliche grundsätzlich nicht ausgehen, da er gemäß Art. 7 Abs. 1 DS-GVO nachweisen muss, dass diese Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat. Diese Nachweispflicht dürfte jedoch schwerfallen. Darüber hinaus weiß die betroffene Person in den meisten Fällen im Vorhinein nicht, wer die Empfänger sein könnten. Auch allein die Tatsache, dass eine betroffene Person eine E-Mail an den Verantwortlichen schreibt, ist grundsätzlich nicht dahingehend auszulegen, dass diese in eine Offenlegung der persönlichen E-Mail-Adresse innerhalb eines großen Empfängerkreises eingewilligt hat, sondern grundsätzlich erst einmal nur darin, dass die öffentliche Stelle mit ihr persönlich kommunizieren kann.

Es gibt jedoch eine einfache Lösung für dieses Problem: eine Versendung der E-Mail in „Blindkopie" (Verwendung des Feldes „Bcc:" in E-Mail-Klienten zur Eintragung der Empfänger). In dem Feld „An" ist dann lediglich der Absender sichtbar und die Empfänger können unter dem Feld „Bcc" („blind carbon copy" = Blindkopie) angegeben werden. So sind sie untereinander nicht sichtbar.

Datenschutz kann auch einfach sein! Man muss nur daran denken.

1.17 Arbeitsunfähig? Was muss man dem Arbeitgeber mitteilen?

Durch das zum 1. Januar 2023 eingeführte Verfahren der eAU (elektronischen Arbeitsunfähigkeitsbescheinigung) erhält die gesetzliche Krankenkasse vom Arzt über ein sicheres Verfahren die für diese erforderlichen Daten zum Patienten. Der Arbeitgeber ist vom Beschäftigten über die Arbeitsunfähigkeit zu unterrichten, was den Arbeitgeber in die Lage versetzt, die erforderlichen Angaben von der Krankenkasse abzurufen.

Ende Januar 2023 erreichte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) eine Anfrage, ob es denn in Ordnung sei, dass der Arbeitgeber von den Beschäftigten verlangt, sie sollen per E-Mail der Personalverwaltung und dem Leiter am Beschäftigungsort Beginn und (voraussichtliche) Dauer der Arbeitsunfähigkeit mitteilen sowie, ob es sich um eine Erst- oder Folgebescheinigung handelt, sofern der Arzt keine Arbeitsunfähigkeitsbescheinigung (AU) in Papierform ausgehändigt habe. Die AU solle wie gewohnt abgegeben werden.
Durch das zum 1. Januar 2023 eingeführte Verfahren der eAU erhält die Krankenkasse vom Arzt über ein sicheres Verfahren die für diese erforderlichen Daten zum Patienten. Der Arbeitgeber ist vom Beschäftigten über die Arbeitsunfähigkeit zu unterrichten, was den Arbeitgeber in die Lage versetzt, die erforderlichen Angaben von der Krankenkasse abzurufen.
Bei den vom Arbeitgeber verlangten Angaben zur Arbeitsunfähigkeit handelt es sich in Verbindung mit dem Namen eines Beschäftigten um dessen Gesundheitsdaten, die gegen unbefugte Kenntnis besonders zu schützen sind. Der Arbeitgeber hat Anspruch auf die Angaben, die auch auf einer für ihn bestimmten Arbeitsunfähigkeitsbescheinigung in Papierform (ohne Diagnose) enthalten sind, jedoch kann er aufgrund der Sensibilität der Angaben als Gesundheitsdaten nicht verlangen, dass sie der Personalverwaltung und weiteren Personen (Einrichtungsleiter) ungesichert per E-Mail übermittelt werden. Ein derartiges Übermittlungsverlangen an die Personalverwaltung wäre nur dann rechtmäßig, wenn die nach dem Grundsatz der Integrität und Vertraulichkeit erforderliche angemessene Sicherheit durch den Einsatz einer geeigneten Verschlüsselungstechnik gewährleistet wäre (Art. 5 Abs. 1 Buchstabe f) Datenschutz-Grundverordnung).

Der/die direkte Vorgesetzte benötigt darüber hinaus lediglich die Dauer der AU, um gegebenenfalls aufgrund seiner/ihrer bestehenden Zuständigkeit das Erforderliche zu veranlassen, um eine Vertretung zu organisieren.
Das Verlangen, auf ungesichertem Kommunikationsweg über E-Mail sowohl der Personalverwaltung als auch dem direkten Vorgesetzten die aufgezählten Informationen zukommen zu lassen, ist daher unzulässig.

1.18 Datenschutz kontra Archivwesen: Corona-Impfdaten für die Nachwelt – wen interessiert das?

Nach dem Grundsatz der Rechtmäßigkeit der Datenverarbeitung (Art. 5 Abs. 1 Buchstabe a) DS-GVO in Verbindung mit Art. 6 Abs. 1 Satz 1 Buchstabe c) DS-GVO) dürfen personenbezogene Daten nach Wegfall der Rechtsgrundlage nicht weiterverarbeitet und somit auch nicht weiter gespeichert werden. Gemäß Art. 17 Abs. 1 Buchstabe a) DS-GVO sind personenbezogene Daten umgehend zu löschen, wenn sie für die Zwecke, für die sie erhoben wurden, nicht mehr benötigt werden.

Im Berichtszeitraum wandte sich ein Beschäftigter aus dem medizinischen Bereich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und fragte, wie mit gespeicherten personenbezogenen Daten zum Corona-Impfstatus von Mitarbeitern in Krankenhäusern und medizinischen Einrichtungen in Thüringen durch die Gesundheitsämter zukünftig umzugehen sei. Der TLfDI beantwortete die Nachfrage und nahm sie zum Anlass, die oberste Gesundheitsbehörde in Thüringen, das Thüringer Ministerium für Arbeit, Soziales, Gesundheit, Frauen und Familie (TMASGFF) auf den datenschutzrechtlich legitimen Umgang mit den personenbezogenen Impfdaten hinzuweisen.
Seit dem 15. März 2022 galt für Mitarbeiter in Gesundheitseinrichtungen gemäß § 20a Infektionsschutzgesetz (IfSG) die einrichtungsbezogene Impfpflicht. Gemäß § 20a Abs. 2 Satz 2 IfSG waren Arbeitgeber im Gesundheitsbereich verpflichtet, fehlende Impf- und/oder Genesenennachweise ihrer Mitarbeiter den zuständigen Gesundheitsbehörden (den Thüringer Gesundheitsämtern) mitzuteilen. Somit wurden diese personenbezogenen Gesundheitsdaten von den Gesundheitsämtern verarbeitet.

Der TLfDI teilte dem TMASGFF schriftlich mit, dass aufgrund der in Artikel 2 des Gesetzes zur Stärkung der Impfprävention gegen COVID-19 beschlossenen Änderungen § 20a IfSG zum 1. Januar 2023 aufgehoben wurde. Mit der Aufhebung entfielen auch die einrichtungsbezogene Impfpflicht und die entsprechende Nachweisführung gegenüber den zuständigen Gesundheitsbehörden mit Wirkung vom 1. Januar 2023. Nach dem Grundsatz der Rechtmäßigkeit der Datenverarbeitung dürfen personenbezogene (Gesundheits-)Daten nach Wegfall der Rechtsgrundlage nicht weiterverarbeitet und somit auch nicht weiter gespeichert werden (Art. 5 Abs. 1 Buchstabe a) Datenschutz-Grundverordnung – DS-GVO in Verbindung mit Art. 6 Abs. 1 Satz 1 Buchstabe c DS-GVO). Der Grundsatz der Datenminimierung aus Art. 5 Abs. 1 Buchstabe c) DS-GVO gebietet zudem, dass die Datenverarbeitung auf das notwendige Maß beschränkt wird und nur Daten verarbeitet werden, die dem Zweck angemessen und erforderlich sind. Gemäß Art. 17 Abs. 1 Buchstabe a) DS-GVO sind personenbezogene Daten umgehend zu löschen, wenn sie für die Zwecke, für die sie erhoben wurden, nicht mehr benötigt werden. Soweit die Daten jedoch gemäß Art. 17 Abs. 3 Buchstabe d) DS-GVO für im öffentlichen Interesse liegende Archivzwecke (weiter-)verarbeitet werden (sollen) gilt die Löschungsvorgabe nicht. Eine gesetzliche Grundlage für die in diesem Falle erfolgende Speicherung der Daten findet sich im Thüringer Archivgesetz (ThürArchivG). Im Hinblick auf die datenschutzrechtlich gebotene Löschung der Impfstatusdaten und deren mögliche weitere Speicherung informierte der TLfDI die oberste Thüringer Gesundheitsbehörde darüber, dass der Löschungsvorgabe der DS-GVO gegebenenfalls § 11 Abs. 3 Satz 1 Nr. 2 des ThürArchivG entgegenstehen könnte, da diese Gesetzesnorm eine punktuelle Anbietungspflicht für bestimmte Unterlagen, an das Thüringer Landesarchiv regelt, einschließlich Unterlagen die besondere Datenkategorien gemäß Art. 9 Abs. 1 DS-GVO enthalten.

Die Bewertung, ob die vorliegenden personenbezogenen (Gesundheits-)Daten über den Impfstatus archivwürdig sind oder nicht, obliegt gemäß § 12 Abs. 1 ThürArchivG jedoch nicht dem TLfDI, sondern dem zuständigen Archiv. Gemäß § 11 Abs. 1 Satz 1 ThürArchivG müssen die Gesundheitsämter die betreffenden Unterlagen „… dem zuständigen öffentlichen Archiv“ (der kreisfreien Stadt beziehungsweise des Landkreises) zur Übernahme anbieten. Nach § 12 Abs. 1 Satz 1 ThürArchivG „… entscheiden die öffentlichen Archive im Be-

nehmen mit der anbietenden Stelle“ über die Übernahme der Dokumente. Da die 23 Gesundheitsämter in Thüringen jeweils „eigene“ für sie zuständige Archive haben, kann es sein, dass ein Archiv die Dokumente übernimmt, während ein anderes Archiv die Dokumente nicht übernimmt. Insofern bestünde dann keine einheitliche Vorgehensweise im Umgang mit diesen personenbezogenen Daten. Ungeachtet dessen teilte der TLfDI dem TMASGFF mit, dass die personenbezogenen Daten zum Corona-Impfstatus gemäß den datenschutzrechtlichen Bestimmungen zu löschen sind, wenn sie nicht als archivwürdig bewertet werden. Der TLfDI empfahl dem TMASGFF, seinen nachgeordneten Gesundheitsbereich, das heißt alle Thüringer Gesundheitsämter, hierüber zu informieren.

1.19 Wichtige Entscheidungen des EuGH im Berichtszeitraum

Der Europäische Gerichtshof hat im Berichtszeitraum einige richtungsweisende Entscheidungen zur Auslegung der Datenschutz-Grundordnung getroffen. Einige werden hier kurz vorgestellt.

Gleich in zwei Entscheidungen beschäftigte sich der Europäische Gerichtshof (EuGH) mit dem Umfang des Auskunftsanspruchs und dem Recht auf Kopie nach Art. 15 Datenschutz-Grundverordnung (DS-GVO). Hierzu gibt es einen gesonderten Beitrag (siehe Beitrag Nr. 1.5).
In der Rechtssache C-60/22 (https://curia.europa.eu/juris/document/document.jsf?text=&docid=273289&pageIndex=0&doclang=DE&mode=lst&dir=&occ=first&part=1&cid=3993129) stellt der EuGH fest, dass Verstöße gegen die Pflichten aus den Artikeln 26 und 30 DS-GVO keine unrechtmäßige Verarbeitung darstellen, die Betroffenen ein Recht auf Löschung oder auf Einschränkung der Verarbeitung gibt. Wenn ein Verantwortlicher keine Vereinbarung mit Festlegungen über die gemeinsame Verantwortung für die Verarbeitung getroffen hat oder kein Verzeichnis über die Verarbeitungstätigkeiten führt, folgt daraus nicht ohne weiteres, dass der Verantwortliche auch gegen den Grundsatz der „Rechenschaftspflicht“ im Sinne von Art. 5 Abs. 2 in Verbindung mit Art. 5 Abs. 1 Buchstabe a) und Art. 6 Abs. 1 DS-GVO verstoßen hat. Auch wenn ein datenschutzrechtlich Verantwortlicher gegen seine Pflichten aus Art. 26 oder 30

DS-GVO verstoßen hat, können personenbezogene Daten ohne die Einwilligung des Betroffenen rechtmäßig verarbeitet werden.
Derartigen Verstößen ist nach Auffassung des EuGH durch die Ausübung der aufsichtsbehördlichen Abhilfebefugnisse zu begegnen, beispielsweise durch die Anordnung nach Art. 58 Abs. 2 Buchstabe d) DS-GVO, Verarbeitungsvorgänge in Einklang mit der DS-GVO zu bringen (Rn. 67). Damit macht der EuGH deutlich, dass zwischen der Frage der Rechtsgrundlage für eine Datenverarbeitung und den übrigen Pflichten nach der DS-GVO differenziert werden muss. Ob eine Verarbeitung unrechtmäßig erfolgt ist, hängt allein davon ab, ob eine Rechtsgrundlage für die jeweilige Verarbeitung existiert.
Mit der spannenden Frage, ob gegen ein Unternehmen ein Bußgeld verhängt werden kann, beschäftigte sich der EuGH in der Rechtssache C-807/21 (https://curia.europa.eu/juris/document/document.jsf?text=&docid=280325&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1&cid=4504591).
Nach deutschem Recht kann in aller Regel nur ein Bußgeld gegen eine natürliche Person verhängt werden, die schuldhaft, also vorsätzlich oder fahrlässig gehandelt hat. Die DS-GVO nimmt aber den Verantwortlichen in die Pflicht, also denjenigen, der Mittel und Zwecke der Verarbeitung bestimmt, Art. 4 Nr. 7 DS-GVO. Das VG Wiesbaden legte dem EuGH daher folgende Frage zur Entscheidung vor:
Kann ein Bußgeldverfahren unmittelbar gegen ein Unternehmen geführt werden, ohne dass es für die Bebußung der Feststellung einer durch eine natürliche und identifizierte Person begangenen Ordnungswidrigkeit bedarf?
Muss das Unternehmen den durch einen Mitarbeitenden vermittelten Verstoß schuldhaft begangen haben, oder reicht für eine Bebußung des Unternehmens im Grundsatz bereits ein ihm zuzuordnender objektiver Pflichtenverstoß gegen die DS-GVO aus?
Der EuGH stellte klar, dass eine Geldbuße gemäß Art. 83 Abs. 4 bis 6 DS-GVO unmittelbar gegen ein Unternehmen verhängt werden darf, wenn dieses als für die betreffende Verarbeitung Verantwortliche eingestuft wird.
Nach dem Wortlaut des Art. 83 Abs. 2 DS-GVO könnten nur Datenschutzverstöße, welche der Verantwortliche schuldhaft begehe, also vorsätzlich oder fahrlässig, zur Verhängung einer Geldbuße führen. Es bedarf deshalb der Feststellung, dass ein Verstoß gegen die DS-GVO vorsätzlich oder fahrlässig begangen wurde (Randziffer 75 des

Urteils). Die Anforderungen hieran setzt der EuGH aber nicht hoch. Es genügt, wenn der Verantwortliche über die „Rechtswidrigkeit seines Verhaltens nicht im Unklaren sein konnte“. Hierbei sei es irrelevant, ob ihm der Verstoß gegen die DS-GVO bewusst sei (Randziffer 76 des Urteils). Auch sei keine Handlung und keine Kenntnis durch ein Leitungsorgan der juristischen Person erforderlich (Randziffer 77 des Urteils).
Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) kann damit an seiner bisherigen Praxis festhalten, Bußgeldverfahren unmittelbar auch gegen Unternehmen zu führen.
Im Fall C-634/21 (https://curia.europa.eu/juris/document/document.jsf?text=&docid=280426&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1) stand das Scoring-Verfahren der SCHUFA im Mittelpunkt. Der EuGH beschäftigte sich mit der Frage, ob die automatisierte Erstellung eines Wahrscheinlichkeitswertes über die Fähigkeit einer Person, einen Kredit zu bedienen, als Profiling im Sinne der Datenschutz-Grundverordnung zu sehen ist und damit möglicherweise die Bonitätseinstufungen der SCHUFA als automatisierte Einzelfallentscheidungen nach Art. 22 DS-GVO grundsätzlich unzulässig sind. Danach hat jeder Mensch das Recht, nicht einer Entscheidung unterworfen zu werden, die ausschließlich auf einer automatisierten Verarbeitung beruht, wenn diese nicht besonders legitimiert ist. Nach Auffassung des EuGH fallen Scoring-Verfahren als automatisierte Entscheidungen im Einzelfall unter Art. 22 DS-GVO. Deshalb sei das Scoring der SCHUFA nur unter bestimmten Voraussetzungen zulässig. Unternehmen dürften nicht ausschließlich auf Grundlage einer automatisierten Bewertung der Kreditwürdigkeit durch die SCHUFA entscheiden, ob sie Verträge mit Kunden abschließen. Der Score ist als eine grundsätzlich verbotene „automatisierte Entscheidung im Einzelfall“ anzusehen, wenn er ohne Legitimation etwa bei der Kreditvergabe „maßgeblich“ zugrunde gelegt wird. Nationale Rechtsvorschriften, die den Einsatz von Score-Werten – ausnahmsweise – erlauben, müssen nach dem Urteil des EuGH Regelungen zur Einhaltung der Grundsätze der DS-GVO beinhalten und insbesondere sicherstellen, dass es nicht zu Diskriminierungen einzelner Betroffener kommt. Der EuGH hat dem VG Wiesbaden aufgegeben, im weiteren Verfahren auch zu prüfen, ob die Rechtsgrundlage für das Scoring in § 31 Bundesdatenschutzgesetz diesen Anforderungen genügt.

Das Urteil hat insbesondere Konsequenzen für die Kreditwirtschaft, aber auch andere Unternehmen, bei welchen man nur dann einen Vertrag abschließen kann, wenn der SCHUFA-Score über einem bestimmten Wert liegt.
In den verbundenen Rechtssachen C-26/22 und C-624/22 (https://curia.europa.eu/juris/document/document.jsf?text=&docid=280428&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1= befasste sich der EuGH mit der Frage, welche Rechtnatur das Beschwerdeverfahren bei den Aufsichtsbehörden hat. Von Datenverarbeitungen betroffene Personen können bei diesen eine Beschwerde einreichen, wenn sie der Meinung sind, dass die Verarbeitung ihrer Daten unzulässig im Sinne der DS-GVO ist. Die Aufsichtsbehörde muss dieser Beschwerde nachgehen und über sie entscheiden. Gegen diese Entscheidung kann die betroffene Person Klage vor dem Verwaltungsgericht erheben. Bis zur Entscheidung des EuGH war der Charakter der Beschwerde und des Beschwerdeverfahrens und die Prüfungsbefugnis der Gerichte teilweise umstritten. Der EuGH stellt nun klar, dass die Entscheidung der Aufsichtsbehörde der vollständigen inhaltlichen Kontrolle durch das zuständige Gericht unterliegt. Es darf sämtliche für den bei ihm anhängigen Rechtsstreits maßgeblichen Sach- und Rechtsfragen prüfen. Die Aufsichtsbehörde muss sich mit aller gebotenen Sorgfalt mit einer Beschwerde befassen, sie hat aber hinsichtlich der in Art. 58 Abs. 2 DS-GVO aufgezählten Abhilfebefugnisse ein Ermessen in Bezug auf die geeigneten und erforderlichen Mittel. Die Gewährleistung eines wirksamen gerichtlichen Rechtsschutzes erfordert nicht, dass das Gericht befugt wäre, seine Beurteilung der Wahl der geeigneten und erforderlichen Abhilfebefugnisse an die Stelle der Beurteilung dieser Behörde zu setzen, sondern verlangt, dass dieses Gericht prüft, ob die Aufsichtsbehörde die Grenzen ihres Ermessens eingehalten hat.
Die Entscheidung des EuGH bestätigt die Rechtsauffassung des TLfDI, der seine Entscheidungen bislang bereits als verbindliche Beschlüsse nach Art. 78 Abs. 1 DS-GVO ausgestaltet hatte.

1.20 Etwas Gutes aus Europa: Die Arbeit des Europäischen Datenschutzausschusses zur einheitlichen Anwendung der Datenschutzregeln

Auch wenn es in Deutschland aufgrund seiner föderalen Struktur insgesamt 18 Datenschutz-Aufsichtsbehörden gibt – am Ende müssen diese sich dank der Datenschutz-Grundverordnung (DS-GVO) alle an die Vorgaben des Europäischen Datenschutzausschusses (EDSA) halten. Dies beweist der Streitbeilegungsbeschluss des EDSA in Sachen TikTok-Einstellungen und zur Verarbeitung von personenbezogenen Daten bei Kindern vom 2. August 2023 einmal mehr!

Nachdem der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) bereits im fünften Tätigkeitsbericht zum Datenschutz nach der DS-GVO über die Leitlinien des Europäischen Datenschutzausschusses (EDSA) berichtet hatte (siehe dazu Beitrag Nr. 1.3 Leitlinien des EDSA), möchte er in diesem Artikel die verschiedenen datenschutzrechtlichen Aufgaben des **Europäischen Datenschutzausschuss**, abgekürzt **EDSA** (auf Englisch: European Data Protection Board, abgekürzt **EDPB**) kurz darstellen und insbesondere auf ein Instrument des EDSA näher eingehen, den verbindlichen Streitbeilegungsbeschluss (auf Englisch: Dispute Resolution) gemäß Artikel 65 Abs. 1 Datenschutz-Grundverordnung (DS-GVO).
Was ist der EDSA überhaupt? Im EDSA sind die Leiter der nationalen Datenschutzaufsichtsbehörden aller Mitgliedsstaaten der Europäischen Union sowie der Europäische Datenschutzbeauftragte vertreten. Der Ausschuss verfügt als Einrichtung der Europäischen Union über eine eigene Rechtspersönlichkeit. Da Deutschland aufgrund seiner föderalen Struktur mehrere, nämlich insgesamt 18 (!) Datenschutzaufsichtsbehörden hat, wird von diesen ein gemeinsamer Vertreter ernannt, der sie in dem Ausschuss vertritt. Die Datenschutz-Grundverordnung (DS-GVO) legt in Artikel 9 DS-GVO fest, dass der EDSA bei der Erfüllung seiner Aufgaben oder in Ausübung seiner Befugnisse unabhängig und weisungsfrei handelt. Die Hauptaufgabe des EDSA besteht in der Sicherstellung und Überwachung der unionweiten einheitlichen Anwendung der DS-GVO. Dazu werden unter anderem Leitlinien bereitgestellt, die eine Präzisierung der DS-GVO-Normen vermitteln. Der EDSA verfügt über Unterarbeitsgruppen, die sogenannten Expert Subgroups, die diese Leitlinien für den Ausschuss vorbereiten. Auch der TLfDI ist mit einem Mitarbeiter in einer solchen

Subgroup vertreten. Eine weitere wichtige Aufgabe des EDSA ist es, dass dieser bei grenzüberschreitenden Fällen (das heißt, mehrere europäische Mitgliedstaaten sind betroffen) verbindliche Entscheidungen zu Datenschutzfragen treffen kann, wenn zuvor kein Konsens erzielt wurde.
Einen solchen verbindlichen Streitbeilegungsbeschluss möchte der TLfDI an dieser Stelle beispielhaft hervorheben und auf den Beschluss 2/2023 des EDSA (auf Englisch verfügbar unter: edpb_bindingdecision_202302_ie_sa_ttl_children_en.pdf (europa.eu) eingehen, in dem es um die Verarbeitung von personenbezogenen Daten von Kindern durch TikTok ging:
Die zuständige irische Datenschutzbehörde hatte dazu gegenüber der TikTok Technologie Limited einen Beschluss-Entwurf zu der Frage vorgelegt, wie diese Firma personenbezogene Daten von registrierten TikTok-Nutzern im Alter zwischen 13 und 17 Jahren verarbeitet. Kurze Zwischeninfo: Bei TikTok handelt es sich um ein Internet-Videoportal für die Lippensynchronisation von Musikvideos und anderen kurzen Videoclips, das auch Funktionen eines sozialen Netzwerks anbietet. Mehreren anderen europäischen Datenschutzaufsichtsbehörden gingen die Feststellungen der irischen Datenschutzaufsichtsbehörde zur TikTok-Datenverarbeitung nicht weit genug.
In seinem verbindlichen Beschluss zur Streitbeilegung beurteilte der EDSA daher die von TikTok verwendeten Gestaltungspraktiken im Zusammenhang mit zwei Pop-ups (= eine bestimmte Form von Werbeeinblendungen im Internet): ein Pop-up zur Registrierung und ein Pop-up zum Video-Posting (also zum Hochladen von Videos bei TikTok). Die Analyse des EDSA ergab, dass den jugendlichen Nutzenden bei beiden Pop-ups keine objektiven und neutralen Optionen präsentiert wurden.
Dazu stellte der EDSA fest: „Im Pop-up zur Registrierung wurden Kinder aufgefordert, sich für ein öffentliches Konto zu entscheiden, in dem sie rechts den Button (= Knopf) „skip“ wählen, was sich folglich auf die Privatsphäre des Kindes auf der Plattform auswirkt, indem beispielsweise Kommentare zu von Kindern erstellten Videoinhalten öffentlich angezeigt werden. Im Pop-up zum Video-Posting wurden die Kinder verleitet auf die Schaltfläche „Post Now“ (= lade es jetzt hoch) zu klicken, die sich in fetter, dunklerer Schrift auf der rechten Seite befindet, und nicht auf die unauffälligere gestaltete Schaltfläche „cancel“ (= abbrechen). Nutzer, die ihr Video nicht öffentlich machen wollten, mussten zunächst „cancel“ auswählen und dann nach den

Einstellungen zum Schutz der Privatsphäre suchen, um zu einem, „privaten Konto“ zu wechseln“ (siehe dazu: Nach Beschluss des EDSA wird TikTok zur Beseitigung unlauterer Gestaltungspraktiken in Bezug auf Kinder aufgefordert | European Data Protection Board (europa.eu).
Für den EDSA lag damit ein Verstoß gegen den Grundsatz der Verarbeitung nach Treu und Glauben (Artikel 5 Abs. 1 Buchstabe a) DS-GVO) vor. In die endgültige Entscheidung der irischen Datenschutzbehörde war diese rechtliche Beurteilung des EDSA aufzunehmen.
Zu den weiteren Aufgaben des EDSA: Er berät die Europäische Kommission, gibt Stellungnahmen ab und fördert den Austausch von Fachwissen über Datenschutzvorschriften und -praxis in aller Welt.
Aktuelle Themenfelder, mit denen sich der EDSA beschäftigt, sind zum Beispiel die Verabschiedung von Leitlinien zur Benutzung von Tracking-Techniken, die Einsetzungen einer Task Force zu ChatGPT sowie die Problematiken rund um Meta und dessen personalisierter Werbung (zum Beispiel die Ende Oktober 2023 ergangene Anweisung an die für Meta zuständige irische Aufsichtsbehörde, dass diese Meta verbietet, personenbezogene Daten ohne Einwilligung der Betroffenen für personalisierte Werbung zu verarbeiten).
Über die Rolle und wichtigen Aufgaben des EDSA kann man sich auch in einem englischsprachigen Video unter https://edpb.europa.eu/about-edpb/who-we-are/edpb-chairmanship_de informieren.
Zu Recht stellte Thüringens Datenschutzbeauftragter Dr. Lutz Hasse, anlässlich des europäischen Datenschutztages am 28. Januar 2024 Folgendes fest: „Der EDSA ist das höchste Gremium, um eine einheitliche Anwendung des Datenschutzrechts in Europa zu erzielen. Dieser institutionalisierte Ausschuss für eine europaweite Datenschutz-Harmonisierung genießt höchste Akzeptanz. Er schafft datenschutzrechtliche Sicherheit und stärkt damit die Europäer in ihrem Grundrecht auf informationelle Selbstbestimmung, das in Zeiten digitalen Umbruchs immer mehr an Bedeutung gewinnt.“ (siehe dazu die Pressemitteilung, abrufbar unter: https://tlfdi.de/fileadmin/tlfdi/presse/Pressemitteilungen_2023/240126_PM_Europ._Datenschutztag.pdf).

2. Fälle öffentlicher Bereich



Rathaus Architektur Gebäude - Pixabay

2.1 Müssen Polizisten für den Dienstherrn ständig erreichbar sein?

Keine beschäftigte Person muss grundsätzlich jeden Tag rund um die Uhr dem Arbeitgeber zur Verfügung stehen. Dennoch muss die Funktionsfähigkeit insbesondere der Polizei bei Gefahren gewährleistet sein. Daher können unter bestimmten Voraussetzungen für den Zweck der Alarmierung auch Erreichbarkeitsdaten wie private Handynummern verarbeitet werden.

Das Thüringer Ministerium für Inneres und Kommunales (TMIK) teilte dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) bereits Anfang 2022 mit, die Dienstanweisung zum Einsatz einer IT-Anwendung zum Zweck der Alarmierung des Gesamtpersonalbestands beziehungsweise von Teilkräften der Landespolizei solle geändert werden. Streitig war, ob die Beschäftigten verpflichtet werden konnten, ihre private Erreichbarkeit außerhalb der regulären Dienstzeiten zum Zweck der Alarmierung anzugeben, um private Handy-/Telefonnummern in dieser IT-Anwendung zu verarbeiten.
Eine Einwilligung der betroffenen Personen zur Verarbeitung ihrer Erreichbarkeit als Rechtsgrundlage für die Verarbeitung der privaten Erreichbarkeitsdaten (Handynummern) schien hierzu nicht geeignet.

Bekanntlich muss eine solche nicht abgegeben werden, denn sie ist nur dann wirksam, wenn sie freiwillig abgegeben wurde; und es war im Übrigen auch nicht damit zu rechnen, dass alle Beamten sie abgeben wollten. Darüber hinaus kann eine Einwilligung im Sinne des Art. 7 Datenschutz-Grundverordnung jederzeit widerrufen werden und die weitere Speicherung der privaten Telefonnummer ist dann nicht mehr zulässig.
Insbesondere zur Erfüllung der Aufgaben der Polizei, im Allgemeinen und im Besonderen bestehende Gefahren für die öffentliche Sicherheit und Ordnung abzuwehren, ist es erforderlich, dass die Funktionsfähigkeit der Polizei rund um die Uhr gewährleistet ist. Um im Falle einer Alarmierung ihrer Dienstverpflichtung zur rechten Zeit am rechten Ort nachkommen zu können, müssen die Polizeibeamten daher auch außerhalb der üblichen Dienstzeiten für den Dienstherrn erreichbar sein.
Als Alternative wurde diskutiert, dass für den Zweck der Erreichbarkeit Diensthandys zur Verfügung gestellt werden könnten. Diese Möglichkeit war seitens der Polizei abgelehnt worden, weil einerseits die Haushaltsmittel für die Ausstattung aller Polizeiangehörigen mit Diensthandys fehlten und andererseits damit dem Dienstherrn sehr viel intensivere Eingriffsmittel in die Rechte und Freiheiten der betroffenen Personen eröffnet gewesen wären. Denn die Polizeibediensteten wären zu verpflichten gewesen, das Diensthandy außerhalb anerkannter Abwesenheitszeiten wie Urlaub und Arbeitsunfähigkeit stets empfangsbereit zu halten, was praktisch einer ständigen Bereitschaft gleichgekommen wäre.
Eine Umfrage, wie in anderen Ländern die Alarmierung sichergestellt wird, ergab kein einheitliches Bild. In manchen Ländern sah man aus dem datenschutzrechtlichen Blickwinkel keine Probleme der Verarbeitung der privaten Erreichbarkeit, weil man diese für die Zwecke der Personalverwaltung und Einsatzsicherstellung aus den beamtenrechtlichen Vorschriften für zulässig erachtete, in anderen Ländern sah man keinerlei Zulässigkeit der Erfassung und Nutzung der privaten Handydaten der Polizeibediensteten, weil keine Rechtsgrundlage hierfür ersichtlich sei.
In Anbetracht der getroffenen technischen und organisatorischen Maßnahmen zum Schutz der betroffenen Polizeibediensteten in der Form, dass die Zugriffsmöglichkeit auf die gespeicherten privaten Erreichbarkeiten mit enger Zweckbindung auf wenige Personen be-

schränkt und ein Zugriff auch nur dann ermöglicht wird, wenn die Person tatsächlich zur Verfügung steht und sich nicht im Urlaub oder Krankenstand befindet, konnte die vorgesehene Vorgehensweise schließlich akzeptiert werden.

2.2 „Buttersäure-Gate“: Herausgabe von Kundendaten an die Polizei aufgrund eines Durchsuchungsbeschlusses

Ein Durchsuchungsbeschluss ist eine Entscheidung im Rahmen der Ausübung der richterlichen Unabhängigkeit. Er kann gemäß § 2 Abs. 9 Satz 2 ThürDSG nicht mit einer datenschutzrechtlichen Beschwerde angegriffen werden.

Ein Händler teilte dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) mit, das Landeskriminalamt Thüringen habe im Rahmen der Aufklärung eines Anschlages unter Verwendung von Buttersäure die Herausgabe der personenbezogenen Daten von 200.000 seiner Kunden verlangt. Er habe sie zwar der Polizei übergeben, aber gleichzeitig Beschwerde eingelegt, weil auch 60.000 personenbezogene Daten der Kunden von Verkäufen nach dem Anschlag herausverlangt worden waren. Zudem seien auch österreichische Kunden betroffen. Er gehe davon aus, dass die Verwendung der Kundendaten rechtswidrig und nicht datenschutzkonform sei.
Aus den dem TLfDI vorgelegten Unterlagen ergab sich, dass das zuständige Amtsgericht die Durchsuchung der Wohn- und Geschäftsräume des Händlers angeordnet hatte. Seine Beschwerde gegen den Durchsuchungsbeschluss des Amtsgerichts verwarf das zuständige Landgericht als unbegründet.
Der TLfDI nimmt gemäß § 6 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) gegenüber öffentlichen Stellen die Aufgaben gemäß Art. 57 der Datenschutz-Grundverordnung (DS-GVO) wahr. Er kontrolliert die Einhaltung der DS-GVO, des ThürDSG und anderer datenschutzrechtlicher Bestimmungen. Gemäß § 6 Abs. 2 ThürDSG überwacht er auch die Einhaltung von im Rahmen des Anwendungsbereichs der Richtlinie 2016/680 (JI-Richtlinie) erlassenen Rechtsvorschriften, hier unter anderem des 3. Abschnitts des ThürDSG. Er ist gemäß § 3 Abs. 1 Nr. 3a Thüringer Verwaltungsverfahrensgesetz für die öffentlichen Stellen des Freistaates Thüringen örtlich zuständig. Da der Händler einem Thüringer Landgericht sowie dem Landeskri-

minalamt Thüringen einen Datenschutzverstoß vorwarf und beide öffentliche Stellen des Freistaats Thüringen sind, bestand auch für die Kundendaten aus Österreich die ausschließliche örtliche Zuständigkeit des TLfDI.
Die Prüfung des TLfDI ergab, dass der vom Händler mitgeteilte Sachverhalt nicht gegen das Datenschutzrecht verstößt beziehungsweise die Zuständigkeit des TLfDI nicht gegeben ist.
Eine unrechtmäßige Verarbeitung personenbezogener Daten durch das Landeskriminalamt Thüringen konnte der TLfDI nicht feststellen. Die Sicherstellung der Kundendaten erfolgte durch die für den Wohn- und Geschäftssitz des Händlers zuständige Polizei. Eine unrechtmäßige Verarbeitung personenbezogener Daten war dabei nicht feststellbar, weil die Sicherstellung der Kundendaten auf dem Durchsuchungsbeschluss des zuständigen Amtsgerichts beruhte. Die Übermittlung der Kundendaten von der Polizei am Wohn- und Geschäftssitz des Händlers an das Landeskriminalamt Thüringen war ebenfalls rechtmäßig, weil das Landeskriminalamt Thüringen die zuständige Ermittlungsbehörde war.
Die Durchsicht, das Auslesen und die Verwendung der auf einem Medium gespeicherten personenbezogenen Daten durch das Landeskriminalamt Thüringen stellte eine Verarbeitung gemäß § 32 Nr. 2 ThürDSG dar. Gemäß § 31 Abs. 1 ThürDSG ist die Verarbeitung personenbezogener Daten zulässig, wenn sie für die Aufgabenerfüllung zu den in § 31 ThürDSG genannten Zwecken erforderlich ist und keine spezielleren Regelungen in anderen Gesetzen vorgehen. § 31 ThürDSG legt als Zwecke die Erfüllung der Aufgaben der Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Straftaten oder Ordnungswidrigkeiten fest.
Die Sicherstellung, Durchsicht und weitere Verarbeitung der personenbezogenen Daten der Kunden durch das Landeskriminalamt Thüringen diente zweifelsohne der Ermittlung und Verfolgung einer Straftat, nämlich eines Buttersäure-Brandanschlags, strafbar nach § 306 Abs. 1 Nr. 1 Strafgesetzbuch. Dass dabei personenbezogene Daten von Kunden verarbeitet wurden, die über das Anschlagsdatum hinaus Ware bei dem Händler erwarben, schließt Ermittlungen im Zusammenhang mit dem Anschlag grundsätzlich nicht aus.
Es ergab sich keinerlei Hinweis, dass die personenbezogenen Daten der Kunden seitens des Landeskriminalamtes Thüringen nicht daten-

schutzkonform behandelt wurden. Daher sah der TLfDI keine Veranlassung für ein datenschutzaufsichtliches Einschreiten gegenüber dem Landeskriminalamt Thüringen.
Die Überprüfung, ob tatsächlich alle Kundendaten – auch über das Anschlagsdatum hinaus – für die Ermittlungen erforderlich waren, oblag nicht dem TLfDI. Vielmehr waren hierüber bereits zwei gerichtliche Entscheidungen ergangen. Der TLfDI ist gemäß § 2 Abs. 9 S. 2 ThürDSG für die Gerichte nur zuständig, soweit diese in Verwaltungsangelegenheiten tätig werden.
Das zuständige Amtsgericht überprüfte den Sachverhalt aufgrund der Beschwerde des Händlers gegen den Durchsuchungsbeschluss. Dem Beschluss des Amtsgerichts war auch nicht zu entnehmen, dass es Zweifel an der Erforderlichkeit der Sicherstellung der Kundendaten über das Anschlagsdatum hinaus gehabt hätte. Vielmehr half das Amtsgericht der Beschwerde nicht ab und legte sie zur Entscheidung dem zuständigen Landgericht vor. Auch das Landgericht überprüfte den Sachverhalt und schränkte den Zeitraum für die Sicherstellung der Kundendaten nicht ein. Es verwarf die Beschwerde des Händlers als unbegründet. Beide Gerichte trafen ihre Entscheidungen im Rahmen der Ausübung ihrer richterlichen Unabhängigkeit und nicht im Rahmen einer Verwaltungstätigkeit. Damit unterlagen sie nicht der datenschutzrechtlichen Aufsicht des TLfDI.

2.3 Übermittlung von Personalaktendaten an den Untersuchungsausschuss 7/4

Die Landesregierung ist verpflichtet, dem Parlament auch personenbezogene Angaben zu übermitteln, soweit dies für die Aufgabenerfüllung eines Untersuchungsausschusses erforderlich ist. Die für einen Untersuchungsauftrag nicht erforderlichen Angaben sind zu schwärzen oder zu pseudonymisieren. Das Parlament muss in eigener Zuständigkeit gegebenenfalls die erforderlichen technischen und organisatorischen Maßnahmen zum Schutz der betroffenen Personen treffen.

Für einigen Wirbel sorgte der Bericht des Thüringer Rechnungshofs zur Einstellungspraxis der Landesregierung bei Staatssekretärinnen und Staatssekretären sowie bei persönlichen Mitarbeitern in den Leitungsbereichen der Ministerien und der Staatskanzlei. In seiner Sitzung am 28. April 2023 hatte der Thüringer Landtag daher die Einsetzung eines Untersuchungsausschusses beschlossen, der ein mögliches

Fehlverhalten der Landesregierung bei der Besetzung öffentlicher Ämter bei Staatssekretärinnen und Staatssekretären sowie Stellen in den Leitungsbereichen der Ministerien und der Staatskanzlei prüfen soll (kurz: „Untersuchungsausschuss Postenaffäre“; Drucksache 7/7914 vom 29. April 2023).
In seiner ersten Sitzung im Juli 2023 forderte der Untersuchungsausschuss die Landesregierung auf, bis Mitte September bestimmte Bestandteile der Personalakten der betroffenen Bediensteten nebst den zugehörigen Sachakten, insbesondere Stellenausschreibungen, Auswahlverfahren und Stellenbewertungen vorzulegen. Kurz darauf erreichten den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erste Beschwerden von betroffenen Personen, nachdem die Ressorts die Betroffenen in unterschiedlicher Form von einer beabsichtigten Übersendung der Personalaktendaten unterrichtet hatten. Dies reichte von dem Angebot, in die zu übersendenden Unterlagen Einsicht zu nehmen, über die Frage der Einwilligung in die Übersendung bis hin zu der Information, man könne vor dem Verwaltungsgericht auch Klage erheben.
Zur Klarstellung: Gemäß § 2 Abs. 6 Sätze 3 und 4 Thüringer Datenschutzgesetz (ThürDSG) unterliegt die Verarbeitung personenbezogener Daten bei der Wahrnehmung parlamentarischer Aufgaben durch den Landtag nicht dem ThürDSG. Der Landtag hat danach eine Datenschutzordnung erlassen. Im Berichtszeitraum war der TLfDI davon ausgegangen, dass er nicht dafür zuständig ist, den Untersuchungsausschuss zu überprüfen oder zu kontrollieren und dass das Parlament die Einhaltung der datenschutzrechtlichen Vorgaben selbst sicherzustellen hat[1].
Jedoch untersteht die Landesregierung bei ihrer Tätigkeit der datenschutzrechtlichen Aufsicht des TLfDI und ist an die Vorgaben der Datenschutz-Grundverordnung (DS-GVO) und der geltenden Datenschutzgesetze gebunden. Eine Übermittlung an den Untersuchungsausschuss darf nur erfolgen, wenn es dafür eine Rechtsgrundlage gibt, Art. 5 Abs. 1 Buchstabe a) DS-GVO in Verbindung mit Art. 6 Abs. 1

[1] Der EuGH hat am 16. Januar 2024 in der Rechtssache C-22/22 entschieden, dass ein parlamentarischer Untersuchungsausschuss grundsätzlich die DS-GVO einhalten muss. Gibt es in diesem Mitgliedstaat nur eine Aufsichtsbehörde, ist diese grundsätzlich auch für die Überwachung der Einhaltung der DS-GVO durch den Untersuchungsausschuss zuständig. Der TLfDI wird die Bedeutung dieser Entscheidung für Thüringen mit dem Thüringer Landtag klären und im nächsten Tätigkeitsbericht über das Ergebnis berichten.

Satz 1 Buchstabe a) bis e) DS-GVO. Nach § 2 Abs. 7 ThürDSG darf die Landesregierung personenbezogene Daten, die für andere Zwecke erhoben worden sind, zur Beantwortung parlamentarischer Anfragen sowie zur Vorlage von Unterlagen und Berichten im Rahmen der Geschäftsordnung des Thüringer Landtags **in dem dafür erforderlichen Umfang** verwenden. Diese Regelung trägt dem im Datenschutz wesentlichen Grundsatz der Erforderlichkeit Rechnung, nach dem auch bei bestehender Rechtsgrundlage eine Verarbeitung personenbezogener Daten nur im Rahmen der Erforderlichkeit zulässig ist.
Maßstab für die Erforderlichkeit der Übermittlung ist der Beschluss zur Einsetzung des Untersuchungsausschusses in der Drucksache 7/7914. Es kann nicht davon ausgegangen werden, dass die Anforderung des Untersuchungsausschusses allein bereits eine Datenübermittlung rechtfertigt. Dem steht die Bestimmung des § 2 Abs. 7 ThürDSG entgegen.
Der Untersuchungsausschuss hat nach dem Einsetzungsbeschluss die Aufgabe, mögliche Versäumnisse, Fehleinschätzungen und mögliches Fehlverhalten der Landesregierung bei der Ernennung beziehungsweise Einstellung von Staatssekretärinnen und Staatssekretären sowie bei der Besetzung von Stellen von persönlichen Mitarbeitern in den Leitungsbereichen der Ministerien und der Staatskanzlei zu untersuchen (I. des Einsetzungsbeschlusses). Auch soll untersucht werden, ob und wenn ja, in welchem Umfang und in welchen konkreten Einzelfällen die seit dem 30. Oktober 2009 im Amt befindlichen Landesregierungen gegen die Vorgaben des Grundsatzes der Bestenauslese nach Art. 33 Abs. 2 des Grundgesetzes in Verbindung mit den einschlägigen beamten-, laufbahn-, tarif- und haushaltsrechtlichen Regelungen sowie den Grundsatz der Wirtschaftlichkeit und Sparsamkeit bei der Besetzung von Stellen von persönlichen Mitarbeitern (Büroleitern, Grundsatzreferenten, persönlichen Referenten sowie Leitern für Presse- und Öffentlichkeitsarbeit) in den Leitungsbereichen der Ministerien und der Staatskanzlei verstoßen haben (II. des Einsetzungsbeschlusses).
Für die Erfüllung dieser Aufgabe bedurfte es nach Auffassung des TLfDI zum damaligen Stand nur der Übersendung von Sachakten zu Auswahlverfahren. Gegenstand der Untersuchung ist die „Ernennung beziehungsweise Einstellung“ beziehungsweise die „Besetzung von Stellen“. Daher geht es nicht um die Überprüfung der betroffenen Bediensteten, sondern um die Untersuchung der jeweiligen Verfahren, die ihrer Einstellung oder Dienstpostenzuweisung zugrunde liegen.

Der TLfDI sah sich im Hinblick auf die Dringlichkeit wegen der kurzfristig anstehenden Übersendung der Personalunterlagen an den Thüringer Landtag veranlasst, vorsorglich eine Warnung nach Art. 58 Abs. 2 Buchstabe a) DS-GVO an die Adresse der Ressorts auszusprechen, die Personalakten ohne Prüfung der Erforderlichkeit der Übermittlung an den Untersuchungsausschuss zu übersenden, weil dies einen Verstoß gegen Art. 5 Abs. 1 Buchstabe a) DS-GVO darstellen würde und bot im Einzelfall Beratung an über den Umfang der zulässigen Übermittlung, Art. 57 Abs. 1 Buchstabe c) DS-GVO. Eine Warnung nach Art. 58 Abs. 2 Buchstabe a) DS-GVO ist dann angezeigt, wenn eine Datenverarbeitung beabsichtigt ist, die voraussichtlich einen Verstoß gegen die Datenschutz-Grundverordnung darstellt und der Verstoß noch nicht stattgefunden hat. Sie soll einen drohenden Verstoß verhindern.
Ein anschließendes Gespräch mit Vertretern der Ressorts in der Thüringer Staatskanzlei und weitere Erörterungen der Sach- und Rechtslage zeigten, dass man es sich in den Ressorts nicht leicht gemacht hatte und anhand der verfügbaren Rechtsprechung des Bundesverfassungsgerichts (2 BvE 3/07) und des Bundesverwaltungsgerichts (6 VR 2.22) sowie Literatur hierzu (Peters in NVwZ 2020, 1550 ff.) zur Vorlageverpflichtung intensiv geprüft hatte, wie man dem Vorlagebegehren des Parlaments pflichtgemäß nachkommen und andererseits die Schutzrechte der betroffenen Personen als Beschäftigte oder ehemalige Beschäftigte wahren kann. Einigkeit bestand darin, dass die Angaben, die für den Untersuchungsausschuss in Wahrnehmung seiner Aufgaben nicht erforderlich waren, zu schwärzen sind. Dies betraf vor allem Daten Dritter in den Personalakten und besondere Kategorien von personenbezogenen Daten nach Art. 9 DS-GVO, wie beispielsweise Gesundheitsdaten. Die Namen der betroffenen Personen wurden pseudonymisiert, um gegebenenfalls auf den Einzelfall rückführen zu können, falls dies für den Untersuchungsauftrag erforderlich sein sollte. Dabei war man davon ausgegangen, dass die Personen, die in der Öffentlichkeit stehen und standen, auch namentlich genannt werden konnten. Dies betraf Staatssekretärinnen und Staatsekretäre, weil die Beantwortung der Frage, wer wann in welchem Ministerium Staatssekretär war, quasi offenkundig ist und deren Lebensläufe und Werdegänge ohnehin allgemein zugänglich waren. Im Weiteren zeigte sich allerdings, dass möglicherweise im Fall von bereits ausgeschiedenen Staatssekretärinnen und Staatsekretären, die nicht mehr im

Rampenlicht standen und auf die bei der Erörterung ihrer personenbezogenen Daten insbesondere in öffentlicher Sitzung des Untersuchungsausschusses besonderer öffentlichkeitswirksamer Fokus fallen würde, ebenfalls eine Pseudonymisierung vorgenommen werden sollte. Es ist nun jedoch Sache des Parlaments, zu prüfen, inwieweit personenbezogene Daten in den öffentlichen Sitzungen zulässigerweise erörtert werden können.

2.4 Kennzeichenerfassung auf dem Parkplatz eines bekannten Thüringer Ausflugszieles

Immer wieder erfährt der TLfDI erst aus den Medien neue und interessante, datenschutzrechtlich zu bewertende Vorgänge. Die in öffentlicher Hand stehende Betreiberin des Parkplatzes an einem beliebten touristischen Ausflugsziel hatte sich von den Werbeversprechen eines Unternehmens für automatische Erfassungs- und Abrechnungssysteme überzeugen lassen. Es wurde ein System installiert, welches die Kennzeichen der einfahrenden Fahrzeuge mittels Videotechnik erfasst und die Abrechnung des Parkvorganges über eine Eingabe desselben übernimmt. Datenschutzrechtlich wurde der TLfDI hier vor einige Herausforderungen gestellt.

Nur einem Artikel aus der Zeitung ist es zu verdanken, dass in zweijähriger intensiver Arbeit die auf einem Parkplatz installierte automatische Kraftfahrzeug (KFZ)-Parkplatzanlage auf datenschutzrechtlich sichere Füße gestellt wurde.
Dabei war die Grundidee der Betreiberin, einen deutlich störungsfreieren und wenig Stau verursachenden Betrieb zu gewährleisten, absolut verständlich. Beim bisherigen auf einem Papierticket basierten Betrieb mit einer Schrankenanlage kam es immer wieder zu langen Rückstaus auf die Landstraße und damit regelmäßig zu gefährlichen Verkehrssituationen. Durch die nun mögliche Zu- und Ausfahrt ohne Schranke sollte der Ein- und Ausfahrtsprozess auf dem Parkplatz beschleunigt werden. Auch der Wegfall der Tickets mit Magnetstreifen und die einfache Abrechnung über das eigene KFZ-Kennzeichen sollte die Nutzung vereinfachen. Zudem hat der Anbieter eine Zahlungsmöglichkeit per App vorgesehen. Grundsätzlich ist der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) bei solchen gebührenpflichtigen Parkplatzanlagen immer für einen Betrieb **mit** Schranken. Diese können wirksam verhindern,

dass Nutzer eines Parkplatzes ohne Schranke, welche nur vergessen haben zu zahlen, mit erheblichen Nachforderungen wegen unberechtigter Nutzung konfrontiert werden. Im hier vorliegenden Fall betrugen diese mindestens 40 Euro. Ob die Möglichkeit, durch Wegfall der Schranken höhere Einnahmen zu generieren, zum Geschäftskonzept des Anbieters gehört, hatte der TLfDI dabei nicht zu bewerten.
Gleich zu Beginn der Prüfung war dem TLfDI eine unzureichende Beschilderung der Kennzeichenerfassung aufgefallen. Der Hinweis auf die automatische Kennzeichenerfassung mittels Videokameras erfolgte erst nach der Einfahrt zum Parkplatz. Wenn ein Autofahrer sein Kennzeichen nicht erfassen lassen wollte, konnte sich dieser nur durch Zurücksetzen seines Wagens auf die belebte Kreisstraße der Erfassung entziehen. Dies konnte dann offensichtlich zur Gefährdung Dritter führen und den Verkehrsfluss beeinträchtigen. Eine Wendemöglichkeit konnte baulich nicht eingerichtet werden, sodass der TLfDI den Betreiber auffordern musste, die Verkehrsteilnehmer rechtzeitig auf die automatische Kennzeichenerfassung hinzuweisen. In diesem Zusammenhang kam aber dann auch die Straßenverkehrsbehörde ins Spiel: Diese musste die Beschilderung, welche nach Auffassung des TLfDI mindestens 200 Meter vor dem Parkplatz angebracht werden sollte, genehmigen. Bislang konnte zumindest eine Beschilderung mit dem Hinweis auf die Kennzeichenerfassung in einem Abstand von ungefähr 50 bis 80 Metern angebracht werden. Der TLfDI stand bis zum Redaktionsschluss dieses Tätigkeitsberichts noch mit der Verkehrsbehörde im Austausch, eine weitere Beschilderung auch an noch weiter vorgelagerten bereits vorhandenen Parkhinweisen zu veranlassen.
Die Kameraerfassung der KFZ-Kennzeichen als solche war datenschutzrechtlich nicht zu beanstanden. Hier erfolgte tatsächlich nur die Aufnahme des Kennzeichens selbst und nicht der Fahrzeuginsassen.
In puncto der notwendigen Datenminimierung durch kurze Speicherfristen konnte der TLfDI nach erfolgten Hinweisen und Korrektur durch die Betreiberin kurzfristig regulierend eingreifen.
Als problematisch erwiesen sich jedoch die an die Videoaufnahme anschließenden Verarbeitungsvorgänge der KFZ-Kennzeichenerfassung und der Abrechnung des Parkvorganges. In diese Vorgänge waren und sind neben der Betreiberin und dem eigentlichen Anbieter der Anlage noch mehrere weitere Unternehmen für bestimmte Park- und/oder Abrechnungsvorgänge eingebunden. So erfolgt beispielsweise die Abrechnung normaler Benutzungen des Parkplatzes, also Einfahrt/Bezahlung/Ausfahrt über ein Unternehmen, während die unzulässige

Nutzung, Einfahrt/Nichtzahlung/Ausfahrt von einem anderen Unternehmen verfolgt werden soll. Für die Zahlung der Parkgebühren über eine App wird wieder eine dritte, andere Firma einbezogen. Hier musste der TLfDI die besondere Verantwortlichkeit für jeden einzelnen Verarbeitungsvorgang intensiv prüfen.
Soweit diese dann festgestellt war, mussten im nächsten Schritt die sogenannten Auftragsverarbeitungsvorgänge geprüft werden. Soweit sich ein für die Datenverarbeitung Verantwortlicher weiterer Verarbeiter als Dienstleister bedient, sind mit diesen besondere Verträge abzuschließen, welche sicherstellen, dass auch von diesen alle datenschutzrechtlichen Vorschriften eingehalten werden. In der Folge mussten dann nach den datenschutzrechtlichen Hinweisen des TLfDI mehrere Verträge mit neuen Formulierungen und geänderten Inhalten geschlossen werden. Zwangsläufig ergab sich dann noch die Notwendigkeit, die nach Art. 12 und 13 Datenschutz-Grundverordnung datenschutzrechtlich notwendigen Hinweisschilder für die Nutzer des Parkplatzes neu zu fassen und zu installieren. Auch dies wurde dann den Vorgaben des TLfDI entsprechend von der Betreiberin umgesetzt.
Es muss in diesem Zusammenhang betont werden, dass sich die Betreiberin des Parkplatzes im gesamten Verfahren sehr kooperativ gezeigt hat. Dieser war offensichtlich die erhebliche datenschutzrechtliche Problematik vor dem Eingreifen des TLfDI nicht bewusst. Sämtliche Änderungen der Hinweise, an der Beschilderung sowie bezüglich der vertraglichen Vereinbarungen folgten dabei stets zeitnah.

2.5 Offenlegung eines Kfz-Kennzeichens auf einem „Knöllchen“ ist zulässig

Die Offenlegung eines Kfz-Kennzeichens auf einem sogenannten Strafzettel („Knöllchen“) stellt keinen Verstoß gegen den Datenschutz dar. Beim Kfz-Kennzeichen handelt es sich um ein personenbezogenes Datum gemäß § 32 Abs. 1 ThürDSG, daher ist die Offenlegung und somit die Verarbeitung des Kfz-Kennzeichens aufgrund von § 33 Abs. 1 ThürDSG zulässig, wenn beides für die Aufgabenerfüllung zu den in § 31 ThürDSG genannten Zwecken erforderlich ist.

Im Berichtszeitraum erreichte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) eine Beschwerde, in der es um die Offenlegung eines sogenannten Strafzettels (im Volksmund: „Knöllchen“) an der Windschutzscheibe eines

rechtswidrig geparkten Autos ging. Der Beschwerdeführer war der Ansicht, dass die Offenlegung des Knöllchens an der Windschutzscheibe und damit die Offenlegung seines Kfz-Kennzeichens einen Verstoß gegen den Datenschutz darstellt. Der TLfDI musste ihm jedoch im Ergebnis mitteilen, dass die Ordnungshüter keinen Verstoß begangen hatten und dass das „Knöllchen“ an der Windschutzscheibe auch auf der Grundlage des Datenschutzrechts rechtens war. Das ist auch dann der Fall, wenn das Kfz-Kennzeichen auf dem „Knöllchen“ ersichtlich ist.

Im hier vorliegenden Sachverhalt richtete sich die Verarbeitung der personenbezogenen Daten nicht nach der Datenschutz-Grundverordnung (DS-GVO), sondern nach der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates, die in den §§ 31 ff. im ThürDSG umgesetzt wurde.

Gemäß § 31 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) gelten die Bestimmungen dieses Abschnitts für die Verarbeitung personenbezogener Daten durch die für die Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Straftaten oder Ordnungswidrigkeiten zuständigen öffentlichen Stellen, soweit sie Daten zum Zweck der Erfüllung dieser Aufgaben verarbeiten. Die öffentlichen Stellen gelten dabei als Verantwortliche. Die Verhütung von Straftaten umfasst den Schutz vor und die Abwehr von Gefahren für die öffentliche Sicherheit.

Die Verarbeitung personenbezogener Daten ist zulässig, wenn diese Verarbeitung für die Aufgabenerfüllung zu den in § 31 ThürDSG genannten Zwecken erforderlich ist und keine spezielleren Regelungen in anderen Gesetzen vorgehen (§ 33 Abs. 1 ThürDSG).

Die Ordnungsbehörden sind gemäß § 2 Nr. 1 Thüringer Verordnung über Zuständigkeiten für die Verfolgung und Ahndung von Verkehrsordnungswidrigkeiten zuständig im übertragenen Wirkungskreis für die Verfolgung und Ahndung von Ordnungswidrigkeiten.

Gemäß § 32 Nr. 1 ThürDSG sind personenbezogene Daten alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (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. Amtliche Kfz-Kennzeichen können mittels einer Auskunft beim Kraftfahrtbundesamt identifiziert werden und stellen somit personenbezogene Daten im Sinne des § 32 Nr. 1 ThürDSG dar.
Zurück zum Ausgangsfall: Die Verarbeitung war hier gemäß § 33 Abs. 1 ThürDSG erforderlich, da das Auto ordnungswidrig abgestellt wurde und das „Knöllchen" den angemessenen Eingriff der dafür erforderlichen Sanktionierung dargestellt hat. Das „Knöllchen" wurde dabei so angebracht, dass es für die vorbeilaufenden Passanten nicht direkt einsehbar war. Des Weiteren war das Auto im Straßenverkehr ordnungswidrig abgestellt worden, sodass jeder, der am Straßenverkehr teilnahm, erkennen konnte, dass mit dem Auto und dem damit verbundenen (sichtbaren) Kfz-Kennzeichen eine Ordnungswidrigkeit begannen wurde.
Im Ergebnis konnte der TLfDI daher keinen Verstoß seitens der Ordnungsbehörde feststellen, da das „Knöllchen" und somit die Offenlegung des Kfz-Kennzeichens zulässig waren.

2.6 Geordnete wirtschaftliche Verhältnisse?

Zur Einstellung im öffentlichen Dienst darf nicht von allen in Frage kommenden Bewerbern eine Erklärung über bestehende Schulden und die wirtschaftlichen Verhältnisse verlangt werden. Eine solche Erklärung zu den wirtschaftlichen Verhältnissen kann nur in den Fällen verlangt werden, in denen die zu besetzende Stelle eine besondere Vertrauenswürdigkeit in finanziellen Fragen voraussetzt.

Einer Anfrage zufolge sollten Beschäftigte im Geschäftsbereich einer obersten Landesbehörde bei Einstellung eine Erklärung abgeben, dass sie keine Schulden haben oder nur Schulden, denen entsprechende Vermögenswerte gegenüberstehen und dass ihre wirtschaftlichen Verhältnisse geordnet sind. Das hierzu verwendete Formular, das dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) zur Verfügung gestellt wurde und von Beschäftigten zu unterzeichnen war, enthielt keine Hinweise darauf, zu welchem konkreten Zweck die Angaben benötigt und verarbeitet werden, noch war zu entnehmen, was unter „geordneten wirtschaftlichen Verhältnissen" zu verstehen ist.
Auf Nachfrage des TLfDI, von welchen Beschäftigten auf welcher Rechtsgrundlage die Erklärung verlangt werde, für welchen konkreten

Zweck die Angaben verarbeitet und ob sie auch aktualisiert werden, führte der Verantwortliche aus, die entsprechende Erklärung werde von allen Bewerbern um eine Stelle im Bereich des Ressorts erbeten, damit die persönliche Eignung der Bewerber als Voraussetzung zur Übernahme in das Beschäftigungsverhältnis geprüft werden könne. Geordnete wirtschaftliche Verhältnisse bildeten eine wesentliche Grundlage für die Frage der Eignung eines Beamten. Der Begriff der persönlichen Eignung umfasse neben den geistigen Anlagen und der körperlichen und gesundheitlichen Eignung auch die charakterliche Eignung und die Persönlichkeit eines Bewerbers. Dies sei unter anderem auch für die Achtung und das Vertrauen in die Person und die Amtsführung von Bedeutung. Für Nicht-Beamte gelte das gleichermaßen, in der arbeitsrechtlichen Literatur und Rechtsprechung sei insoweit anerkannt, dass die Frage nach den Vermögensverhältnissen dann zulässig ist, wenn für die zu besetzende Stelle ein besonderes Maß an Vertrauen gefordert sei. Die Gefahr der Bestechung sei im Ressort jedenfalls gegeben.

Der TLfDI hielt diese Begründung nicht für ausreichend. Zur Berufung in das Beamtenverhältnis kann aufgrund der Anforderungen an einen Bewerber auch dessen wirtschaftliche Situation einbezogen werden. Für Beschäftigte im Angestellten-, Arbeits- und Ausbildungsverhältnis zu einer öffentlichen Stelle gilt dies allerdings nicht zwingend. Zwar sind auf diese Bewerber über Art. 88 Datenschutz-Grundverordnung (DS-GVO), § 27 Thüringer Datenschutzgesetz (ThürDSG) die §§ 79 bis 87 Thüringer Beamtengesetz (ThürBG) entsprechend anzuwenden, es sei denn, besondere Rechtsvorschriften oder tarifliche Regelungen gingen dem vor. Insoweit ist hier den Grundsätzen des Arbeitsrechts zu folgen, nach denen die privaten Vermögensverhältnisse grundsätzlich „tabu“ sind. Überschuldung und hohe Unterhaltsansprüche dürfen nur dann erfragt werden, wenn der in Aussicht genommene Arbeitsplatz beträchtliche finanzielle Spielräume eröffnet oder tatsächlich eine Anfälligkeit für Korruption bietet (vergleiche Däubler in: Däubler/Wedde/Weichert/Sommer, EU-Datenschutzgrundverordnung und BDSG-neu, Kompaktkommentar 2018 zu § 26 BDSG RN. 23). Insoweit kann zumindest von nicht zu verbeamtenden Bewerbern nicht ausnahmslos abgefragt werden, ob sie in geordneten Vermögensverhältnissen leben.

Zu Zweck und Rechtsgrundlage der Verarbeitung der Bewerberdaten verwies der Verantwortliche auf die Bediensteten-Information im Intranet. In den Hinweisen für die Bewerber fanden sich allerdings keine

Hinweise darauf, was unter „geordneten“ wirtschaftlichen Verhältnissen zu verstehen ist. Insoweit war eine subjektive Deutung durch die Bewerber und den potentiellen Arbeitgeber möglich und damit die Geeignetheit der Erhebung der Angaben für die genannten Zwecke erheblich in Frage gestellt.
Nochmals zur Notwendigkeit der Angaben der wirtschaftlichen Verhältnisse durch Bewerber auf Stellen außerhalb des Beamtentums befragt, legte der Verantwortliche dar, Überschuldung und hohe Unterhaltsansprüche dürften vom Arbeitgeber nachgefragt werden, weil es im Blick auf eine angemessene Verwendung der Beschäftigten und der sich im steten Wandel befindlichen Aufgabengebiete notwendig sei, bereits im Vorfeld einer Einstellung von jedem Bewerber die Erklärung über persönliche wirtschaftliche Verhältnisse einzuholen.
Abgesehen davon, dass zweifelhaft ist, ob nahezu alle Bediensteten im Laufe ihrer Tätigkeit im Geschäftsbereich Verantwortung für Finanzgeschäfte tragen oder eine leitende Funktion übernehmen werden, muss nach Auffassung des TLfDI beachtet werden, dass die „Erforderlichkeit“ im Sinne einer strikten Verhältnismäßigkeitsprüfung zu sehen ist. Eine Erklärung zum Zeitpunkt der Einstellung, die nicht aktualisiert wird (weil hierfür auch keine pauschale Rechtgrundlage besteht), verliert im Laufe der Beschäftigung an Aussagekraft, sodass sie für den herangezogenen Zweck nicht dauerhaft geeignet ist.
Auch für Beamtenbewerber stellt § 79 Abs. 1 ThürBG eine gesetzliche bereichsspezifische Datenschutzregelung dar, die dem Dienstherrn ein Fragerecht nur insoweit zugesteht, als die Beantwortung seiner Fragen zur Begründung des Beamtenverhältnisses erforderlich ist. Mit Blick auf die Ausübung hoheitlicher Befugnisse und das besondere Dienst- und Treueverhältnis des Beamten zum Staat kann in die Eignungsprüfung zwar auch die wirtschaftliche Situation des Bewerbers einbezogen werden. Der Prüfungsmaßstab ist aber auch hier an den Anforderungen auszurichten, die das Amt im konkret-funktionellen Sinne stellt (Münch/Kunig/*Bickenbach*, GG-Kommentar, Art. 33 RN 69). Die vom Verantwortlichen herausgestellte Pflicht zu einem außerdienstlich vertrauensvollen Verhalten nach § 34 Abs. 1 Satz 3 Beamtenstatusgesetz (BeamtStG) erwartet von Beamten kein wesentlich anderes Sozialverhalten als von anderen Bürgern und stellt ansonsten auf die Erfüllung der dem Beamten konkret obliegenden Dienstpflichten ab (Brinktrine/Schollendorf/*Werres*, BeckOK Beamtenrecht Bund, § 34 BeamtStG RN 15 f.; *Reich*, BeamtStG-Kommentar, § 9 RN 12). Erfordert das Amt keine besondere Zuverlässigkeit

beim Umgang mit Geld, ist die leichtsinnige Begründung von Schuldverpflichtungen als solche noch keine Pflichtverletzung, selbst wenn sich der Beamte in der Folgezeit als schlechter Schuldner erweist (vergleiche BVerwG, Urteil vom 22. April 1991 – 1 D 62/90 = BVerwGE 93, 78). Demgemäß kann auch von Beamtenbewerbern nicht in jedem Fall eine Erklärung über die persönlichen wirtschaftlichen Verhältnisse eingeholt werden.
Ist die Frage nach den Vermögensverhältnissen der Sache nach zulässig, muss der Betroffene in der Lage sein, selbstbestimmt über die Verwendung seiner Daten zu befinden. Soll ein Bewerber erklären, dass er sich in geordneten wirtschaftlichen Verhältnissen befindet, wird nicht nur auf einen auslegungsbedürftigen, sondern auf einen zudem wertungsabhängigen Begriff zurückgegriffen (BVerwG, Urteil vom 17. August 2005 – 6 C 15/04 = NJW 2005, 3795, 3796; *Bleutge*, DS 2020, 72, 73 ff.), der mit Blick auf den Grundsatz der Transparenz (Art. 5 Abs. 1 Buchstabe a) Variante 3 DS-GVO) einer Konkretisierung bedarf. Sind Schulden vorhanden, denen keine realisierbaren Vermögenswerte gegenüberstehen, liegen ungeordnete Vermögensverhältnisse vor, wenn der Betroffene außerstande ist, in absehbarer Zeit seinen laufenden Verpflichtungen nachzukommen (BGH, Beschluss vom 22. März 2004 – NotZ 23/03 = NJW 2004, 2018, 2019). Hierzu könnte nach dem Vorbild im beruflichen Satzungsrecht auf relevante Tatbestände Bezug genommen werden, etwa, dass keine Lohnpfändungen oder -abtretungen erfolgt sind, der Bewerber keine Vermögensauskunft nach § 802c Zivilprozessordnung (frühere eidesstattliche Versicherung) abgegeben hat oder kein privates Insolvenzverfahren eröffnet wurde (vgl. *Gola*/Heckmann, BDSG-Kommentar, § 26 RN 40; Muster-Sachverständigenordnung des DIHK, Ziff. 3.2.6).
Nachdem hierzu keine weitere Äußerung des Verantwortlichen beim TLfDI einging, wurde der Verantwortliche vor Erlass einer Maßnahme nach Art. 58 Abs. 2 DS-GVO nach § 7 Abs. 1 ThürDSG nochmals angehört und eine Verwarnung angekündigt. Daraufhin lenkte der Verantwortliche ein und teilte mit, man habe die rechtlichen Ausführungen des TLfDI geprüft. Zukünftig werde man nur noch in den Fällen eine Erklärung zu den wirtschaftlichen Verhältnissen verlangen, in denen die zu besetzende Stelle eine besondere Vertrauenswürdigkeit in finanziellen Fragen voraussetze. Die wegen Verstoßes gegen Art. 5 Abs. 1 Buchstabe a) DS-GVO daraufhin ausgesprochene Verwarnung gemäß Art. 58 Abs. 2 Buchstabe b) DS-GVO hielt man

zwar nicht für angemessen, teilte allerdings mit, man bereinige die Personalakten um die bis dahin unzulässig erhobenen „geordneten wirtschaftlichen Verhältnisse“. Weitere Maßnahmen seitens der TLfDI als die Verwarnung waren daher nicht erforderlich.

2.7 Unzulässige Übermittlung einer IBAN durch eine Kommune

Im Falle einer „Datenpanne“ nach Art. 33 DS-GVO ist eine zügige Benachrichtigung aller Betroffenen über den Vorfall wichtig, um weitere nachteilige Auswirkungen für sie zu begrenzen und den Vorfall abzumildern. Nach Art. 33 Abs. 1 DS-GVO ist die Verletzung des Schutzes personenbezogener Daten durch den Verantwortlichen unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, der zuständigen Aufsichtsbehörde zu melden. Bei Verzögerung der gesetzlich vorgeschriebenen Frist ist der Meldung eine Begründung beizufügen.

Durch eine Thüringer Kommune wurde dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) als zuständige Aufsichtsbehörde im Berichtszeitraum eine Verletzung des Schutzes personenbezogener Daten nach Art. 33 Datenschutz-Grundverordnung (DS-GVO) gemeldet.
Aus der Meldung ging hervor, dass es zur Bekanntgabe der International Bank Account Number (= IBAN) eines Bürgers und seiner Frau als kommunale Bankverbindung auf Schriftstücken der Kommune gekommen sei. Als Ursache wurde zum Meldungszeitpunkt ein technischer Fehler in einer verwendeten zentralen Adressdatei (ZAD) angenommenen. ZAD wird verwendet, um beispielsweise intern Adress- und Kontaktdaten zu verwalten und diese strukturiert, integriert, effektiv und zentral für notwendige Vorgänge zur Verfügung zu stellen. Diese Daten können dann zielgerichtet in bestimmten Vorgängen, Akten und Dokumenten verwendet werden. Die Anzahl der Adressaten entsprechender Schreiben, denen die IBAN des Bürgers und seiner Frau als jene der Kommune angezeigt wurde, konnte zum Meldezeitpunkt bereits auf einen mittleren zweistelligen Bereich eingegrenzt werden, und es wurde ausschließlich die IBAN, nicht jedoch der Name der zugehörigen Person, verwendet. Rückschlüsse auf die Iden-

tität des „Inhabers“ der IBAN durch Zusammenführungen von personenbezogenen Daten konnten hier durch die Empfänger der Schreiben nicht erfolgen.
Die Kommune gab zur Behebung und Abmilderung der oben genannten Verletzung des Schutzes personenbezogener Daten an, dass sie zum einen die Kontoinhaber der irrtümlich angegebenen IBAN umgehend sowohl telefonisch als auch schriftlich über den Vorfall informiert und in diesem Zusammenhang gebeten hätte, eventuelle Geldeingänge keinesfalls an die Absender, sondern auf das vorgesehene kommunale Konto zu überweisen, um die Identität der betroffenen Kontoinhaber weiterhin zu schützen. Denn eine Überprüfung der Übereinstimmung zwischen dem Empfängernamen und der IBAN findet im Zahlungsverkehr üblicherweise nicht mehr statt und ist auch laut § 675r Bürgerliches Gesetzbuch nicht mehr vorgeschrieben.
Zum anderen gab die besagte Kommune zwecks Behebung und Abmilderung der oben genannten Datenschutzverletzung an, dass alle Empfänger entsprechender Schreiben der Kommune umgehend informiert sowie aufgefordert wurden, das betroffene Schriftstück mit der IBAN des Bürgers und seiner Frau zu vernichten und eben nicht auf das dort genannte Konto hin zu überweisen.
Zusätzlich zur Meldung nach Art. 33 DS-GVO ergriff die Kommune sowohl technische als auch organisatorische Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten. So wurden bereits Fehleranalysen der Software, Überprüfung der Zugriffsrechte und eine Verkleinerung des zugriffsberechtigten Personenkreises durchgeführt, da ein menschliches Versagen nicht ausgeschlossen werden konnte.
Der TLfDI forderte abschließend noch die Bestätigung der Verschwiegenheitserklärungen des Bürgers und seiner Frau ab, da zwei Personen aufgrund der falsch angegebenen IBAN auf das besagte Konto überwiesen hatten. Diese Erklärungen wurden dem TLfDI zeitnah vorgelegt. Die von der Kommune getroffenen technischen und organisatorischen Maßnahmen wurden anschließend vom TLfDI als ausreichend und angemessen erachtet, und das Verfahren der Meldung nach Art. 33 DS-GVO beim TLfDI konnte abgeschlossen werden.

2.8 Wenn die Beschwerde zulässig, aber in der Sache unbegründet ist

Nach Art. 5 Abs. 1 Buchstabe a) DS-GVO müssen personenbezogene Daten auf rechtmäßige Weise verarbeitet werden. Für jede Datenverarbeitung muss es eine Rechtsgrundlage geben. Die Rechtsgrundlagen für die Datenverarbeitung sind in Art. 6 Abs. 1 DS-GVO aufgeführt.

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichte eine Beschwerde, in der bemängelt wurde, dass bei einer telefonischen Anfrage bei der zentralen Stelle einer Behörde zum einen die Kontaktdaten des Anfragenden und zum anderen der Sachverhalt abgefragt wurden. Der Beschwerdeführer war außerdem nicht einverstanden, dass die zentrale Stelle nicht die direkten Kontaktdaten wie beispielsweise die E-Mail-Adresse des zuständigen Sachbearbeiters herausgegeben hatte. So konnte der Beschwerdeführer den zuständigen Sachbearbeiter nicht direkt kontaktieren.
Der TLfDI prüfte den Sachverhalt und kam zu folgendem Ergebnis:
Zunächst zur Abfrage des Namens und des Anliegens:
Offensichtlich handelte es sich um ein Verfahren in dem zuständigen Dezernat der Behörde. Die Leitung hatte dieses festgelegt, um einen geschäftsmäßigen Vorgang in der Behörde für eine effektive Bearbeitung der eingehenden Fälle zu gewährleisten. Aufgrund der Vielzahl an telefonischen Anfragen sollte der jeweilige Mitarbeiter die Möglichkeit haben, das Anliegen oder auch bereits vorliegende Fälle an den zuständigen und richtigen Ansprechpartner zu vermitteln. Außerdem sei die Herausgabe der personalisierten E-Mail-Adressen schon deshalb nicht notwendig, da es Kontaktadressen für einzelne Bereiche gibt und diese auch im Internet abrufbar seien.
Nach Art. 5 Abs. 1 Buchstabe a) Datenschutz-Grundverordnung (DS-GVO) müssen personenbezogene Daten auf rechtmäßige Weise verarbeitet werden. Für jede Datenerhebung muss es eine Rechtsgrundlage geben. Die Rechtsgrundlagen für die Datenverarbeitung sind abschließend in Art. 6 Abs. 1 DS-GVO aufgeführt.
Die Behörde darf in diesem Zusammenhang nach Art. 6 Abs. 1 Satz 1 Buchstabe c) DS-GVO in Verbindung mit Art. 6 Abs. 3 Satz 1 Buchstabe b) in Verbindung mit den einschlägigen nationalen Fachgesetzen personenbezogene Daten verarbeiten, soweit das für die Erfüllung der Aufgaben erforderlich ist. Ein Verfahren, wonach die allgemeine

Telefonzentrale nach Namen und Anliegen fragt, ist nicht unzulässig, wenn die Datenverarbeitung für die Bearbeitung des Anliegens erforderlich ist, vergleiche § 16 Thüringer Datenschutzgesetz. Denn hierfür liegt, wie von der betreffenden Behörde dargelegt, ein sachlicher Grund vor. Der Anruf soll einem bestimmten Bearbeiter beziehungsweise Sachbereich zugeordnet werden können. Selbstverständlich dürfen nur die zu diesem Zweck erforderlichen Daten, also allgemeine Angaben, abgefragt werden. Auch müssen Anfragende ihren Namen nicht nennen und können sich auf ihr Anliegen beschränken oder das Aktenzeichen benennen.
Zur Herausgabe der E-Mail-Adresse der Mitarbeitenden:
Es ist auch nach hiesiger Auffassung zulässig und im Übrigen auch beim TLfDI üblich, nicht die personalisierten E-Mail-Adressen der Beschäftigten bekanntzugeben. Dies hat in aller Regel organisatorische Gründe und eine Benennung der personalisierten Adresse ist für die sachgerechte Bearbeitung nicht erforderlich. Darüber hinaus beinhalten personalisierte E-Mail-Adressen mitunter die vollständigen Namen der Mitarbeiter, deren Offenlegung aus datenschutzrechtlicher Sicht nicht geboten ist. Die Gesetze legen grundsätzlich nur die Zuständigkeit einer Behörde, nicht aber eines bestimmten Mitarbeiters fest, sodass das Handeln der Bediensteten im Vollzug der Gesetze auch stets der Behörde zugerechnet wird. Folglich ist es für Beteiligte eines Verwaltungsverfahrens auch nicht erforderlich, personalisierte Kontaktdaten von Mitarbeitern benannt zu bekommen. Ob und wie die Behörde die Erreichbarkeit einzelner Mitarbeiter gestaltet, ist im Übrigen eine Sache ihrer Organisationsautonomie. Eine Behörde kann im Rahmen ihrer Organisationshoheit festlegen, dass Anrufe zunächst über eine Zentrale entgegengenommen und dann an den zuständigen Bearbeiter verbunden werden. Die Datenverarbeitung durch den dafür zuständigen Beschäftigten muss sich dabei auf das erforderliche Maß beschränken. Dass in diesem Fall ein Verstoß gegen den Grundsatz der Erforderlichkeit vorliegt, war nicht ersichtlich. Dies wurde dem Beschwerdeführer mitgeteilt. Die Entscheidung ist rechtskräftig.
Die datenschutzrechtliche Beurteilung ist dabei von der Frage zu unterscheiden, ob möglicherweise ein Anspruch auf Herausgabe personalisierter Mitarbeiterdaten nach dem Thüringer Transparenzgesetz besteht. Diese Frage war nicht Gegenstand des Verfahrens, denn dem Beschwerdeführer kam es darauf an, grundsätzlich die personalisierte E-Mail-Adresse des jeweiligen Bearbeiters proaktiv zu erhalten. Ein solcher Anspruch käme nur dann in Betracht, wenn die Personen als

Ansprechpartner offiziell fungieren und als solche auch veröffentlicht wurden.

2.9 Kita-Apps können viel, dürfen aber nicht alles … Ohne Einwilligung der Eltern müssen Informationen auch auf anderem Weg ausgetauscht werden

Bei der Einführung einer Kita-App zum Informationsaustausch zwischen Kita und Eltern dürfen die Kontaktdaten der Eltern nicht ohne deren Einwilligung in der App aufgenommen werden. Eine Einrichtung hatte dies dennoch getan und die Eltern damit unter Druck gesetzt, dass ansonsten kein geordneter Informationsaustausch mehr möglich wäre. Beruht die Verarbeitung personenbezogener Daten auf einer Einwilligung, dürfen die Betroffenen, die keine Einwilligung erteilen, gemäß Erwägungsgrund 42 Satz 5 DS-GVO aber keine Nachteile erleiden; der gesetzliche Informationsanspruch zwischen Kita und Eltern gilt unabhängig davon. Für die Verarbeitung der personenbezogenen Daten der Eltern ohne Einwilligung verwarnte der TLfDI den Träger der Kita.

Anwendungssoftware für Kindertagesstätten (Kita Apps) ist groß im Kommen – von der Anmeldung für und der Vergabe von Betreuungsplätze(n) über die Weitergabe wichtiger Informationen wie Schließzeiten für die Eltern, dem Versenden von Fotos bis zur Aufzeichnung von Schlaf- und Toilettengängen der Kleinen ist fast alles möglich – aber nicht alles, was möglich ist, ist auch erlaubt. Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichten im Berichtszeitraum zahlreiche Anfragen und Beschwerden im Zusammenhang mit der Einführung solcher Apps, so auch im vorliegenden Fall, bei dem eine Kita die Eltern schriftlich dazu aufforderte, ihre Einwilligung zur Nutzung einer App zu erteilen, um künftig auf diesem Weg wichtige Nachrichten aus der Gruppe ihres Kindes zu erhalten. Bereits auf diesem Formular war ein personifizierter Code auf den Namen des jeweiligen Kindes angegeben, der bei Aufrufen der App eingegeben werden sollte. Außerdem fehlten alle Informationen die gemäß Art. 13 Datenschutz-Grundverordnung (DS-GVO) bei der Datenerhebung mitzuteilen sind.
Auch auf Nachfrage erhielt eine Familie keine Auskunft von der Kita-Leitung, wer zu welchen Zwecken welche personenbezogenen Daten

in der App verarbeitet und erteilte daher auf dem Formular keine Einwilligung. Die Kita erklärte den Eltern daraufhin, dass eine Kommunikation ohne App nicht gewährleistet werden könne und versuchte, die Eltern doch noch von der Nutzung zu überzeugen. Erst als die Eltern mehrfach darum baten, Informationen per E-Mail zu erhalten, schrieb die Kita, dass sie nun, da die Eltern es „eindeutig wünschen", die Familie und ihre personenbezogenen Daten endgültig aus der App löschen würden.

Diese indirekte Bestätigung, dass ihre Daten bereits in der App verarbeitet wurden, ohne dass sie zuvor eine Einwilligung erteilt hatten, veranlasste die Eltern, sich beim TLfDI zu beschweren. In der vom TLfDI angeforderten Stellungnahme gab der Träger der Kita an, dass tatsächlich zunächst ohne Einwilligung alle Kontaktdaten der Eltern in die App eingepflegt worden waren, daraufhin personifizierte Einladungscodes erstellt und den Eltern das Papier-Formular zur Einwilligung vorgelegt wurde. Mit der Anmeldung bei der App und der Nutzung des Codes sollte dann in der App eine elektronische Einwilligungserklärung im System hinterlegt werden.

Für eine rechtmäßige Verarbeitung von personenbezogenen Daten bedarf es einer Rechtsgrundlage, hier einer Einwilligung der Sorgeberechtigten gemäß Art. 6 Abs. 1 Satz 1 Buchstabe a) DS-GVO. Diese wurde von den Eltern nicht erteilt, dennoch wurden die Daten in der App aufgenommen und gespeichert. Außerdem fehlten bei der Erhebung der Daten sämtliche Informationen gemäß Art. 13 DS-GVO, also unter anderem Angaben zu Zweck, Rechtsgrundlage und Empfänger der Daten sowie die Aufklärung über die Rechte des Betroffenen. Somit hatte die Kita gegen datenschutzrechtliche Vorschriften verstoßen.

Im Rahmen seiner Befugnisse gemäß Art. 58 Abs. 2 Buchstabe b) DS-GVO hat der TLfDI den Träger der Kita als Verantwortlichen im Sinne des Art. 4 Nr. 7 DS-GVO schriftlich verwarnt. Da es sich um einen nicht-öffentlichen Träger handelte, fiel die Kostenentscheidung für die Erstellung des Bescheids zu Lasten des Trägers aus.

Das Anmeldeverfahren für die App wurde durch den Träger mit sofortiger Wirkung dahingehend geändert, dass zunächst eine schriftliche Einwilligung bei den Eltern eingeholt und dabei die Informationen nach Art. 13 DS-GVO in Form eines Informationsblattes zur Verfügung gestellt wurden. Nur sofern eine Einwilligung erteilt wird, erfolgt nunmehr eine Aufnahme der Daten in die App.

Grundsätzlich ist anzumerken, dass es einen gesetzlichen Anspruch der Eltern auf Informationen aus der Kita gibt. Im Thüringer Kindergartengesetz heißt es dazu in § 7 Abs. 3 Satz 1: „Die Kindertageseinrichtungen nehmen ihren Auftrag zum Wohl des Kindes im ständigen engen Austausch mit den Eltern wahr und gewährleisten deren Anspruch auf Information und Beratung hinsichtlich aller Fragen zur Entwicklung ihres Kindes.“ Wie dieser Austausch vorgenommen werden soll, schreibt das Gesetz nicht vor. Sofern für die Nutzung einer App, wie im vorliegenden Fall, keine Rechtsgrundlage außer einer Einwilligung besteht, ist die Einwilligung nur rechtmäßig, wenn der Betroffene eine echte oder freie Wahl hat und in der Lage ist, die Einwilligung zu verweigern, ohne Nachteile zu erleiden (Erwägungsgrund 42 Satz 5 DS-GVO). Die Verwendung einer App kann den Eltern also nicht verpflichtend vorgeschrieben werden, vielmehr muss ihnen eine alternative Möglichkeit angeboten werden, wie dem gesetzlichen Informations- und Beratungsanspruch der Eltern nachgekommen wird.

2.10 Wenn die Einwilligung zur Veröffentlichung von Schülerfotos im Internet fehlt, darf dies nicht zu Nachteilen führen

Für die Veröffentlichung von Schülerfotos auf der Internetseite der Schule bedarf es zwingend einer Einwilligung durch die Betroffenen beziehungsweise deren Sorgeberechtigte. Die Schule kann sich nicht auf das Kunsturhebergesetz berufen, wonach es keiner Einwilligung bedarf, wenn einzelne Schüler nur als „Beiwerk neben einer Örtlichkeit“ gezeigt werden. Das entstellende Unkenntlichmachen durch gezeichnete Bärte, Brillen oder Haare von Schülerinnen und Schülern auf solchen Fotos kann als datenschutzrechtlich nicht zulässiger Nachteil angesehen werden, den der Betroffenen erleidet, wenn er keine Einwilligung erteilt. Auch dies ist datenschutzrechtlich nicht zulässig.

Die Eltern einer Grundschülerin staunten nicht schlecht, als sie auf der Schulhomepage ein Klassenfoto fanden, auf dem das Gesicht ihrer Tochter wenig schmeichelhaft mit einem schwarzen Bart, einer dicken Brille und zotteligen langen Haaren übermalt worden war.
Vorausgegangen waren mehrere Hinweise und Bitten der Eltern an die Schulleitung und die Klassenlehrerin, keine Fotos ihrer Tochter im Internet zu veröffentlichen. Bereits im Einschulungsbogen, bei dem in Thüringen routinemäßig die Einwilligung zur Veröffentlichung von

Fotos bei den Sorgeberechtigten abgefragt wird, hatten die Eltern keine Einwilligung erteilt. Dennoch wurden mehrmals Fotos, auf denen das Mädchen erkennbar war, auf der Homepage der Schule veröffentlicht und auch auf Nachfrage der Eltern nicht wieder entfernt. Das Foto, auf dem ihre Tochter nun derart verunstaltet war, nahmen die Eltern schließlich zum Anlass, sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) zu wenden.

Bei der Veröffentlichung von personenbezogenen Daten (hier eines Fotos) auf der Internetseite der Schule handelt es sich um die Verarbeitung von personenbezogenen Daten, für die es einer Rechtsgrundlage bedarf. In diesem Fall kam Art. 6 Abs. 1 Satz 1 Buchstabe a) Datenschutz-Grundverordnung (DS-GVO) in Betracht, wonach es einer Einwilligung der betroffenen Person bedurft hätte. Diese Einwilligung lag jedoch generell nicht vor, da die Eltern auf dem Schülerbogen der Veröffentlichung von Fotos ihres Kindes nicht zugestimmt hatten. Auch für einzelne schulische Ereignisse, für die die Klassenlehrerin gesondert nach dem Einverständnis der Eltern für die Darstellung auf der Schulhomepage gefragt hatte, hatten die Sorgeberechtigten ausdrücklich widersprochen.

Auch eine Veröffentlichung in Wahrnehmung einer öffentlichen Aufgabe beziehungsweise in Ausübung öffentlicher Gewalt, die dem Verantwortlichen gemäß Art. 6 Abs. 1 Satz 1 Buchstabe e) DS-GVO übertragen wurde, war hier nicht einschlägig, da weder das Thüringer Schulgesetz noch die Thüringer Schulordnung eine entsprechende Regelung enthalten, die eine Veröffentlichung von Fotos im Internet legitimiert. Nach § 57 Abs. 1 Thüringer Schulgesetz sind die Schulen zwar ermächtigt, personenbezogene Daten zu verarbeiten, sofern es für die Erfüllung der durch Rechtsvorschriften zugewiesenen Aufgaben erforderlich ist. Wenngleich eine Information beziehungsweise Werbung über die Schulhomepage eine erforderliche Aufgabe der Schule darstellen kann, muss diese in einem angemessenen Verhältnis zu den schutzwürdigen Interessen der Betroffenen stehen. Die Veröffentlichung von Fotos im Netz, insbesondere von Kindern, stellt einen besonders schwerwiegenden Eingriff in das Recht am eigenen Bild dar, das hier mit dem Grundrecht auf informationelle Selbstbestimmung aus Art. 1 Abs. 1 in Verbindung mit Art. 2 Abs. 1 Grundgesetz sowie Art. 6 Abs. 2 Thüringer Verfassung einhergeht. Besonders schwerwiegend deshalb, da eine schier unendliche Zahl von Nutzerinnen und Nutzern im Internet auf die Website zugreifen kann, Bilder

kopiert und damit auch potentiell über andere Medien weitergeleitet werden können. Die Angemessenheit für einen solchen Eingriff in die Persönlichkeitsrechte ist bei der Anfertigung und Veröffentlichung von Schülerfotos nicht gegeben. Die Veröffentlichung von Fotos auf der Internetseite der Schule, auf denen eine Schülerin zu erkennen ist, ohne dass dafür eine Einwilligung der Sorgeberechtigten erteilt wurde, stellt damit einen Verstoß gegen die Datenschutz-Grundverordnung dar.

Der TLfDI hatte daher die Schulleitung gemäß § 7 Abs. 1 Satz 2 Thüringer Datenschutzgesetz in Verbindung mit Art. 58 Abs. 2 Buchstabe b) DS-GVO zu einer Stellungnahme aufgefordert. Die Schulleitung berief sich in ihrer Antwort auf § 23 Abs. 1 Kunsturhebergesetz (KunstUrhG), wonach Personen auch ohne Einwilligung abgebildet werden dürfen, wenn bei der Darstellung die Veranstaltung im Mittelpunkt steht. Dies sei bei der Einschulungsfeier und anderen schulischen Events der Fall. Außerdem seien, bis auf das Klassenfoto, keine Bilder veröffentlicht worden, auf denen die Schülerin alleine oder in einer Kleingruppe zu sehen war, auch eine Abbildung in einer unvorteilhaften Situation sei nicht erfolgt.

Die Prüfung der Stellungnahme der Schulleitung durch den TLfDI ergab jedoch, dass sich die Schulleitung nicht auf § 23 Abs. 1 Nr. 2 und 3 KunstUrhG berufen kann. Gemäß § 23 Abs. 1 Nr. 2 KunstUrhG bedarf es keiner Einwilligung, wenn Personen nur als Beiwerk neben einer Landschaft oder sonstigen Örtlichkeit erscheinen. Bei der Einschulung und anderen schulischen Veranstaltungen steht jedoch nicht die Schule als Örtlichkeit im Vordergrund, vielmehr sind dies Veranstaltungen, bei denen die Personen entscheidend für den Aussagewert der Bildaufnahme sind (Kinder werden eingeschult, Kinder machen Sport und vieles mehr). Solche Veranstaltungen sind auch keine Versammlungen im Sinne des § 23 Abs. 1 Nr. 3 KunstUrhG, sondern schulische Veranstaltungen, daher galten die oben bereits erläuterten Grundsätze zur Erforderlichkeit und Angemessenheit. Die Rechtsauffassung der Schulleitung ging hier fehl, die Bilder, auf denen die Schülerin zu sehen war, hätten nicht auf die Schulhomepage gestellt werden dürfen. Der TLfDI hat die Schulleitung daher gemäß Art. 58 Abs. 2 Buchstabe b) DS-GVO verwarnt.

Auch bei der Unkenntlichmachung des Gesichts der Schülerin auf dem Klassenfoto hatte die Schulleitung gegen Datenschutzrecht verstoßen. Grundsätzlich darf den Betroffenen bei Nichterteilung einer Einwilligung kein Nachteil entstehen (Erwägungsgrund 42 zur DS-

GVO). Die entstellende Unkenntlichmachung des Gesichts des Mädchens unter anderem durch Bart und Zottelhaare kann jedoch als herabwürdigende Sanktion angesehen werden. Das Foto, auf dem das Mädchen dergestalt unkenntlich gemacht wurde, wurde zwar unmittelbar nach Hinweis durch die Sorgeberechtigten von der Schulhomepage gelöscht. Dennoch wies der TLfDI die Schulleitung darauf hin, dass eine Veröffentlichung von Fotos, auf denen Schülerinnen und Schüler in herabwürdigender Art unkenntlich gemacht werden, auch mögliche andere (straf- beziehungsweise zivil-) rechtliche Konsequenzen nach sich ziehen kann. Der TLfDI riet dazu, in vergleichbaren Fällen die Kinder, für die keine Einwilligung zur Veröffentlichung von Fotos besteht, bestenfalls gar nicht erst zu fotografieren oder eine Unkenntlichmachung durch Herausschneiden beziehungsweise Pixeln mit einem Bildbearbeitungsprogramm unkenntlich zu machen.

2.11 Abfrage in Schule zu Läusebefall

Läuse sind eine lästige Angelegenheit – und der Befall ist dazu noch meldepflichtig. Für Gemeinschaftseinrichtungen wie Kindergärten oder Schulen besteht für die von den Blutsaugern Betroffenen ein Betretungsverbot und die Pflicht, die Kita- beziehungsweise Schulleitung zu informieren, außerdem muss die Einrichtungsleitung das Gesundheitsamt unterrichten. Um die Ausbreitung des Läusebefalls unter den Kindern einzudämmen, darf eine Grundschule die Eltern zwar darüber informieren, dass Läuse in der Einrichtung aufgetreten sind, für die Abfrage, ob die Kinder Läuse haben besteht jedoch keine Rechtsgrundlage.

Sie gehen reihum und oft kommen sie am Ende dort wieder an, wo sie angefangen haben. Die Rede ist von Läusen, die wohl keinen Kinderkopf in der Kita oder Grundschule auslassen. Kaum hat man sie weitergegeben und die Haare mit Spezialshampoo gewaschen, die Nissen ausgekämmt und die Bettwäsche wahlweise tiefgefroren oder gekocht, sind sie schon wieder da, ein fröhlicher Ringelreihen durch die einzelnen Gruppen und Klassen und darüber hinaus. Um der „Seuche“ Herr zu werden, teilte eine Grundschule einen Elternbrief aus, bei dem die Sorgeberechtigten nicht nur über den Läusebefall in der Klasse ihres Kindes und die Behandlungsmöglichkeiten informiert wurden, die Eltern sollten auch auf einem Antwortabschnitt des Blattes Angaben

machen, ob ihr Kind von Läusen befallen und eine entsprechende Behandlung durchgeführt wurde oder ob der Kopf des Kindes frei von diesen Parasiten und ihren Eiern sei. Der ausgefüllte Abschnitt solle nach der Untersuchung des Kindes ausgefüllt und unterschrieben in der Schule abgegeben werden; ein Hinweis, dass die Angaben „diskret“ behandelt würden, war vorsorglich angegeben.
Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichte daraufhin eine Mitteilung von Eltern, die diese Form der Abfrage von Gesundheitsdaten nicht nur für unzulässig hielten, sie wiesen außerdem darauf hin, dass bei der Erhebung von personenbezogenen Daten den Betroffenen die Informationen gemäß Art. 13 DS-GVO mitgeteilt werden müssen. Das Formular der Schule enthielt aber weder die dort geforderten Angaben zur Rechtsgrundlage der Abfrage, noch zu den Zwecken oder den Empfängern der Daten oder die Hinweise zu den Rechten der Betroffenen wie zum Beispiel das Recht auf Löschung der Daten oder das Beschwerderecht bei der Aufsichtsbehörde.
Die Datenschutz-Grundverordnung (DS-GVO) kennt den Ausdruck „Diskretion“ nicht, wohl aber schreibt sie in Art. 9 Abs. 1 vor, dass die Verarbeitung von besonderen Kategorien personenbezogener Daten, wie zum Beispiel Gesundheitsdaten, grundsätzlich untersagt ist. Artikel 9 Abs. 2 DS-GVO regelt jedoch Ausnahmen von diesem Grundsatz, insbesondere in Art. 9 Abs. 2 Buchstabe g) DS-GVO gibt es eine Öffnungsklausel, wonach die Verarbeitung dann möglich ist, wenn sie auf der Grundlage des Rechts eines Mitgliedstaates, 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 erforderlich ist. Eine solche Rechtsgrundlage findet sich im Infektionsschutzgesetz. Bei der Verarbeitung von Gesundheitsdaten aufgrund einer möglichen Verlausung käme daher als Rechtsgrundlage Art. 6 Abs. 1 Satz 1 Buchstabe e) DS-GVO in Verbindung mit § 34 Abs. 1 Satz 2, Abs. 5 und 6 Infektionsschutzgesetz (IfSG) in Betracht, wonach Verlausung eine meldepflichtige Erkrankung ist, die zunächst dem Leiter der Gemeinschaftseinrichtung (hier der Schule) und weiterführend dem zuständigen Gesundheitsamt zu melden ist. Im geschilderten Fall könnte allerdings eine Schülerin beziehungsweise ein Schüler, der tatsächlich Kopfläuse hat, den besagten Zettel gar nicht in der Schule abgeben, da gemäß § 34 Abs. 1

Satz 2 IfSG für Betroffene ein Zutrittsverbot zur Schule besteht. Hier bestünde nur die Möglichkeit einer telefonischen Meldung bei der Schule oder die Abgabe des Zettels durch Dritte. Da aber bei Läusebefall für die Betroffenen sowieso eine unverzügliche Meldepflicht besteht, ist eine Abfrage, ob Läuse auf den Kinderköpfen zu finden sind, zu einem beliebigen Zeitpunkt nicht nur überflüssig, sondern es besteht dafür auch keine Rechtsgrundlage.
Für die Abfrage, ob ein Befall mit Läusen NICHT vorliegt, besteht ebenfalls KEINE Rechtsgrundlage. § 34 IfSG sieht nur für die Positivmeldung eines Läusebefalls eine Meldepflicht vor. Eine Negativmeldung stellt für die Schule letztendlich auch ein „überflüssiges Datum“ dar, da sie für die Aufgabenerfüllung der Schule (Benachrichtigung anderer Eltern und des Gesundheitsamtes im Falle des Auftretens von Kopfläusen) nicht erforderlich ist und damit auch dem Grundsatz der Datensparsamkeit widerspräche. Für eine Negativmeldung käme nur eine Einwilligung der Sorgeberechtigten in Betracht (Art. 6 Abs. 1 Satz 1 Buchstabe a) in Verbindung mit Art. 9 Abs. 2 Buchstabe a) DS-GVO). Für eine wirksame Einwilligung müssen neben den Informationen gemäß Art. 13 DS-GVO jedoch auch die Hinweise vorliegen, dass es sich um eine freiwillige Angabe handelt, die jederzeit widerrufen werden kann und dass den Betroffenen keine Nachteile entstehen, sofern sie keine Auskunft erteilen.
Der TLfDI wandte sich daher an die Schule und forderte die Schulleitung zur Stellungnahme auf, ob die Angaben durch die Sorgeberechtigten freiwillig aufgrund einer Einwilligung erhoben werden sollten und erläuterte die entsprechenden Bedingungen sowie die Rechtslage gemäß Infektionsschutzgesetz. Sofern keine Einwilligung eingeholt werden solle, könne das Formular nur in Form einer reinen Information zu den Untersuchungs- und Behandlungsmöglichkeiten bei Läusebefall ausgeteilt werden, lediglich eine Kenntnisnahme könne dann durch die Unterschrift der Sorgeberechtigten eingeholt werden.
Die Schulleitung entschied daraufhin unverzüglich, den Elternbrief dahingehend abzuändern, dass neben der allgemeinen Information zu Kopfläusen und den Behandlungsempfehlungen der Hinweis auf die gesetzliche Meldepflicht gegenüber der Schulleitung erteilt wurde und nur die Kenntnisnahme durch die Sorgeberechtigten über das Hausaufgabenheft bestätigt werden musste. Der TLfDI konnte den Eltern daher zeitnah mitteilen, dass das Verfahren an der Schule aufgrund ihres Hinweises datenschutzkonform abgeändert wurde.

2.12 Unentgeltliche Kopien – ja! Aber in welcher Form?

Um Missverständnisse zu vermeiden, sollten Bürgerinnen und Bürger bei der Durchsetzung ihres Auskunftsrechts nach Art. 15 Abs. 1 und Abs. 3 Satz 1 in Verbindung mit Art. 12 Abs. 5 Satz 1 DS-GVO konkret benennen, in welcher Form sie die Übermittlung etwaiger Dokumente begehren. Dabei ist zu beachten, dass eine unverschlüsselte E-Mail weder gegen eine Kenntnisnahme durch Unbefugte noch gegen eine inhaltliche Veränderung geschützt ist.

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichte im Berichtszeitraum die Beschwerde einer Bürgerin, welche ihr Recht auf Erstellung einer unentgeltlichen Kopie gemäß Art. 15 Abs. 1 und Abs. 3 Satz 1 in Verbindung mit Art. 12 Abs. 5 Satz 1 Datenschutz-Grundverordnung (DS-GVO) gegenüber einer öffentlichen Stelle des Landes Thüringen geltend machte. Die Behörde hatte der Bürgerin zwar die von ihr beantragten Unterlagen übermittelt, diese jedoch unverschlüsselt per E-Mail und nicht in kopierter postalischer Form. Zugleich übersandte die Beschwerdeführerin dem TLfDI sämtliche in Rede stehenden Dokumente – ebenfalls per E-Mail! Der TLfDI gelangte nach Prüfung des zugrundeliegenden Sachverhalts zu dem Ergebnis, dass die öffentliche Stelle durch die Zusendung der Dokumente via unverschlüsselter Mail einen Verstoß gegen Art. 5 Abs. 1 Buchstabe f) DS-GVO beging. Diese Norm regelt, dass personenbezogene Daten in einer Weise verarbeitet werden müssen, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet. Dies schließt den Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“) ein.
Die Feststellung des TLfDI, dass im konkreten Fall ein Verstoß gegen Art. 5 Abs. 1 Buchstabe f) DS-GVO vorlag, stützte sich darauf, dass durch den unverschlüsselten Versand via E-Mail an den E-Mail-Dienst Gmail.com, welchen die Bürgerin nutzte, ein Bruch der Vertraulichkeit von personenbezogenen Daten zumindest nicht ausgeschlossen werden konnte. Konkret sah der TLfDI ein Risiko darin, dass Gmail.com alle Inhalte im Klartext auf seinen Servern speichert und damit die Möglichkeit hat, diese für eigene Zwecke zu verarbeiten. Entsprechend der Orientierungshilfe der Datenschutzkonferenz

(DSK) zur Verschlüsselung (https://www.datenschutzkonferenz-online.de/media/oh/20210616_orientierungshilfe_e_mail_verschluesselung.pdf) müssen Verantwortliche, die E-Mail-Nachrichten versenden, bei denen ein Bruch der Vertraulichkeit von personenbezogenen Daten im Inhalt der Nachricht ein hohes Risiko für die Rechte und Freiheiten von natürlichen Personen darstellt, regelmäßig eine Ende-zu-Ende-Verschlüsselung und eine qualifizierte Transportverschlüsselung vornehmen. Eine solche Verschlüsselung nahm im konkreten Fall die öffentliche Stelle gerade nicht vor, sodass vom TLfDI ein datenschutzrechtlicher Verstoß gegen Art. 5 Abs. 1 Buchstabe f) DS-GVO festgestellt werden musste.
Von einer Verwarnung gemäß Art. 58 Abs. 2 Buchstabe b) DS-GVO sah der TLfDI jedoch in diesem konkreten Fall dennoch ab und machte von seinem Ermessen Gebrauch. Bei der Ermessensausübung spielten gleich mehrere Gesichtspunkte eine Rolle:
Grundsätzlich ist eine Datenkopie an keine bestimmte Form gebunden, wie sich auch aus Art. 12 Abs. 1 Satz 2 und 3 DS-GVO ergibt. Außerdem ergibt sich laut Europäischem Gerichtshof (EuGH-Urteil C-487/21) aus der DS-GVO, dass der Verantwortliche geeignete Maßnahmen zu treffen hat, um der betroffenen Person alle unter anderem in Art. 15 DS-GVO genannten Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln, und dass die Übermittlung der Informationen **schriftlich oder in anderer Form, gegebenenfalls auch elektronisch, zu erfolgen hat**, es sei denn, die betroffene Person verlangt, dass diese mündlich erteilt werden. Diese Bestimmung, die Ausdruck des Transparenzgrundsatzes ist, soll gewährleisten, dass die betroffene Person in die Lage versetzt wird, die an sie gerichteten Informationen in vollem Umfang zu verstehen. Bei einer aktiven Informationspflicht besteht damit grundsätzlich ein Entscheidungsspielraum des Verantwortlichen, in welcher Form er die gebotenen Informationen bereitstellt (vergleiche Kühling/Buchner, DS-GVO und BDSG, 2. Auflage, Artikel 12, Randnummer 16).
Im konkreten Fall war aber auch Folgendes zu beachten: Sämtliche durch die Beschwerdeführerin initiierte Korrespondenz (im Übrigen auch jene an den TLfDI) erfolgte über die genannte Gmail.com-Adresse, welche die Beschwerdeführerin als Kontaktadresse gegenüber der öffentlichen Stelle angegeben hatte. Zwar hatte die Beschwerdeführerin ihren Auskunftsantrag bei der Behörde schriftlich gestellt, sie hatte aber mit ihrem Antrag nicht ausdrücklich erklärt, in welcher

Form (papierhaft oder elektronisch) sie die Übersendung der Datenkopie begehrte. Vielmehr bat die Beschwerdeführerin darum, dass ihr die begehrten Dokumente „zur Verfügung gestellt werden“. Im Briefkopf ihres Antrags war zudem schriftbildlich gleichrangig neben der Postadresse die E-Mail-Adresse bei dem Anbieter Google (Gmail.com) von ihr angegeben worden. Dies konnte objektiv nicht anders verstanden werden, als dass die Beschwerdeführerin die Form der Kommunikation einschließlich der mit diesem Schreiben beantragten Übersendung der Datenkopien der verantwortlichen Behörde zur Disposition stellte.
Nicht zuletzt war bei der Ermessensentscheidung des TLfDI auch Folgendes im Kontext zu betrachten: Die Beschwerdeführerin selbst hatte sämtliche Pdf-Dokumente dem TLfDI über ihre Gmail.com-E-Mail-Adresse zugeleitet, was ebenfalls ein hohes Risiko eines Bruchs der Vertraulichkeit von personenbezogenen Daten in sich trug. Insoweit hatte die Beschwerdeführerin auch ein Stück weit selbst dazu beigetragen, dass etwaige Daten zu ihrer Person gegebenenfalls auf den Gmail.com-Servern im Klartext gespeichert und durch diesen Dienst weiterverarbeitet werden konnten.
Deshalb ist es dem TLfDI sehr wichtig, an dieser Stelle darauf hinzuweisen, dass eine unverschlüsselte E-Mail weder gegen eine Kenntnisnahme durch Unbefugte noch gegen eine inhaltliche Veränderung geschützt ist. Die Verwendung des E-Mail-Kontos gerade des Anbieters Gmail.com als Empfängeradresse fällt auch in den jeweiligen eigenen Risikobereich. Wie mit etwaigen Daten nach deren Eingang auf dem E-Mail-Konto verfahren wird, hat somit jeder einzelne Nutzer durch die eigene Auswahl des Anbieters Google und die Annahme von dessen Vertragsbedingungen zu vertreten.
Ungeachtet dessen teilte die verantwortliche öffentliche Stelle dem TLfDI mit, dass künftig den Antragstellenden, sofern sie es wünschen, die entsprechenden Daten über die Thüringer Datenaustauschplattform in verschlüsselter Form zum Abruf zur Verfügung gestellt werden.

2.13 Anfrage zur Weitergabe von Meldedaten durch eine Stadtverwaltung für das Mammographie-Screening-Programm

Der Zentralen Stelle Mammographie-Screening Thüringen werden für die Versendung von Einladungen zum Mammographie-Screening-Programm an anspruchsberechtigte Frauen regelmäßig entsprechende

Meldedaten durch das Thüringer Landesrechenzentrum übermittelt. Diese Datenübermittlung ist datenschutzrechtlich zulässig aufgrund von Art. 6 Abs. 1 Satz 1 Buchstabe c) DS-GVO in Verbindung mit § 17 ThürMeldeVO.

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichte im Berichtszeitraum die Anfrage einer Bürgerin, die von der Zentralen Stelle Mammographie-Screening Thüringen eine Einladung zur Mammographie (= Röntgenuntersuchung zur Früherkennung von Brustkrebs) erhalten hatte. Aufgrund der Datenschutzhinweise aus dem Anschreiben ging die Bürgerin davon aus, dass die Thüringer Kommune, in der sie ihren Wohnsitz hat, ihre Adressdaten an die Zentrale Stelle Mammographie-Screening weitergegeben hatte.
Nach Angaben der Stadt, die der TLfDI daraufhin anschrieb, war es bei ihr jedoch zu keiner Übermittlung personenbezogener Daten der Bürgerin an die Zentrale Stelle Mammographie-Screening Thüringen gekommen. Den TLfDI bat die Bürgerin vor diesem Hintergrund um eine datenschutzrechtliche Prüfung der Weitergabe ihrer Daten an die Zentrale Stelle Mammographie-Screening Thüringen. Der TLfDI konnte mit folgendem Prüfungsergebnis zur Klärung des Sachverhalts beitragen:
Für die regelmäßige Versendung von Einladungen im Mammographie-Screening-Programm werden von den für das Einladungswesen und Terminmanagement zuständigen Zentralen Stellen die Daten der anspruchsberechtigten Frauen aus den Melderegistern verwendet. Die Nutzung der Meldedaten für die Versendung von Einladungen zum Mammographie-Screening-Programm ist durch die Richtlinien des Gemeinsamen Bundesausschusses der Ärzte und Krankenkassen über die Früherkennung von Krebserkrankungen (Krebsfrüherkennungsrichtlinie – KFE-RL) vorgegeben. § 13 Abs. 1 KFE-RL bestimmt: „Jede Frau ab dem Alter von 50 Jahren bis zum Ende des 70. Lebensjahres soll von der Zentralen Stelle zeitnah mit Erreichen des Anspruchsalters und anschließend zwischen 22 und 26 Monaten nach der letzten Teilnahme oder im Falle der Nichtteilnahme nach der letzten Einladung, persönlich und schriftlich unter Angabe von Untersuchungsort und -termin zur Teilnahme eingeladen werden.“
§ 13 Abs. 3 KFE-RL ergänzt im Hinblick auf die Verwendung von Meldedaten für das Einladungswesen Folgendes: „Für die Einladung verwendet die Zentrale Stelle Daten der Melderegister. Der von den

Melderegistern übermittelte Datensatz soll Vornamen, Familienname, frühere Familiennamen einschließlich Geburtsname, Geburtsdatum, Geburtsort und Anschrift beinhalten."
In Thüringen erhält die bei der Kassenärztlichen Vereinigung Thüringen eingerichtete Zentrale Stelle Mammographie-Screening Thüringen die notwendigen Meldedaten vom Thüringer Landesrechenzentrum (nicht öfter als monatlich), welches konkret den Familiennamen, frühere Namen, Vornamen unter Kennzeichnung des gebräuchlichen Vornamens, Doktorgrad, das Geburtsdatum und den Geburtsort sowie die Anschrift der alleinigen oder Hauptwohnung aller 50- bis 69-jährigen Frauen übermitteln darf. Dies ergibt sich aus § 17 Thüringer Meldeverordnung (ThürMeldeVO). Mit der Regelung ist eine ausreichende gesetzliche Grundlage im Sinne des Art. 6 Abs. 1 Satz 1 Buchstabe c) Datenschutz-Grundverordnung für die Übermittlung der Meldedaten anspruchsberechtigter Frauen gemäß den Vorgaben der KFE-RL durch das Thüringer Landesrechenzentrum an die Zentrale Stelle Mammographie-Screening Thüringen gegeben.
Der Übermittlung eines Datensatzes aus dem Melderegister durch das Thüringer Landesrechenzentrum an die Zentrale Stelle Mammographie-Screening Thüringen zwecks Einladungsmanagement der Vorsorgeuntersuchung kann nicht widersprochen werden. Die Einrichtung einer Übermittlungssperre bei der zuständigen Meldebehörde ist für diesen Fall der Datenübermittlung nicht möglich. Möglich ist aber ein Widerspruch gegen den Erhalt weiterer Einladungen von der Zentralen Stelle. Darauf weist auch die KFE-RL in § 13 Abs. 3 Satz 2 wie folgt hin: „Weiteren Einladungen kann in Textform widersprochen werden; in den Einladungen ist auf dieses Widerspruchsrecht hinzuweisen."
Nachdem der Bürgerin vom TLfDI mitgeteilt werden konnte, dass die Zentrale Stelle Mammographie-Screening Thüringen die Daten der anspruchsberechtigten Frauen zwar aus den Melderegistern erhält, eine regelmäßige Übermittlung jedoch nicht durch die jeweilige Gemeinde erfolgt, sondern gemäß § 17 ThürMeldeVO rechtmäßig durch das Thüringer Landesrechenzentrum, wurde in dieser Angelegenheit noch Kontakt mit der Zentralen Stelle aufgenommen. Denn auf dem der Einladung zum Mammographie-Screening-Programm beiliegenden Informationsschreiben, welches dem TLfDI vorgelegt wurde, befand sich unter dem Punkt Datenschutz der unzutreffende Hinweis, dass die Adresse der angeschriebenen Person durch die Gemeinde

übermittelt worden sei. Der TLfDI wies daher gegenüber der Zentralen Stelle Mammographie-Screening Thüringen darauf hin, dass auf den Informationsschreiben zu den Einladungen eine Korrektur des Datenschutzhinweises dahingehend vorgenommen wird, dass das Thüringer Landesrechenzentrum zukünftig als die nach den gesetzlichen Bestimmungen übermittelnde Stelle der Meldedaten der anspruchsberechtigten Frauen benannt wird.

2.14 Woher, wer und wieso – Transparenz ist alles und ohne Transparenz ist alles nichts, besonders im Datenschutz!

Im Berichtszeitraum erhielt der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) eine Beschwerde über die Verletzung des Schutzes personenbezogener Gesundheitsdaten. Die Beschwerdeführerin hatte sich in der Vergangenheit mit dem Corona-Virus infiziert und dies ihrem zuständigen Gesundheitsamt mitgeteilt. Mehrere Monate später erhielt sie von einem Thüringer Klinikum ein Schreiben, in dem auf ihre Corona-Infektion Bezug genommen und sie gebeten wurde, in die Teilnahme an einer medizinischen Studie einzuwilligen. Ausführliche Datenschutzhinweise zur Herkunft, Verarbeitung und Empfängern der Daten gemäß Art. 13 Datenschutz-Grundverordnung (DS-GVO) enthielt das Schreiben des Klinikums jedoch nicht.
Das Klinikum nahm in seinem Schreiben ausdrücklich Bezug auf das Gesundheitsamt, dem die Infektion der Beschwerdeführerin bekannt war, und teilte mit, dass der Versand des Schreibens durch dieses Gesundheitsamt (mit Briefkopfbogen des Klinikums) erfolgt sei. Für die Beschwerdeführerin war nicht ersichtlich, ob und wie das Klinikum ihre personenbezogenen Gesundheitsdaten zur Corona-Infektion erhalten hatte und mutmaßte naheliegend, dass das Gesundheitsamt ihre Daten dem Klinikum übermittelt hatte, ohne dass die Beschwerdeführerin hierzu ihre Einwilligung erteilt hatte.
Bei positiven und negativen Testergebnissen über das Vorliegen oder Nichtvorliegen einer Infektion mit COVID-19 handelt es sich um personenbezogene Gesundheitsdaten, sogenannte besondere Kategorien von Daten im Sinne von Art. 9 Abs. 1 in Verbindung mit Art. 4 Nr. 15 DS-GVO. Nach Art. 5 Abs. 1 Buchstabe f) DS-GVO in Verbindung mit Art. 32 Abs. 1 DS-GVO sind personenbezogene Daten durch geeignete Maßnahmen vor dem Zugriff unbefugter Dritter zu schützen,

um ihre Integrität und Vertraulichkeit zu wahren. Dies gilt für sensible Gesundheitsdaten in besonderem Maße.
Adresse (Einzelfelder)(Briefanrede)Um festzustellen, ob das Gesundheitsamt tatsächlich personenbezogene Daten der Beschwerdeführerin ohne deren Einwilligung und somit unbefugt an das Klinikum übermittelt hatte und aufgrund welcher Verfahrensweise und welcher rechtlichen Grundlage die Beschwerdeführerin das Schreiben des Klinikums erhalten hatte, wandte sich der TLfDI mit einem Auskunftsersuchen zunächst an den Verantwortlichen des zuständigen Gesundheitsamts. Im Falle kreisangehöriger Gesundheitsämter ist der/die jeweilige Landrat/-rätin verantwortlich und im Falle von Gesundheitsämtern kreisfreier Städte der/die jeweilige Oberbürgermeister/in.
Die Verantwortliche teilte dem TLfDI auf sein Auskunftsersuchen mit, dass sie bereits selbst zahlreiche Nachfragen von betroffenen Personen erhalten habe, die das beschwerdegegenständliche Schreiben des Klinikums ebenfalls erhalten hatten. Betroffen waren rund 4.600 Personen. Zu den Umständen des Schreibens erklärte die Verantwortliche, dass ein verwaltungsinterner Krisenstab im Zusammenhang mit einer Studie des betreffenden Klinikums zu Langzeitfolgen einer Corona-Infektion der verwaltungsinternen Verwendung der Adressen aller an Corona erkrankten Personen zugestimmt hatte und die personenbezogene Daten der Betroffenen für das beschwerdegegenständliche Anschreiben des Klinikums verwendet worden seien. Das Klinikum habe das Anschreiben einschließlich des beigefügten Studienfragebogens selbst erstellt und dem Gesundheitsamt zum Versand an die betroffenen Personen übergeben. Ein Mitarbeiter des Gesundheitsamtes habe dann entsprechende Serienbriefe erstellt, die über die Poststelle der Verantwortlichen ausgedruckt und versandt worden seien. Die Verantwortliche habe die Adressen der betroffenen Personen zu keinem Zeitpunkt unbefugt dem Klinikum übermittelt.
Nach datenschutzrechtlicher Prüfung des von der Verantwortlichen geschilderten Sachverhalts teilte der TLfDI der Verantwortlichen mit, dass die Betroffene keine Einwilligung zur Verarbeitung ihrer personenbezogenen Daten für andere Zwecke als zur Kontaktaufnahme beziehungsweise Kontaktnachverfolgung im Zusammenhang mit einer positiven Testung auf das Corona-Virus SARS-CoV-2 erteilt hatte. Zudem war für die Betroffene aufgrund des Briefkopfes vom Klinikum nicht erkennbar, dass das Anschreiben des Klinikums tatsächlich von der Verantwortlichen und nicht vom Klinikum versandt worden war. Damit verstieß die Verarbeitung der personenbezogenen Daten

der Beschwerdeführerin durch die Verantwortliche im beschwerdegegenständlichen Schreiben gegen das Transparenzgebot nach Art. 5 Abs. 1 Buchstabe a) DS-GVO in Verbindung mit Art. 13 DS-GVO und Art. 9 Abs. 2 Buchstabe a) DS-GVO. Gemäß Art. 5 Abs. 1 Buchstabe a) DS-GVO müssen personenbezogene Daten auf rechtmäßige und in einer für die betroffene Person nachvollziehbaren, transparenten Weise verarbeitet werden. Gemäß Art. 13 Abs. 1 DS-GVO in Verbindung mit Art. 12 Abs. 1 DS-GVO muss der Verantwortliche die betroffene Person in präziser, transparenter und verständlicher Form über die Verarbeitung ihrer personenbezogenen Daten informieren.
Zudem dürfen personenbezogene Daten nur für festgelegte, eindeutige Zwecke verarbeitet werden (Art. 5 Abs. 1 Buchstabe b) DS-GVO). Eine Verarbeitung für wissenschaftliche Zwecke ist gemäß Art. 9 Abs. 2 Buchstabe j) DS-GVO in Verbindung mit Erwägungsgrund 53 DS-GVO sowie gemäß § 16 Abs. 2 Nr. 3 Thüringer Datenschutzgesetz zur Durchführung wissenschaftlicher Forschung durch öffentliche Stellen wie beispielsweise öffentliche Kliniken zwar zulässig; jedoch ist es besonders in diesen Fällen zwingend geboten, die Betroffenen gemäß Art. 13 beziehungsweise 14 DS-GVO in Verbindung mit Art. 12 Abs. 1 DS-GVO über die Verarbeitung ihrer Daten umfassend in transparenter und verständlicher Form zu informieren. Diese Information erfolgte durch die Verantwortliche im vorliegenden Fall nicht, sodass für die Beschwerdeführerin nicht nachvollziehbar war, woher das Klinikum ihre Daten hatte beziehungsweise dass ihre Daten ausschließlich durch die Verantwortliche und gerade nicht durch das Klinikum, dessen Kopfbogen sich auf dem beschwerdegegenständlichen Schreiben befand, verarbeitet worden waren. Somit war die Verarbeitung der Daten der Betroffenen für diese weder transparent noch nachvollziehbar und verstieß damit gegen Art. 5 Abs. 1 Buchstabe a) DS-GVO in Verbindung mit Art. 13 DS-GVO.
Aufgrund dieses Verstoßes gegen den Schutz personenbezogener Daten sprach der TLfDI nach Anhörung der Verantwortlichen gegen diese eine Verwarnung nach Art. 58 Abs. 2 Buchstabe b) DS-GVO aus. Der TLfDI informierte die Beschwerdeführerin über die Verwarnung der Verantwortlichen und erklärte das Verwaltungsverfahren damit für erledigt. Weitergehende Maßnahmen waren nicht erforderlich, da mit einer Wiederholung nicht zu rechnen war.

2.15 Krankheit oder Versagensangst – darf eine Hochschule für den Nachweis der Prüfungsunfähigkeit eine ärztliche Diagnose verlangen?

Prüfungsunfähig oder doch nur Prüfungsangst – um zu unterscheiden, ob Prüfungskandidaten zwar erkrankt, aber dennoch in der Lage wären, die Prüfung zu absolvieren oder ob es ihnen so schlecht geht, dass sie tatsächlich außer Stande sind, an der Prüfung teilzunehmen, forderte eine Thüringer Hochschule von ihren Studierenden im Fall der Fälle ein ärztliches Attest, das Angaben zu Symptomen enthalten solle. Aufgrund der Angabe dieser, durch Art. 9 DS-GVO besonders geschützten Gesundheitsdaten, würde dann das Prüfungsamt – und nicht etwa der Arzt – entscheiden, ob der Nachweis zur Prüfungsunfähigkeit akzeptiert werde.

Große Aufregung an einer Thüringer Hochschule: Gleich mehrere Beschwerden erreichten den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Darin weitergeleitet wurde eine E-Mail, in der den Studierenden durch ihre Hochschule mitgeteilt wurde, dass künftig zum Nachweis der Prüfungsunfähigkeit nicht mehr ein einfaches ärztliches Attest ausreiche. Vielmehr müsse der Arzt beziehungsweise die Ärztin künftig die notwendigen Informationen übermitteln, aufgrund derer dann das Prüfungsamt entscheide, ob diese für die Anerkennung der Prüfungsunfähigkeit ausreichen oder nicht. Das dazugehörige Formular, das vom Arzt auszufüllen sei, enthielt dann zwei Optionen zu den Angaben der Beeinträchtigungen des erkrankten Studierenden. Option 1 forderte per Ankreuzverfahren die genaue Angabe, welche Form der Prüfung nicht angetreten werden könne (mündliche Leistung, schriftliche Leistung unter oder ohne Aufsicht oder fachpraktische Leistungen). Bei Option 2 konnte detailliert geschildert werden, welche Symptome vorliegen und wie die Krankheit bezeichnet würde, inklusive ICD-Code. Wenngleich die Angaben unter Option 2 als „freiwillig“ gekennzeichnet waren, stellten die Studierenden in ihren Beschwerden beim TLfDI die Frage, ob eine Verarbeitung dieser Gesundheitsdaten auch auf freiwilliger Basis rechtmäßig sei, zumal Bedenken bestanden, dass bei einem Nicht-Ausfüllen dieser Option 2 das Prüfungsamt besonders kritisch sei und die Prüfungsunfähigkeit möglicherweise nicht anerkenne.

Gemäß Art. 5 Abs. 1 Buchstabe a) Datenschutz-Grundverordnung (DS-GVO) muss die Verarbeitung von personenbezogenen Daten nachvollziehbar und rechtmäßig erfolgen. Die Voraussetzungen für eine rechtmäßige Datenverarbeitung sind in Art. 6 DS-GVO aufgeführt. Nach Art. 5 Abs. 1 Buchstabe b) DS-GVO dürfen personenbezogene Daten zudem nur für festgelegte, eindeutige und legitime Zwecke verarbeitet werden. Zweck in diesem Falle war die Feststellung der Prüfungsunfähigkeit. Da im von der Hochschule verwendeten Formular auch besondere Kategorien personenbezogener Daten, nämlich Gesundheitsdaten, verarbeitet werden sollten, war für die Prüfung der Rechtmäßigkeit außerdem Art. 9 Abs. 2 DS-GVO einschlägig. Danach ist die Verarbeitung von personenbezogenen Gesundheitsdaten ausnahmsweise dann rechtmäßig, wenn sie zur Erfüllung einer rechtlichen Verpflichtung, der der Verantwortliche unterliegt, erforderlich ist und auf der Grundlage einer entsprechenden nationalen Rechtsnorm erfolgt (Art. 6 Abs. 1 Satz 1 Buchstabe c) DS-GVO in Verbindung mit Art. 9 Abs. 2 Buchstabe g) DS-GVO).
Verantwortliche Stelle für die Verarbeitung der personenbezogenen Daten ist die Leitung beziehungsweise das Prüfungsamt der Hochschule. Rechtsgrundlage für die Angaben personenbezogener Daten zur Feststellung der Prüfungsunfähigkeit ist § 54 Abs. 11 Thüringer Hochschulgesetz (ThürHG) in Verbindung mit § 55 Abs. 2 Nr. 16 ThürHG.
In § 54 Abs. 11 ThürHG heißt es: „Für den Nachweis der krankheitsbedingten Prüfungsunfähigkeit reicht eine ärztliche Bescheinigung über das Bestehen der Prüfungsunfähigkeit aus, es sei denn, es bestehen zureichende tatsächliche Anhaltspunkte, die eine Prüfungsfähigkeit als wahrscheinlich annehmen oder einen anderen Nachweis als sachgerecht erscheinen lassen. Bestehen derartige Anhaltspunkte, ist die Hochschule berechtigt, auf ihre Kosten eine amtsärztliche Bescheinigung zu verlangen.“
In der Option 1 des Formulars sollte durch die Ärztin beziehungsweise den Arzt lediglich per Ankreuzverfahren bescheinigt werden, für welche Form der Prüfungsleistung eine krankheitsbedingte Prüfungsunfähigkeit vorliegt. Weitere gesundheitliche Angaben mussten dabei nicht gemacht werden. Die Verarbeitung von personenbezogenen Daten in dieser Form ist daher zulässig (Art. 5 Abs. 1 Buchstabe a) DS-GVO und Art. 5 Abs. 1 Buchstabe b) DS-GVO in Verbindung mit Art. 6 Abs. 1 Satz 1 Buchstabe c) DS-GVO in Verbindung mit Art. 9

Abs. 2 Buchstabe g) DS-GVO in Verbindung mit § 54 Abs. 11 ThürHG). Soweit kein (datenschutzrechtliches) Problem.
Die Option 2 des von der Hochschule entworfenen Formulars forderte hingegen konkretere Angaben zu Symptomen und medizinischen Diagnosen sowie ICD-Codes und die daraus resultierende Art der physischen beziehungsweise psychischen Leistungseinschränkung. Für diese detaillierte Angabe von Gesundheitsdaten lässt sich jedoch aus § 54 Abs. 11 ThürHG keine Rechtsgrundlage im Sinne von Art. 6 Abs. 1 Satz 1 Buchstabe c) DS-GVO in Verbindung mit Art. 9 Abs. 2 Buchstabe g) DS-GVO ableiten. Auch eine andere Rechtsgrundlage ist nicht vorhanden. Wenngleich diese Angaben als „freiwillig“ gekennzeichnet waren und damit einer Einwilligung gemäß Art. 9 Abs. 2 Buchstabe a) DS-GVO unterliegen könnten, sind diese Angaben nicht für die Feststellung der Prüfungsunfähigkeit gemäß § 54 Abs. 11 ThürHG erforderlich. Nach Erwägungsgrund 39 DS-GVO dürfen personenbezogene Daten nur in dem für den Zweck notwendigen Maß und auch nur dann verarbeitet werden, wenn für den Zweck nicht ein geeigneteres Mittel vorhanden ist, welches die betroffene Person weniger belastet. Da der Zweck – der Nachweis der Prüfungsunfähigkeit – bereits mit den unter der Option 1 gemachten Angaben des Formulars erfüllt werden konnte, war die Option 2, bei der darüber hinaus Gesundheitsdaten abgefragt wurden, nicht erforderlich und daher aus datenschutzrechtlicher Sicht unzulässig.
Noch bevor der TLfDI die Hochschule angeschrieben und die Rechtslage erläutert hatte, war die Hochschule bereits tätig geworden und hatte das Formular von sich aus entsprechend den datenschutzrechtlichen Grundlagen geändert und die Option 2, bei der Symptome und Diagnosen angegeben werden konnten, wurde gestrichen. Der TLfDI hat die Hochschulleitung aufgefordert, eventuell bereits von Studierenden unter Option 2 gemachte Angaben zu löschen. Dieser Aufforderung ist die Hochschule unverzüglich nachgekommen, verbunden auch mit dem Hinweis, dass die Verwendung des Formblatts generell nicht vorgeschrieben sei und die Studierenden auch die Möglichkeit hätten, eine durch die Ärztin beziehungsweise den Arzt frei formulierte Bescheinigung vorzulegen.
Gemäß Erwägungsgrund 129 der DS-GVO war danach abzuwägen, ob eine Maßnahme nach Art. 58 Abs. 2 Buchstabe b) DS-GVO, das heißt der Ausspruch einer Verwarnung, unter Berücksichtigung der Umstände des vorliegenden Falls geeignet, erforderlich und angemes-

sen wäre. Die Hochschule hatte die Verwendung des Formulars ausdrücklich nicht vorgeschrieben und die Angaben der Symptome beziehungsweise der Diagnose explizit mit dem Zusatz „freiwillig“ gekennzeichnet. Zudem hatte die Hochschule das Formular bereits kurz nach Veröffentlichung wieder zurückgezogen und ist einer entsprechenden Aufforderung des TLfDI sogar zuvorgekommen. Daher wurde im vorliegenden Fall von einer Verwarnung abgesehen.

2.16 Beschwerde über Versand von Langzeitstudiengebührenbescheiden an alle Betroffenen durch eine Thüringer Hochschule

Verpatzte Prüfung, ernsthaft erkrankt, zu ausgiebig gefeiert, sonstige Ablenkungen – es gibt viele Gründe, warum man die Regelstudienzeit überschreitet. Ärgerlich genug, dass mit jedem extra Semester zusätzliche Studiengebühren entrichtet werden müssen, noch ärgerlicher allerdings, wenn alle Betroffenen untereinander einsehen können, wer wie lange für welches Fach benötigt hat und vieles mehr. Dass der Versand aller Gebührenbescheide an alle Langzeitstudierenden per unverschlüsselter E-Mail von einer Thüringer Hochschule erfolgte, hatte eine Beschwerde noch vor dem Eingang der Meldung gemäß Art. 33 DS-GVO zur Folge. Das Beschwerdeverfahren wurde in diesem Fall aufgrund des schwerwiegenden Verstoßes mit einer Verwarnung abgeschlossen.

Dass Bescheide und andere behördliche Texte lange Paragraphenschlangen enthalten, ist nicht ungewöhnlich, aber eine ganze Reihe von Studierenden einer Thüringer Hochschule staunte nicht schlecht, als sie eine E-Mail mit dem Betreff „Bescheid zur Langzeitstudiengebührenpflicht im Wintersemester 2023/2024“ erhielt und das angefügte Dokument rund 550 Seiten lang war. Schnell stellte sich heraus, dass der Gebührenbescheid für den Empfänger lediglich drei Seiten umfasste, alle anderen Seiten waren mit Bescheiden der weiteren fast 200 betroffenen Langzeitstudierenden gefüllt. Zu lesen waren neben dem Namen und Vornamen auch die Matrikelnummer, der Studiengang, der geplante Studienabschluss, die bereits absolvierten Hochschulsemester sowie eventuelle Minderungs- und Urlaubssemester.
Dass hier ein Datenschutzverstoß vorlag, war mehr als offensichtlich, und so erreichte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit auch gleich eine Beschwerde eines

Betroffenen. Zeitlich kurz danach meldete die Hochschule auch selbst den Fall in einer Meldung nach Art. 33 Datenschutz-Grundverordnung (DS-GVO). Danach ist der Verantwortliche – hier die Hochschulleitung – verpflichtet, bei einer Verletzung des Schutzes von personenbezogenen Daten unverzüglich die zuständige Aufsichtsbehörde – den TLfDI – zu informieren und unter anderem darzulegen, welche Art von Verletzung des Schutzes personenbezogener Daten stattgefunden hat, welche Folgen diese haben kann und welche Maßnahmen vom Verantwortlichen ergriffen wurden, um die möglichen nachteiligen Auswirkungen für die Betroffenen abzumildern.
Die Hochschule schilderte, dass unmittelbar nach Bekanntwerden der Datenpanne ein Teil der versendeten E-Mails händisch zurückgerufen werden konnte. Ein vollständiger Rückruf war aus technischen Gründen nicht möglich. Alle weiteren Studierenden wurden in einer zweiten E-Mail angeschrieben, über die Verletzung ihrer personenbezogenen Daten informiert und zur Löschung des Datensatzes aufgefordert.
Im Beschwerdeverfahren hörte der TLfDI die Hochschule dazu an, warum die Bescheide nicht per verschlüsselter E-Mail oder postalisch versendet wurden und welche Maßnahmen geplant seien, um einen solchen Verstoß künftig zu vermeiden. Die Hochschule gab an, dass beim postalischen Versand in der Vergangenheit ein großer Prozentsatz der Schreiben wegen veralteter Adressen nicht mehr zugestellt werden konnte. Man sei derzeit dabei, den Prozess der Benachrichtigung zu überdenken. Dabei seien verschiedene Varianten in der Prüfung, beispielsweise die Bescheide im pdf-Format in einem eigenen Studienportal oder auf einer anderen datenschutzkonformen Plattform, zu der jeder Studierende sein eigenes Login habe, zum Abruf bereitzustellen und lediglich eine Benachrichtigung per E-Mail zu versenden, dass das Dokument zum Download bereitstehe. Bis diese Prüfung abgeschlossen und ein neues Verfahren etabliert sei, werde der Versand im Vier-Augen-Prinzip mit einem Zeitversatz von 30 Minuten abgewickelt.
Wegen des gravierenden Datenschutzverstoßes hat der TLfDI die Hochschule gemäß Art. 58 Abs. 2 Buchstabe b) DS-GVO verwarnt. Außerdem wurde die Hochschule dazu aufgefordert, den TLfDI zu informieren, sobald eine Entscheidung über das Verfahren zum künftigen Versand datenschutzrelevanter Dokumente getroffen wurde.

2.17 Anfrage von Schülern zur Erstellung eines Instagram-Accounts für die Schule im Rahmen einer Seminarfacharbeit

Dass Instagram, Facebook und Co. für die schulische Nutzung ein No-Go sind, hat sich mittlerweile herumgesprochen. Aber was ist, wenn Schüler selbst einen Instagram-Account betreiben wollen, um für ihre Schule zu werben? Ist dies auch dann ein privater Account, wenn die Schülerinnen und Schüler ihn im Rahmen ihrer Seminarfacharbeit anlegen?

Mit Interviews in den Medien, Briefen an die Schulleitungen, in Fort- und Weiterbildungen für Lehrkräfte und zahllosen Gesprächen hat der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) davor gewarnt, Social Media Plattformen wie Instagram oder Facebook für schulische Zwecke zu nutzen. Ein Erfolg dieser Aufklärung las sich aus einem Brief, den eine Gruppe von Schülerinnen und Schülern der 11. Klasse eines Thüringer Gymnasiums an den TLfDI geschickt hatten. Die Gymnasiasten wollten im Rahmen ihrer obligatorischen Seminarfacharbeit einen Instagram-Account anlegen, schrieben aber, dass ihnen bewusst sei, dass die Nutzung von Instagram für Schulen rechtlich unzulässig sei.
Unter der Bedingung, dass der Account nicht von der Schule, sondern von ihnen selbst verantwortet werde, erhoffte sich die Gruppe vom TLfDI Antworten, unter welchen Voraussetzungen auf diesem Kanal über schulische Aktivitäten, Veranstaltungen und Neuigkeiten berichtet werden könne. Bevor mit der Seminarfacharbeit begonnen werde, wolle man sichergehen, hier keinen datenschutzrechtlichen Verstoß zu begehen.
Als Erfolg wertete der TLfDI die Anfrage und lobte die Jugendlichen für ihre datenschutzrechtliche Sensibilität und ihren Weitblick, die Anfrage zu stellen, bevor der Instagram-Account eingerichtet wurde. In einer ausführlichen Antwort, die auch als Argumentationshilfe für die Seminarfacharbeit verwendet werden konnte, begründete er seine rechtliche Einschätzung.
Das US-amerikanische Technologieunternehmen „Meta“ (Meta Platforms Inc.), zu dem neben Instagram unter anderem auch Facebook und WhatsApp gehören, verarbeitet in großem Umfang personenbezogene Daten, die für die Nutzer der Dienste zum Teil nur schwer nachvollziehbar sind. So ist es Instagram zum Beispiel möglich, die Nutzeraktionen und auch die Verweildauer auf einer Instagram-Seite

extrem detailliert zu erfassen. Alle weiteren Verarbeitungen dieser detaillierten Überwachungsdaten finden auf den Servern von Instagram statt. Was damit passiert, ist Betriebsgeheimnis. Es ist nur bekannt, dass Instagram und Facebook die Daten gemeinsam zu Profilen verarbeiten. Diese so erstellten Profile können nach demografischen Daten oder anderen Kriterien gefiltert werden, damit Werbetreibende gezielt Personenbereiche ansprechen können. Aber auch politische, religiöse oder gesellschaftliche Werte der Nutzer können erfasst und so auch durch das Ausspielen gezielter (Des-)Information Meinungen beeinflusst werden. Diese Statistiken und die daraus folgenden Algorithmen werden aus den gesammelten Einzeldaten generiert, welche jeweils immer einen Personenbezug haben.

Es findet also eine umfangreiche Verarbeitung personenbezogener Daten statt. Die europäische Datenschutz-Grundverordnung (DS-GVO) schreibt vor, dass personenbezogene Daten nur mit einer Rechtsgrundlage verarbeitet werden dürfen (Art. 5 Abs. 1 Buchstabe a) in Verbindung mit Art. 6 Abs. 1 DS-GVO). Sollte eine Schule einen eigenen Instagram-Account betreiben wollen, müsste es dafür also eine Regelung im Thüringer Schulgesetz oder in der Thüringer Schulordnung geben, in der festgelegt ist, dass ein solcher Account für die Erfüllung der schulischen Aufgaben erforderlich ist. Zum einen gibt es jedoch keine solche Regelung, zum anderen ist fraglich, ob diese umfangreiche Datenverarbeitung, wie sie durch Meta erfolgt, überhaupt für die Erfüllung der schulischen Aufgaben erforderlich wäre – aus datenschutzrechtlicher Sicht wäre das zu verneinen. Dazu kommen weitere Pflichten der Schule als Verantwortliche, wie den Betroffenen Auskunft zu erteilen, unter anderem über die Verarbeitungszwecke, die Empfänger, gegenüber denen die personenbezogenen Daten offengelegt werden sowie die Information über das Recht auf Löschung der personenbezogenen Daten, die eine Schule nur über einen Auftragsverarbeitungsvertrag mit Meta Platforms Inc. lösen könnte. Der TLfDI hat jedoch erhebliche Zweifel, ob dies in der für einen datenschutzkonformen Betrieb notwendigen Form überhaupt möglich ist.

Auch wenn der Instagram-Account im vorliegenden Fall nicht von der Schulleitung selbst erstellt und verantwortet werden sollte, sondern von Schülerinnen und Schülern im Rahmen einer Seminarfacharbeit, war fraglich, ob nicht die Schule diesen Account als „Umweg“ dazu nutzen könnte, ihre Informationen auf einer nicht datenschutzkonformen Plattform zu verbreiten. Sofern die Schülerinnen und Schüler,

wie in ihrer Anfrage erläutert, Informationen über schulische Aktivitäten, Veranstaltungen, Projekte und Neuigkeiten auf dem Account posten wollten, um Schüler, Eltern und die Öffentlichkeit zu informieren, hat dies aus Sicht des TLfDI keinen privaten Charakter mehr, insbesondere, da die Informationen, die geteilt werden sollten, zumindest zum Teil von der Schulleitung beziehungsweise Lehrkräften kommen würden und der Account im Rahmen einer schulischen Aufgabe (Seminarfacharbeit) erstellt und betrieben werden sollte.
Der TLfDI hat den Gymnasiasten daher von der Erstellung eines Instagram-Accounts im Zusammenhang mit einer Seminarfacharbeit dringend abgeraten.

3. Fälle nicht-öffentlicher Bereich



Erfolg Kurve Hand - Pixabay

3.1 Insolvenzverwalter hat Verpächterdaten an die Käuferinnen der Insolvenzschuldnerin weitergegeben

Auch im Rahmen eines Insolvenzverfahrens sind durch den jeweiligen Insolvenzverwalter die Vorgaben der DS-GVO zu beachten. Im Rahmen eines „Asset-Deals“ werden einzelne Wirtschaftsgüter eines insolventen Unternehmens ohne ihren Rechtsträger durch den Insolvenzverwalter veräußert. Werden dabei personenbezogene Daten von Kunden oder Vertragspartnern des insolventen Unternehmens an die Erwerber übermittelt, so bedarf diese Übermittlung datenschutzrechtlich einer Rechtsgrundlage.

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) erhielt aufgrund eines Hinweises Kenntnis von dem folgenden Sachverhalt:
Der Hinweisgeber ist Eigentümer von einzelnen landwirtschaftlichen Flächen. Dieser hatte landwirtschaftliche Flächen an ein Agrarunternehmen verpachtet (im folgenden „Pächterin“ genannt). Er staunte nicht schlecht, als plötzlich ein anderes Agrarunternehmen, mit dem er gar keinen Vertrag geschlossen hatte, dessen Name der bisherigen Pächterin aber zum Verwechseln ähnlich klang, mit einem Schreiben an ihn herantrat und über eine Kündigung des Pachtvertrags mit ihm

verhandeln wollte. Der Hinweisgeber und Verpächter brachte daraufhin in Erfahrung, dass über das Vermögen der bisherigen Pächterin das Insolvenzverfahren eröffnet worden war und dass die Daten der Verpächter durch den Insolvenzverwalter der Pächterin an das andere Agrarunternehmen übermittelt worden waren. Das Agrarunternehmen hatte Teile des Geschäftsbetriebes sowie einzelnen Grundbesitz der insolventen Pächterin erworben. Um prüfen zu lassen, ob es bei der Übermittlung der Verpächterdaten durch den Insolvenzverwalter mit rechten Dingen zugegangen war, wandte sich der Hinweisgeber mit einer Anzeige über den Insolvenzverwalter an den TLfDI.
Die Datenschützer vom TLfDI wandten sich daraufhin mit mehreren Auskunftsverlangen an den Insolvenzverwalter, um den Sachverhalt vollständig zu ermitteln. Im Rahmen seiner Auskunft trug der Insolvenzverwalter vor, dass er als Insolvenzverwalter über das Vermögen der Pächterin einen notariellen Kaufvertrag mit vier Käuferinnen (im folgenden „Erwerberinnen“) geschlossen hatte, darunter das Agrarunternehmen, welches an den Hinweisgeber herangetreten war und einen ähnlichen Namen wie die bisherige Pächterin trug. Gegenstand des Kaufvertrags sei der im Eigentum der Insolvenzschuldnerin, also der Pächterin, stehende Grundbesitz einschließlich der darauf stehenden Biogasanlagen gewesen. Im Rahmen des Abschlusses des notariellen Kaufvertrags übergab der Insolvenzverwalter dann den Erwerberinnen eine Liste mit Pachtverträgen. Die Liste enthielt Angaben zu den Namen und Vornamen der Verpächter sowie zum Ende des jeweiligen Pachtverhältnisses, dem Preis, dem Flurstück, der Fläche, der Größe, der Gemarkung und der Nutzung. Der Insolvenzverwalter holte weder die Einwilligung der betroffenen Verpächter vor der Übermittlung ein, noch informierte er diese über die Übermittlung.
Der Insolvenzverwalter stellte sich auf den Standpunkt, dass die Übermittlung der Verpächterdaten an die Erwerberinnen auf der Grundlage des Art. 6 Abs. 1 Satz 1 Buchstabe f) Datenschutz-Grundverordnung (DS-GVO) zulässig gewesen sei. Die Erwerberinnen hätten das wesentliche Asset der Pächterin beziehungsweise der Insolvenzschuldnerin erworben. Der Geschäftsbetrieb der Insolvenzschuldnerin sei im Wesentlichen durch die Erwerberinnen übernommen worden. Die dem Kaufvertrag beigefügte Auflistung der Verpächter sei für die Erwerberinnen auch von Bedeutung gewesen, um auf die Verpächter zugehen zu können und die Übernahme oder Neuverhandlung von Pachtverträgen verhandeln zu können. Die vorherige Zustimmung der

Verpächter einzuholen, sei im Agrarbereich nicht praktikabel und hätte eines unverhältnismäßigen Aufwands bedurft.
Nach Prüfung der Sach- und Rechtslage durch den TLfDI bewertete dieser die Vorgehensweise des Insolvenzverwalters als Verstoß gegen Art. 5 Abs. 1 Buchstabe a) DS-GVO.
Nach dieser Vorschrift müssen personenbezogene Daten unter anderem auf rechtmäßige Weise verarbeitet werden („Rechtmäßigkeit“). Nach Art. 6 Abs. 1 Satz 1 DS-GVO ist eine Verarbeitung nur rechtmäßig, wenn mindestens eine der in den Buchstaben a) bis f) genannten Bedingungen erfüllt ist.
Die Liste mit den Pachtverträgen enthielt personenbezogene Daten der Verpächter. Die Übermittlung dieser Liste an die Erwerberinnen des Grundbesitzes der Insolvenzschuldnerin stellte eine Verarbeitung im Sinne des Art. 4 Nr. 2 DS-GVO dieser Daten dar.
Da der Insolvenzverwalter in seiner Eigenschaft als Insolvenzverwalter den Kaufvertrag mit den Erwerberinnen abschloss und dabei die Verpächterdaten übermittelte, handelte er auch als Verantwortlicher nach Art. 4 Nr. 7 DS-GVO, da er die Zwecke und Mittel der Verarbeitung von Daten der Verpächter festlegte.
Als Rechtsgrundlage für die Verarbeitung der Verpächterdaten kam allein Art. 6 Abs. 1 S. 1 Buchstabe f) DS-GVO in Betracht. Danach ist die Verarbeitung von personenbezogenen Daten rechtmäßig, wenn sie 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
Der TLfDI nahm zunächst ein berechtigtes Interesse sowohl des Insolvenzverwalters als Verantwortlichem als auch der Erwerberinnen als Dritte an. Das berechtigte Interesse des Insolvenzverwalters ergab sich dabei aus dessen Verpflichtung nach § 159 Insolvenzordnung, aus dem schuldnerischen Vermögen den höchstrealisierbaren Ertrag zu erzielen, um eine bestmögliche Befriedigung der Gläubiger sicherzustellen. Das berechtigte Interesse der Erwerberinnen folgte aus dem Umstand, dass die Übermittlung der Verpächterdaten nach den Angaben des Insolvenzverwalters der Fortführung des Geschäftsbetriebs der Insolvenzschuldnerin dienen sollte.
Aus Sicht des TLfDI war die Übermittlung der Liste mit den personenbezogenen Daten der Verpächter an die Erwerberinnen allerdings nicht erforderlich. Voraussetzung für die Erforderlichkeit ist, dass kein milderes, gleich effektives Mittel zur Verfügung steht, um die

Interessen des Verantwortlichen oder des Dritten zu erreichen. Hier hätte der Insolvenzverwalter die Möglichkeit gehabt, sich an die jeweiligen Verpächter zu wenden und diese um ihre Zustimmung zur Übernahme der Pachtverträge durch die Erwerberinnen zu ersuchen. Auf diese Weise wären die berechtigten Interessen des Insolvenzverwalters und der Erwerberinnen gleichermaßen gewahrt worden, ohne dass personenbezogene Daten der Verpächter ohne deren Zustimmung an die Erwerberinnen herausgegeben werden mussten. Die Verpächter hätten in diesem Fall selbst die Entscheidungsfreiheit gehabt zu wählen, ob ihre personenbezogenen Daten an die Erwerberinnen herausgegeben werden oder nicht. Auf diese Weise hätte auch eine Beschwerde wie die vorliegende vermieden werden können.
Der Einwand des Insolvenzverwalters, die Einholung der Zustimmung jedes Verpächters sei im Agrarbereich nicht praktikabel, überzeugte den TLfDI nicht. Zwar kann die Ermittlung von Verpächtern und die Kontaktaufnahme mit diesen einen erheblichen Aufwand verursachen. Die Möglichkeit einer schnellen und effektiven Gläubigerbefriedigung entbindet einen Insolvenzverwalter aber nicht von der Beachtung datenschutzrechtlicher Vorgaben. Die DS-GVO enthält keine allgemeine Regelung, wonach von der Beachtung der datenschutzrechtlichen Grundsätze abgesehen werden kann, wenn diese einen unverhältnismäßigen Aufwand verursachen. Grundsätzlich müssen die Regelungen des Insolvenzrechts mit den datenschutzrechtlichen Bestimmungen in Einklang gebracht werden.
Des Weiteren überwog im Rahmen der nach Art. 6 Abs. 1 S. 1 Buchstabe f) DS-GVO zu treffenden Interessenabwägung das Recht auf informationelle Selbstbestimmung der betroffenen Verpächter nach Art. 8 Abs. 1 EU-Grundrechte-Charta (EU-GR-Charta) das berechtigte Interesse des Insolvenzverwalters und der Erwerberinnen.
Hierbei war zunächst zu beachten, dass die Veräußerung des Grundbesitzes der Pächterin durch den Insolvenzverwalter an die Erwerberinnen im Rahmen eines „Asset-Deals“ erfolgte. Bei einem „Asset-Deal“ werden die jeweiligen Vermögensgüter eines Unternehmens ohne ihren Rechtsträger veräußert. Zurück bleibt dann der insolvente Rechtsträger, der abgewickelt wird. Werden im Rahmen eines Asset-Deals personenbezogene Daten durch den Verkäufer an die Käufer übermittelt, so liegt eine Verarbeitung personenbezogener Daten sowohl durch Verkäufer als auch durch die Käufer vor, die einer Rechtsgrundlage nach Art. 6 DS-GVO bedarf.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat hierzu einen Katalog von Fallgruppen entwickelt, die im Rahmen der Interessenabwägung nach Art. 6 Abs. 1 S. 1 Buchstabe f) in Verbindung mit Abs. 4 DS-GVO bei einem „Asset-Deal“ zu berücksichtigen sind. Erfasst wird insbesondere die Fallgruppe, dass Kundendaten bei laufenden Verträgen übertragen werden sollen. Hierbei stellt die DSK darauf ab, dass der Vertragsübergang zivilrechtlich einer Genehmigung der Kunden bedarf und sieht in der zivilrechtlichen Genehmigung als Minus auch die datenschutzrechtliche Zustimmung zum Übergang der erforderlichen Daten. Das bedeutet, dass die (zivilrechtliche) Genehmigung der Kunden **vor der Übermittlung** ihrer personenbezogenen Daten an einen Erwerber eingeholt werden muss. Im Fall des Insolvenzverwalters bestand allerdings die Besonderheit, dass keine Kundendaten, sondern die Daten von Vertragspartnern der Pächterin, den Verpächtern der landwirtschaftlichen Flächen, betroffen waren. Der TLfDI stützte sich bei seiner rechtlichen Bewertung gleichwohl auf diese Fallgruppe, da aus seiner Sicht eine vergleichbare Interessenlage zwischen Kundendaten und den Daten der Verpächter bestand. Auch in dieser Konstellation hätte daher vor der Übermittlung der personenbezogenen Daten der betroffenen Verpächter eine zivilrechtliche Genehmigung eingeholt werden müssen (vergleich § 415 Abs. 1 Bürgerliches Gesetzbuch). Nach den Angaben des Insolvenzverwalters wurden die Verpächter jedoch vor der Übermittlung ihrer Daten weder informiert noch wurde ihre Zustimmung zur Weitergabe der Daten eingeholt.
Darüber hinaus war bei der Interessenabwägung zu berücksichtigen, dass die übermittelten Daten zwar einen wirtschaftlichen, aber keinen rechtlichen Bezug zu dem notariellen Kaufvertrag über das Vermögen der Pächterin aufwiesen. Der Insolvenzverwalter hat sich zwar insoweit darauf berufen, dass die Erwerberinnen den Geschäftsbetrieb der Pächterin fortführen sollten. Allerdings war Gegenstand des notariellen Kaufvertrags die Veräußerung des Grundbesitzes der Pächterin. Ein Übergang der Pachtverträge zwischen Verpächtern und Pächterin auf die Erwerberinnen war hiermit jedoch nicht verbunden. Die Veräußerung der Pachtverträge an die Erwerberinnen hätte somit eines weiteren Rechtsaktes bedurft, da der Grundbesitz und die Pachtverträge unterschiedliche Vermögensgegenstände aus dem Vermögen der Pächterin darstellen. Eine Veräußerung der Pachtverträge an die Erwerberinnen war jedoch nicht vorgetragen worden.

Damit kam der TLfDI zu dem Ergebnis, dass die Übermittlung der Verpächterdaten an die Erwerberinnen unzulässig war. Der Insolvenzverwalter als Verantwortlicher für diese Datenverarbeitung wurde deshalb nach Art. 58 Abs. 2 Buchstabe b) DS-GVO wegen des Verstoßes gegen Art. 5 Abs. 1 Buchstabe a) DS-GVO verwarnt.

3.2 Ausweiskopie bei Blutspende nicht erforderlich

Auch wenn eine Rechtsgrundlage zur Verarbeitung von Personalausweisdaten vorliegt, muss die Kopie des amtlichen Personaldokuments für die Zweckerfüllung auch erforderlich sein. Sofern eine mildere Alternative zur Verfügung steht, ist die Kopie des Personalausweises nicht erforderlich. Das kann der Abgleich mit dem Personaldokument oder die Benutzung einer Kopierschablone sein. Der Inhaber kann nur mit einer wirksamen Einwilligung der Personalausweiskopie zustimmen.

Mit einer Beschwerde erhielt der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) Kenntnis von einer unbefugten Datenverarbeitung eines Blutspendedienstes. Der Beschwerdeführer hatte sich als Spender registrieren lassen. Zu diesem Zeitpunkt war eine Registrierung jedoch nur möglich, nachdem er einer Kopie seines Personalausweises zugestimmt hatte. Die Mitarbeiterin des Blutspendedienstes teilte mit, dass ohne die Anfertigung einer Ausweiskopie eine Registrierung nicht möglich sei. Die Mitarbeiterin berief sich hierbei auf eine nicht näher genannte Dienstanweisung. Sie konnte keine Auskunft über den Verbleib, die Aufbewahrung oder die Vernichtung der Kopie machen. Bezüglich des Zweckes deutete sie an, die EDV-Abteilung benötige diese zum Abgleich der Adressdaten.
Im Rahmen des Verwaltungsverfahren war zu prüfen, zu welchem Zweck und aufgrund welcher Rechtsgrundlage die Verarbeitung der Personalausweiskopie durch den Blutspendedienst stattfand. Weiterhin waren die technisch-organisatorischen Maßnahmen in Verbindung mit der Aufbewahrung und Vernichtung der Personalausweiskopien zu prüfen.
Im Ergebnis eines Auskunftsverlangens nach § 40 Abs. 4 Bundesdatenschutzgesetz (BDSG) trug der Blutspendedienst vor, als Arzneimittelproduzent Blutspenden durchzuführen, um die Versorgung der Bevölkerung mit Blut und Blutbestandteilen sicherzustellen. Im Rahmen

dieser Tätigkeit unterliege sie den Vorgaben des Gesetzes zur Regelung des Transfusionswesens (TFG) und der „Richtlinie zur Gewinnung von Blut und Blutbestandteilen und zur Anwendung von Blutprodukten“. Demzufolge sei anlässlich jeder Spende beziehungsweise jeder spendenbezogenen Untersuchung die Identität des Spenders ohne die Gefahr einer Verwechslung festzustellen (gültiges amtliches Personaldokument mit Lichtbild). Die Schwarz-Weiß-Kopie des amtlichen Personaldokuments bei Erstspendern werde zur Erhöhung der Sicherheit der Feststellung der zweifelsfreien Identität zum Zweck der Nachkontrolle und Korrektur der schon erhobenen Daten im Sinne eines Vier-Augen-Prinzips angefertigt. Die fehlerfreie Datenerhebung sei Grundlage der Identitätssicherung bei Folgespenden des gleichen Spenders. Die Identifizierung des Spenders und die Anfertigung einer Personalausweiskopie erfolge auf der Grundlage von Arbeitsanweisungen. Die Vorgangsbeschreibungen der Spenderregistrierung, der Identitätsprüfung und auch der Kopie des Personalausweises/Reisepasses wurden dem TLfDI unter Vorlage der einschlägigen Arbeitsanweisungen nachgewiesen.
Für die Erhebung der Personalausweiskopie nutzte der Blutspendedienst eine „Datenschutz- und Einwilligungserklärung“. Mit einer Anlage „Informationen zur Datenschutz- und Einwilligungserklärung“ wurden die nach Art. 13 Datenschutz-Grundverordnung (DS-GVO) geforderten Informationen im Zusammenhang mit der Datenverarbeitung abgedruckt. Die Einwilligung zielte darauf ab, die Informationen nach Art. 13 DS-GVO zur Kenntnis zu nehmen und den darin beschriebenen Datenverarbeitungen und Rechtsgrundlagen zuzustimmen.
Nach der rechtlichen Prüfung kam der TLfDI zu dem Ergebnis, dass der Blutspendedienst hinsichtlich der Verarbeitung personenbezogener Daten im Zusammenhang mit der Spenderregistrierung und Identitätsfeststellung Verantwortlicher im Sinne des Art. 4 Nr. 2 DS-GVO ist. Er erhebt und speichert personenbezogene Daten der (Erst-)Spender, um eine Blutspende zu ermöglichen. Eine Verarbeitung von personenbezogenen Daten nach Art. 4 Nr. 2 DS-GVO lag somit vor. 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 damit letztlich um ein Verbot mit Erlaubnisvorbehalt. Die Verarbeitung der personenbe-

zogenen Daten der (Erst-)Spender im Zusammenhang mit der Spenderregistrierung und der Blutspende erfolgte unrechtmäßig. Nach der „Richtlinie zur Gewinnung von Blut und Blutbestandteilen und zur Anwendung von Blutprodukten“ sind zur Spenderregistrierung Name, Vorname, Geburtsdatum, Geschlecht und Adresse des Spenders zu erfassen. Alle Spenderdaten unterliegen der ärztlichen Schweigepflicht und den Bestimmungen des Datenschutzes. Als gültiges amtliches Personaldokument sind der Personalausweis und der Reisepass anzusehen. Darüber hinaus unterliegt der Blutspendedienst dem TFG.
Folglich ist die Erhebung und Verarbeitung der zweifelsfreien Identität eines Spenders nach Art. 6 Abs. 1 Buchstabe c) DS-GVO erforderlich, um den rechtlichen Verpflichtungen aus dem TFG und der Richtlinie zur Gewinnung von Blut und Blutbestandteilen und zur Anwendung von Blutprodukten nachzukommen. Darin wird allerdings nur die Erfassung von Name, Vorname, Geburtsdatum, Geschlecht und Adresse des Spenders gefordert. Der Personalausweis enthält neben diesen Daten noch weitere sensible Daten, die für eine Identitätsfeststellung des Spenders nicht erforderlich sind. Das gilt insbesondere für die auf dem Ausweis aufgedruckte Zugangsnummer sowie die Seriennummer, sofern nicht gesetzliche Regelungen diese Angaben erfordern, zum Beispiel das Geldwäschegesetz (https://www.personalausweisportal.de/DE/Buergerinnen-und-Buerger/Der-Personalausweis/Ausweis_kopieren/ausweis_kopieren_node.html). Ausweisdaten, die nicht zur Identifizierung benötigt werden, dürfen nicht kopiert werden. Aus den Festlegungen des Arzneimittelgesetzes und der Arzneimittel- und Wirkstoffherstellungsverordnung ergibt sich, dass alle Arzneimittelhersteller ein Dokumentationssystem unterhalten, in dem jeweils alle durchgeführten Tätigkeiten im Zusammenhang mit der Herstellung von Arzneimitteln beschrieben sind. Bei dem Blutspendedienst waren diese Anforderungen in den Arbeitsanweisungen enthalten. So hieß es: „… Der Personalausweis oder ggf. der Reisepass werden nach Möglichkeit kopiert, um später zur EDV mäßigen Erfassung bzw. zum Abgleich der Daten genutzt werden zu können …“. Diese Erfassung erfolgte am Tag nach der durchgeführten Spende durch speziell ausgebildete und geschulte Mitarbeiter der Abteilung EDV / Blutbankmanagementsystem. Diese Mitarbeiter verglichen und kontrollierten die Daten, die vom Aufnahmepersonal im Blutbankmanagementsystem erfasst wurden, mit den Daten der Kopie des amtlichen

Personaldokuments. Dabei wurden festgestellte Fehler korrigiert. Somit wurde durch ein Vier-Augen-Prinzip eine fehlerfreie Erfassung der Spenderdaten sichergestellt.
Der TLfDI stellte fest, dass eine Erhebung und Verarbeitung über den Namen, den Vornamen, das Geburtsdatum, das Geschlecht und die Adresse des Spenders hinaus nicht erforderlich und auch nicht rechtmäßig war.
Die Verarbeitung personenbezogener Daten der Personalausweiskopie von Erstspendern im Zusammenhang mit dem Registrierungsvorgang/der Identitätsfeststellung verstieß damit gegen die Regelungen des Datenschutzrechts. Daher waren bei der Erstellung der Personalausweiskopie alle nicht gesetzlich geforderten Ausweisdaten mittels einer Kopierschablone vom Kopiervorgang auszuschließen, da nur so eine zuverlässige Unkenntlichmachung der Daten beim Kopierprozess herbeigeführt werden konnte. Eine Ausstreichung mit einem schwarzen Marker genügte indes nicht.
Der Inhaber kann den Ausweis grundsätzlich gegenüber nicht-öffentlichen Stellen als Identitätsnachweis und Legitimationspapier verwenden, § 20 Abs. 1 Personalausweisgesetz (PAuswG). Nach Absatz 2 dieser Vorschrift darf der Ausweis nur vom Ausweisinhaber oder von anderen Personen mit Zustimmung des Ausweisinhabers abgelichtet werden. Diese „andere Person“ war beim Blutspendedienst das Aufnahmepersonal, welches die Daten des Spenders aufnimmt. Darüber hinaus sollte der Ausweis in der Weise abgelichtet werden, dass die Ablichtung eindeutig und dauerhaft als Kopie erkennbar war. Dies wurde mit einer Schwarz-Weiß-Kopie des Personalausweises gewährleistet und genügte damit den Anforderungen des Personalausweisgesetzes. Die Erkennbarkeit als Kopie wurde mit einer Erstellung in Monochromstufen (zum Beispiel schwarz-weiß) im Entwurf des Personalausweisgesetzes beschrieben.
Trotz der Erforderlichkeit der Identifizierung des Spenders nach der „Richtlinie zur Gewinnung von Blut und Blutbestandteilen und zur Anwendung von Blutprodukten“ müssen die Vorschriften des Personalausweisgesetzes zur Anfertigung einer Personalausweiskopie eingehalten werden. In § 20 Abs. 1 Satz 3 PAuswG wird geregelt, dass Ablichtungen personenbezogener Daten aus dem Personalausweis nur mit der Einwilligung des Ausweisinhabers von der datenerhebenden und -verarbeitenden Stelle erfolgen dürfen. Dem TLfDI lag ebenfalls die Einwilligungserklärung des Blutspendedienstes vor. Diese eingeholte „Einwilligung“ zur Personalausweiskopie war nicht mit den

Bestimmungen der DS-GVO vereinbar und somit unwirksam. Die Datenverarbeitung war nicht in ausreichend transparenter Form erläutert. Der Blutspendedienst stellte den Spendern im Einwilligungstext nicht die erforderlichen Informationen bereit. Vielmehr wurde auf die Informationspflichten nach Art. 13 und 14 DS-GVO auf der Rückseite der Einwilligung verwiesen. Hierdurch wurde die Kontrolle der Verarbeitung personenbezogener Daten durch den Nutzer illusorisch. Damit fehlte es an der Informiertheit der Einwilligung.
Darüber hinaus erfüllte die Einwilligung in die Anfertigung der Personalausweiskopie nicht die Anforderungen der Freiwilligkeit. Die Erhebung und Verarbeitung sowie spätere Nutzung der Personalausweiskopie war nicht zwingend erforderlich. In der Arbeitsanweisung des Blutspendedienstes hieß es weiterhin: „Lehnt der Spender eine Kopie ab, ist aber eine ordnungsgemäße Identitätssicherung erfolgt, kann er trotzdem zur Spende zugelassen werden (entsprechender Vermerk auf dem Fragebogen) …“. Darüber hinaus war die Registrierung der Erstspender beschrieben: „Der Teamhelfer/Aufnahmeschwester erfasst an Hand des vorgelegten Personaldokuments die persönlichen Daten (Name, Vorname, Geburtsdatum und wenn möglich, auch sofort die Adresse) im Blutbanksystem und druckt einen entsprechenden Fragebogen für den Spender aus. Er/Sie dokumentiert die Überprüfung der Angaben und die Identitätsprüfung durch Unterschrift in dem dafür vorgesehenen Feld auf dem Fragebogen sowie den Stempel ADRESSDATEN GEPRÜFT im Bereich ‚Bemerkungen‘ des Fragebogens.“
Die Erfassung der zur Identifizierung erforderlichen personenbezogenen Daten (Name, Vorname, Geburtsdatum, Anschrift) mittels Erfassungsbogen stellte eine mildere Alternative zur Personalausweiskopie dar. Daher musste die Freiwilligkeit der Erklärung sichergestellt werden, um Wirksamkeit zu entfalten. Freiwillig konnte die Entscheidung der Spender nur dann sein, wenn auch darauf verzichtet werden konnte und der Erklärende dies auch wusste. Die Entscheidung über eine Personalausweiskopie musste nach § 20 Abs. 1 Satz 3 PAuswG den Spendern überlassen bleiben. Daher müssen diese zwischen Einverständnis und Verweigerung wirklich wählen können, also auch nicht latent einem auf ansonsten drohenden Nachteilen beruhenden Zwang zur Einwilligung ausgesetzt sein. Innerhalb der Einwilligungserklärung verwies der Blutspendedienst auf die angefügten „Informationen zur Datenschutz- und Einwilligungserklärung“. Darin war unter „Identität der spendenden Person“ erklärt, dass „bei Erstspendern zur

eindeutigen Erfassung und zum Abgleich der Daten eine Ablichtung/Kopie des gültigen amtlichen Personalausweises oder Reisepasses in Schwarz/Weiß erfolgt.“ Diese Formulierung ließ keinen Rückschluss auf eine etwaige Freiwilligkeit zum Alternativverfahren der Identitätsfeststellung mittels Erfassungsbogen zu.
Aufgrund des Einschreitens des TLfDI passte der Blutspendedienst das Dokumentationssystem über die Beschreibung der Arbeitsabläufe bei der Blutspende an. Damit erfolgt seither die Absicherung einer fehlerfreien Datenerfassung des Erstspenders nur noch durch eine Gegenkontrolle der im Spenderfragebogen eingetragenen Adressdaten bei der Spenderaufnahme. Dabei wird nur noch die Vorlage des Personaldokuments zur Einsichtnahme des anwesenden Spenders einbezogen.
Darüber hinaus wurde durch den TLfDI festgestellt, dass die Aussage der entsprechenden Mitarbeiterin gegenüber dem Beschwerdeführer falsch war, ohne Personalausweiskopie nicht als Erstspender registriert werden zu können. Der Blutspendedienst führte in Auswertung dieser Vorkommnisse mit dem Aufnahmepersonal eine Nachschulung auf Basis der entsprechenden Arbeitsanweisung durch.
Der TLfDI hat das Verfahren gegen den Blutspendedienst mit einer Verwarnung nach Art. 58 Abs. 2 Buchstabe b) DS-GVO abgeschlossen. Eine weitere Maßnahme des TLfDI war nicht notwendig, da der Verantwortliche die Verstöße gegen die Datenschutz-Grundverordnung schon während des Verfahrens bereitwillig abgestellt hat.

3.3 Wenn der Arbeitgeber durch ein arbeitsmedizinisches Tauglichkeitsgutachten mehr erfährt als er sollte

Die Verarbeitung von Gesundheitsdaten ist nach der DS-GVO grundsätzlich untersagt. Eine Ausnahme von diesem Grundsatz ist auch dann nicht anzunehmen, wenn bei der Übermittlung eines arbeitsmedizinischen Tauglichkeitsgutachtens zur Verwendung im Rahmen des betrieblichen Eingliederungsmanagements Diagnosen, die einen Arbeitnehmer betreffen, an den Arbeitgeber übermittelt werden.

Durch eine Beschwerde nach Art. 77 Abs. 1 Datenschutz-Grundverordnung (DS-GVO) erlangte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) Kenntnis davon,

dass ein Unternehmen, welches unter anderem auf arbeitsmedizinische Dienstleistungen spezialisiert ist, Gesundheitsdaten der Beschwerdeführerin an deren Arbeitgeber übermittelt hatte.
Wie sich der Beschwerde und den zur Verfügung gestellten Unterlagen entnehmen ließ, war der hier relevanten Datenverarbeitung ein Erstgespräch zwischen der Geschädigten und ihrem Arbeitgeber im Rahmen des betrieblichen Eingliederungsmanagements vorausgegangen, da diese bereits längere Zeit arbeitsunfähig erkrankt war. In der Folge des Erstgesprächs wurde das Unternehmen, gegen das sich das Bußgeldverfahren richtete, mit der Erstellung eines arbeitsmedizinischen Tauglichkeitsgutachtens beauftragt. Nachdem die hierfür erforderlichen Informationen und medizinischen Unterlagen zusammengetragen worden waren, erstellte ein beim Unternehmen angestellter Arzt das beauftragte Tauglichkeitsgutachten und übersandte dieses einschließlich der relevanten Diagnosen an den Arbeitgeber der Geschädigten. Einer Kenntnis der konkreten Diagnosen durch den Arbeitgeber bedurfte es jedoch zur Durchführung des betrieblichen Eingliederungsmanagements nicht. Hierfür reicht allein die Information, ob beziehungsweise inwieweit ein Beschäftigter für die geschuldete Arbeitsleistung tauglich ist, nicht aber die Gründe hierfür. Auf Grundlage dieser Erkenntnisse leitete der TLfDI umgehend ein Verfahren wegen einer Ordnungswidrigkeit gemäß Art. 83 Abs. 5 Buchstabe a) DS-GVO gegen das Unternehmen ein, dass das Tauglichkeitsgutachten an den Arbeitnehmer verschickt hatte.
Im Rahmen der Anhörung durch den TLfDI gemäß § 55 Ordnungswidrigkeitengesetz, § 163a Abs. 1 Strafprozessordnung räumte der Verteidiger des Unternehmens den Tatvorwurf im Wesentlichen ein, erklärte aber überdies, dass diese Vorgehensweise nicht der gängigen Praxis des Unternehmens entspreche, sondern vielmehr ein einmaliges Versehen darstelle. Die weiteren Ermittlungen des TLfDI bestätigten diese Angaben. Demnach versandte das Unternehmen in der Vergangenheit die arbeitsmedizinischen Tauglichkeitsgutachten immer mit ausgeblendetem Diagnosebereich an die Auftraggeber.
Aufgrund dieser Sach- und Rechtslage erging ein Bußgeldbescheid gegen das Unternehmen. 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. Vorliegend hatte das betroffene Unternehmen mit den Diagnosen Gesundheitsdaten gemäß Art. 4 Nr. 15 DS-GVO verarbeitet, da sich diese auf die körperliche

und geistige Gesundheit der Geschädigten bezogen und daher Informationen über den Gesundheitszustand offenbarten. Der Versand des arbeitsmedizinischen Tauglichkeitsgutachtens an den Arbeitgeber der Geschädigten stellte eine Offenlegung durch Übermittlung der Gesundheitsdaten und damit eine Verarbeitung gemäß Art. 4 Nr. 2 DS-GVO dar. Hierbei hatte das Unternehmen als Verantwortlicher im Sinne des Art. 4 Nr. 7 DS-GVO gehandelt. Da in der Praxis immer einzelne natürliche Personen handeln und Daten verarbeiten, ist zu ermitteln, wem das Handeln zuzurechnen ist, den handelnden Personen selbst oder der Organisation, für die sie gegebenenfalls tätig werden, wobei aus Sicht der Art. 29-Datenschutzgruppe in der Regel der Rechtsträger der juristischen Person als Verantwortlicher betrachtet werden soll und nicht einzelne, handelnde Personen. Sofern natürliche Personen Daten für ihre eigenen Zwecke außerhalb des Tätigkeitsbereichs und der möglichen Kontrolle ihrer Organisation verarbeiten, können sie selbst Verantwortlicher werden. Vorliegend wurde das arbeitsmedizinische Tauglichkeitsgutachten von einem Arzt des Unternehmens unterzeichnet und zur Post gegeben. Diese Handlungen sind dem Unternehmen zuzurechnen, da der Arzt hier nicht zu eigenen, möglicherweise privaten Zwecken handelte, sondern zur Erfüllung des Gutachtenauftrages.
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. Demgegenüber unterliegen Gesundheitsdaten aufgrund ihrer besonderen Schutzbedürftigkeit erhöhten Rechtmäßigkeitsvoraussetzungen, weshalb deren Verarbeitung bis auf wenige, in Art. 9 DS-GVO gesetzlich normierte Ausnahmen verboten ist. Vorliegend konnte die Datenverarbeitung nicht auf eine Einwilligung nach Art. 6 Abs. 1 Satz 1 Buchstabe a), Art. 9 Abs. 2 Buchstabe a) DS-GVO gestützt werden. Hierzu wäre es erforderlich gewesen, dass die Geschädigte vorab und in Kenntnis des Zweckes der Verarbeitung in die Offenlegung ihrer Daten einwilligt hätte. Eine solche Einwilligung lag dem Unternehmen jedoch nicht vor. Die Zulässigkeit der Datenverarbeitung ergab sich auch nicht aus Art. 6 Abs. 1 S. 1 Buchstabe f) DS-GVO, da es bereits an einem berechtigten Interesse fehlte. Allerdings hätte auch die Annahme eines solchen Interesses nicht zu einer Rechtmäßigkeit der Datenverarbeitung geführt, da diese nicht gemäß Art. 9 Abs. 2 Buchstabe h) DS-GVO erforderlich gewesen

wäre. Zusätzlich zu den allgemeinen Grundsätzen der Verarbeitung personenbezogener Daten sind gemäß Erwägungsgrund 51 DS-GVO die speziellen Anforderungen an eine Verarbeitung besonderer Kategorien personenbezogener Daten zu beachten. Art. 9 Abs. 1 DS-GVO bestimmt insoweit ein grundsätzliches Verbot der Verarbeitung von Daten dieser Kategorien. Allerdings werden in Art. 9 Abs. 2 Buchstabe a) bis j) DS-GVO zugleich umfangreiche Ausnahmen von diesem Grundsatz geregelt. Gemäß Art. 9 Abs. 2 Buchstabe h) DS-GVO ist die Verarbeitung von Gesundheitsdaten unter anderem dann nicht untersagt, wenn die Verarbeitung für die Beurteilung der Arbeitsfähigkeit von Beschäftigten erforderlich ist. Allerdings ist das Ziel des Betrieblichen Eingliederungsmanagements, dass Arbeitgeber und Arbeitnehmer gemeinsam nach Lösungen suchen, mit denen eine vorliegende Arbeitsunfähigkeit des Arbeitnehmers überwunden werden kann. Dazu muss der Arbeitgeber lediglich wissen, welche Tätigkeiten der Arbeitnehmer auf Grundlage seiner gesundheitlichen Disposition noch ausüben und in welchen Bereichen er aus gesundheitlichen Gründen nicht mehr eingesetzt werden kann. Einer Kenntnis der konkreten medizinischen Diagnosen durch den Arbeitgeber bedarf es dazu jedoch nicht. Dementsprechend war in dem hier geschilderten Fall die Übermittlung der konkreten Diagnosen für die Planung der künftigen Einsatzmöglichkeiten der Geschädigten an den Arbeitgeber nicht erforderlich.
Bei der Bemessung der Geldbuße gemäß Art. 83 Abs. 2 DS-GVO wurde durch den TLfDI ein fahrlässiges Handeln berücksichtigt. Mildernd wirkte sich aus, dass die Tat im Rahmen der Anhörung eingeräumt wurde und die Gesundheitsdaten lediglich einem kleinen Personenkreis offenbart wurden. Erschwerend musste jedoch berücksichtigt werden, dass besondere Kategorien personenbezogener Daten von der Tat betroffen waren. Die in dem inzwischen rechtskräftigen Bußgeldbescheid festgesetzte Geldbuße im mittleren vierstelligen Bereich war damit zugleich wirksam, verhältnismäßig wie ausreichend abschreckend für die Zukunft.

3.4 Wenn eine private Auseinandersetzung zu einem Mitarbeiterexzess führt

Die Nutzung polizeilicher Auskunfts- und Recherchesysteme durch Polizeibeamte ohne dienstliche Veranlassung stellt einen „Mitarbeiterexzess“ dar. Hierbei handeln die Polizeibeamten objektiv außerhalb

des ihnen übertragenen Aufgabenbereichs, weshalb sie allein über die Zwecke und Mittel der Verarbeitung entscheiden und daher als Verantwortliche im Sinne der Datenschutz-Grundverordnung anzusehen sind.

Den Fund eines anonymen Briefes nahm ein Geschädigter zum Anlass, um Strafanzeige bei der zuständigen Landespolizeiinspektion zu erstatten. Neben dem bedrohlichen Charakter des Schriftstückes fiel dieses insbesondere durch die Schilderung der familiären Situation und des Arbeitsumfeldes des Geschädigten sowie durch die Benennung seines Geburtsdatums und des amtlichen Kennzeichens seines Fahrzeuges auf. Da der angezeigte Sachverhalt einen Straftatbestand nicht erfüllte, übersandte die zuständige Staatsanwaltschaft die Akte nach Einstellung des Ermittlungsverfahrens zur Verfolgung einer Ordnungswidrigkeit gemäß § 43 Ordnungswidrigkeitengesetz (OWiG) an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI).
Bereits im Rahmen der staatsanwaltschaftlichen Ermittlungen wurde festgestellt, dass es sich bei dem Verfasser des anonymen Briefes um einen Beamten der Thüringer Polizei handelte. Dieser hatte den Geschädigten in den ihm zugänglichen polizeilichen Auskunfts- und Recherchesystemen „ComVor-Index“ und „INPOL“ innerhalb weniger Tage nachweislich insgesamt zehn Mal abgefragt und hierbei dessen persönliche Verhältnisse in Erfahrung gebracht. Ein dienstlicher Grund konnte für die getätigten Abfragen nicht ermittelt werden. Vielmehr war es zwischen dem verantwortlichen Polizeibeamten und dem Geschädigten im Straßenverkehr zu einer privaten Auseinandersetzung gekommen, die man offensichtlich nicht auf sich beruhen lassen wollte. Daher hatte der Polizeibeamte zunächst die Abfragen vorgenommen und die so erlangten personenbezogenen Daten später zum Verfassen des anonymen Briefs unter Verwendung eines Textverarbeitungsprogramms verwendet.
Im Rahmen der Anhörung durch den TLfDI gemäß § 55 OWiG, § 163a Abs. 1 Strafprozessordnung hatte der verantwortliche Polizeibeamte erklärt, dass er sich durch die Auseinandersetzung mit dem Geschädigten beziehungsweise durch dessen Verhalten im Straßenverkehr mit „etwas zu viel Frust und Wut im Bauch“ zum Verfassen des anonymen Briefes habe hinreißen lassen, sprach überdies aber das Bedauern über sein Verhalten aus und entschuldigte sich.

Aufgrund dieser Sach- und Rechtslage erging ein Bußgeldbescheid gegen den verantwortlichen Polizeibeamten, wobei hinsichtlich der einzelnen Abfragen in den polizeilichen Auskunfts- und Recherchesystemen und der anschließenden Verwendung der personenbezogenen Daten zur Anfertigung des anonymen Briefes Tatmehrheit angenommen wurde.
Nach Art. 83 Abs. 5 Buchstabe a) Datenschutz-Grundverordnung (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. Vorliegend hatte der Verantwortliche unter anderem mit dem Geburtsdatum und dem amtlichen Kennzeichen des Fahrzeugs des Geschädigten personenbezogene Daten im Sinne des Art. 4 Nr. 1 DS-GVO verarbeitet, da sich diese auf den Geschädigten bezogen und ihn identifizierbar machten. Mit den Abfragen in dem polizeilichen Auskunfts- und Recherchesystemen „ComVor-Index“ und „INPOL“ hatte der Verantwortliche außerdem personenbezogene Daten erhoben und später verwendet und damit im Sinne des Art. 4 Nr. 2 DS-GVO verarbeitet. Da der Verantwortliche die jeweiligen Verarbeitungsvorgänge ohne dienstliche Veranlassung und insoweit außerhalb seines Aufgabenbereichs bei der Thüringer Polizei vorgenommen hatte, handelte er im Rahmen eines sogenannten Mitarbeiterexzesses als eigener Verantwortlicher im Sinne des Art. 4 Nr. 7 DS-GVO. Auch war im hier geschilderten Fall insbesondere hinsichtlich der Anfertigung des anonymen Briefes der sachliche Anwendungsbereich der DS-GVO eröffnet.
Zwar findet die Verordnung mit der „Haushaltsausnahme“ gemäß Art. 2 Abs. 2 Buchstabe c) DS-GVO keine Anwendung auf die Verarbeitung personenbezogener Daten durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten. Allerdings hatte der Verantwortliche die verwendeten personenbezogenen Daten während seiner Dienstzeit recherchiert und zusätzlich in den rein für den Dienstgebrauch zu verwendenden Auskunfts- und Recherchesystemen abgefragt. Die „Haushaltsausnahme“ gelangt jedoch dann nicht zur Anwendung, wenn – wie hier – eine Vermischung privater und dienstlicher Tätigkeiten erfolgt.
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 Da-

tenverarbeitung zulässig ist. Die Datenverarbeitungsvorgänge konnten nicht auf eine Einwilligung gemäß Art. 6 Abs. 1 S. 1 Buchstabe a) DS-GVO gestützt werden, da es hierzu erforderlich gewesen wäre, dass der Geschädigte vorab unter Nennung des Zweckes in die Verarbeitung einwilligt hätte. Eine solche Einwilligung lag dem betroffenen Polizeibeamten jedoch nicht vor. Die Zulässigkeit der Datenverarbeitungsvorgänge ergab sich auch nicht aus dem einzig noch in Betracht zu ziehenden und für selbstverantwortlich im Exzess handelnden Beamte anwendbaren Art. 6 Abs. 1 S. 1 Buchstabe f) DS-GVO, da selbst bei der Annahme eines berechtigten Interesses die schützenswerten Interessen des Geschädigten überwogen. Die vernünftigen Erwartungen der von der Datenverarbeitung betroffenen Person, die auf ihrer Beziehung zu dem Verantwortlichen beruhen, sind in diesem Kontext zu berücksichtigen. Damit ist auch auf die subjektiven Erwartungen der betroffenen Person im Einzelfall abzustellen. Vorliegend musste der Geschädigte nicht damit rechnen, dass seine jeweiligen, in dem polizeilichen Auskunfts- und Recherchesystem gespeicherten und insoweit für polizeiliche Zwecke vorgesehenen personenbezogenen Daten dafür genutzt werden, die privaten Interessen des Polizeibeamten an der Erhebung und Verwendung der personenbezogenen Daten zu befriedigen. Die geschilderten Datenverarbeitungsvorgänge zu rein privaten Zwecken sind nicht mit dem ursprünglichen Erhebungszweck zu vereinbaren.
Bei der Bemessung der Geldbuße gemäß Art. 83 Abs. 2 DS-GVO wurde durch den TLfDI ein vorsätzliches Handeln und der erhebliche Umfang der vorgenommenen Abrufe berücksichtigt. Erschwerend musste auch die Eingriffsintensität in das Persönlichkeitsrecht des Geschädigten berücksichtigt werden, da die gewonnenen Informationen unter Ausnutzung der beruflichen Stellung erlangt wurden. Mildernd wirkte sich hingegen aus, dass sich der Polizeibeamte im Rahmen der Anhörung geständig gezeigt und sein Bedauern über den Vorfall zum Ausdruck gebracht hatte. Die in dem inzwischen rechtskräftigen Bußgeldbescheid festgesetzte Geldbuße im vierstelligen Bereich war damit zugleich wirksam, verhältnismäßig wie ausreichend abschreckend für die Zukunft.

3.5 Nichts ist so, wie es scheint – auch nicht die Patientenquittung

Eine Verarbeitung von Gesundheitsdaten ist unter anderem gemäß Art. 6 Abs. 1 Satz 1 Buchstabe a) DS-GVO in Verbindung mit Art. 9 Abs. 2 Buchstabe a) DS-GVO zulässig, wenn die betroffene Person in die Verarbeitung dieser Daten eingewilligt hat. Die Entscheidung, ob ein Notfalldatensatz angelegt wird oder nicht, obliegt ausschließlich der betroffenen Person.

Im Berichtszeitraum beschwerte sich eine betroffene Person beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) über mehrere Ärzte, Gemeinschaftspraxen und Medizinische Versorgungszentren (MVZ). Der Beschwerdegegenstand war in sämtlichen Fällen der gleiche: Die Beschwerdeführerin trug vor, dass die genannten Ärzte und medizinischen Einrichtungen Notfalldatensätze über sie ohne ihre Einwilligung angelegt hätten. Zu dieser Erkenntnis war die Beschwerdeführerin nach eigenen Angaben nach Einsichtnahme in ihre Patientenquittungen der Krankenkasse gelangt. Aus den Patientenquittungen sei die Abrechnung von „Notfalldatensätzen“ hervorgegangen beziehungsweise seien diese dort aufgeführt gewesen.
Unter anderem gemäß Art. 6 Abs. 1 Satz 1 Buchstabe a) Datenschutz-Grundverordnung (DS-GVO) in Verbindung mit Art. 9 Abs. 2 Buchstabe a) DS-GVO dürfen personenbezogene (Gesundheits-)Daten verarbeitet werden, wenn die betroffene Person in die Verarbeitung dieser Daten eingewilligt hat. Die Grundsätze für die Einwilligung sind in Art. 7 DS-GVO geregelt.
Zur datenschutzrechtlichen Prüfung der Beschwerden wandte sich der TLfDI gemäß Art. 58 Abs. 1 Buchstabe a) DS-GVO jeweils mit einem Auskunftsersuchen an alle von der Beschwerdeführerin genannten Ärzte und Einrichtungen. Hierbei stellte sich zunächst heraus, dass nicht in jedem Falle die von der Beschwerdeführerin genannte Einrichtung verantwortliche Stelle im Sinne von Art. 4 Nr. 7 DS-GVO war, sondern dass beispielsweise im Falle eines MVZ und der darin tätigen Ärzte das Klinikum verantwortliche Stelle war, dem das MVZ angehörte.
Alle verantwortlichen Stellen beantworteten das Auskunftsersuchen des TLfDI und teilten – unabhängig voneinander – mit, dass die An-

gaben in den Patientenquittungen hinsichtlich der Anlage von Notfalldatensätzen nicht den Tatsachen entsprächen, weil kein Notfalldatensatz angelegt worden sei. Auf den Patientenquittungen stünden bestimmte Abrechnungsziffern (sogenannte Gebührenordnungspositionen – GOP). Die von der Beschwerdeführerin genannte GOP „06141“ zuzüglich der Angabe „Notfalldatensatz“ werde automatisch durch die Kassenärztliche Vereinigung Thüringen (KVT) zugesetzt, wenn ein Arzt mitteile, dass er über den sogenannten Kommunikationsdienst im Medizinwesen grundsätzlich in der Lage *wäre*, einen Notfalldatensatz anzulegen. Dieser pauschale Zusatz sage jedoch nichts darüber aus, ob ein Notfalldatensatz tatsächlich auch für den Patienten angelegt worden sei.
Zur Bestätigung dieser Darlegung der verantwortlichen Stellen wandte sich der TLfDI direkt selbst an die KVT. Die KVT teilte dem TLfDI mit, dass die sogenannte Gebührenordnungsnummer 01641 („Notfalldatensatz“) auf Patientenquittungen nicht durch den Arzt, sondern durch die KVT eingesetzt würde und daraus nicht abgeleitet werden könne, dass die jeweilige Arztpraxis tatsächlich einen Notfalldatensatz vom Patienten angelegt habe. Vielmehr würde diese Gebührenordnungsnummer mit dem Zusatz „Notfalldatensatz“ von der KVT in die Rechnung aufgenommen, da die Ärzte eine Art „Strukturpauschale“ von den Krankenkassen erhalten, um die technischen Voraussetzungen zu implementieren, die zur Anlage eines Notfalldatensatzes erforderlich sind, also eine Art „technische Aufwandspauschale“. Nach Mitteilung der KVT wüssten viele Ärzte gar nicht, dass diese Abrechnungsposition von der KVT hinzugefügt würde. Somit könne der Patient aufgrund der Angabe dieser Position auf der Patientenquittung schlussfolgern, dass tatsächlich ein Notfalldatensatz vom Patienten angelegt wurde.
Die Beantwortung der datenschutzrechtlichen Auskunftsersuchen durch die Arztpraxen und medizinischen Einrichtungen sowie die Ausführungen der KVT zu den Angaben auf Patientenquittungen ergaben, dass sich aus der Angabe der GOP und dem Zusatz „Notfalldatensatz“ *lediglich die Möglichkeit* ergibt, dass die jeweilige Arztpraxis bestimmte medizinische Behandlungen und/oder Sachverhalte wie das Anlegen von Notfalldatensätzen leisten *kann*, aber tatsächlich nicht geleistet und keinen Notfalldatensatz über die Beschwerdeführerin angelegt hatte, sodass auch keine Einwilligung der Beschwerde-

führerin fehlte. Somit lag kein Verstoß gegen den Schutz personenbezogener Daten der Beschwerdeführerin vor und der TLfDI stellte das Verwaltungsverfahren ein.

3.6 Wer will was und weswegen? – Die Durchsetzung von Rechtsansprüchen im gerichtlichen Verfahren – geht das ohne personenbezogene Daten?

Gemäß Art. 9 Abs. 1 DS-GVO ist die Verarbeitung von Gesundheitsdaten grundsätzlich untersagt. Nach Art. 9 Abs. 2 Buchstabe f) DS-GVO ist die Verarbeitung dieser Daten jedoch zulässig, wenn sie zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder bei Handlungen der Gerichte im Rahmen ihrer justiziellen Tätigkeit erforderlich ist. Hierbei sind an die Frage der „Erforderlichkeit" in einem Rechtsstreit keine allzu strengen Maßstäbe anzusetzen, wenn die betreffenden Daten nachweislich mit dem Streitgegenstand in Verbindung stehen.

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) erhielt im Berichtszeitraum mit Schreiben eines Rechtsanwalts die Beschwerde einer betroffenen Person über einen Verstoß gegen den Schutz personenbezogener Daten durch das Medizinische Versorgungszentrum (MVZ) eines Thüringer Klinikums.
Nach einem Klinikaufenthalt war der Beschwerdeführer im beschwerdegegenständlichen MVZ eines anderen Klinikums weiterbehandelt worden. Aufgrund der Weiterbehandlung war dem MVZ die Aufnahmediagnose der Klinik, in der sich der Beschwerdeführer befunden hatte, bekannt. Der Beschwerdeführer befand sich aufgrund von Abrechnungsfragen beziehungsweise Zahlungsforderungen des MVZ mit dem MVZ seit mehreren Monaten in einem Rechtsstreit. Im Zuge dieses Rechtsstreits hatte das MVZ die oben genannte Aufnahmediagnose des Klinikums an die das MVZ vertretende Rechtsanwaltskanzlei übermittelt. Gegen diese Datenübermittlung richtet sich die Beschwerde an den TLfDI.
Nach Angaben seines Rechtsanwalts hatte der Beschwerdeführer dem MVZ keine Einwilligung zur Übermittlung seiner personenbezogenen (Gesundheits-)Daten in Form der Aufnahmediagnose an die Rechtsanwaltskanzlei des MVZ erteilt. Somit bestand aus seiner Sicht nach der Datenschutz-Grundverordnung (DS-GVO) keine Erlaubnis für die

Datenübermittlung nach Art. 6 Abs. 1 Satz 1 DS-GVO in Verbindung mit Art. 9 Abs. 2 DS-GVO. Daher erachtete der Beschwerdeführer die Übermittlung der Aufnahmediagnose durch das MVZ als schweren Verstoß gegen geltendes Datenschutzrecht.
Bei der Aufnahmediagnose handelt es sich gemäß Art. 9 Abs. 1 DS-GVO um sogenannte besondere Kategorien von Daten, vorliegend Gesundheitsdaten, die einem erhöhten Schutz unterliegen. Den Schriftsätzen, die der Anwalt des Beschwerdeführers dem TLfDI übersandt hatte, war zu entnehmen, dass die Übermittlung der Aufnahmediagnose durch das MVZ an dessen Rechtsanwalt in Verbindung mit der Zahlungsaufforderung des MVZ an den Beschwerdeführer erfolgt war, um im gerichtlichen Verfahren Rechtsansprüche durchzusetzen, da der Beschwerdeführer die Zahlung verweigert hatte. Unter Bezugnahme auf diesen Sachverhalt teilte der TLfDI dem Rechtsanwalt des Beschwerdeführers mit, dass die Verarbeitung von personenbezogenen Daten im Sinne von Art. 9 Abs. 1 DS-GVO, mithin auch der Gesundheitsdaten, nach Art. 9 Abs. 2 Buchstabe f) DS-GVO zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen zulässig ist. Die Zulässigkeit der Verarbeitung dieser (erforderlichen) Daten schließt gemäß Art. 4 Nr. 2 DS-GVO auch deren Offenlegung durch Übermittlung ein.
Der TLfDI wies den Rechtsanwalt des Beschwerdeführers darauf hin, dass die Zulässigkeit der Verarbeitung nicht mit Interessen der betroffenen Person abzuwägen ist. Weder Art. 9 Abs. 2 Buchstabe f) DS-GVO noch die Erwägungsgründe 51 bis 56 zu Art. 9 DS-GVO sowie die einschlägige datenschutzrechtliche Kommentarliteratur zu Art. 9 DS-GVO sehen eine Abwägung mit Interessen der Betroffenen vor, wenn die Offenlegung der Daten für die Durchsetzung von Rechtsansprüchen erforderlich ist. Daher sei eine Einwilligung des Beschwerdeführers zur Datenübermittlung nach Art 9 Abs. 2 Buchstabe a) DS-GVO durch das MVZ an dessen Rechtsanwalt nicht erforderlich gewesen, da die Übermittlung der personenbezogenen Gesundheitsdaten (Aufnahmediagnose) auf Art. 9 Abs. 2 Buchstabe f) DS-GVO gestützt werden konnte. Deswegen konnte der TLfDI keinen Verstoß gegen datenschutzrechtliche Vorschriften durch das Klinikum als verantwortliche Stelle, zu der das MVZ gehörte, feststellen und informierte den Rechtsanwalt des Beschwerdeführers über die Einstellung des Verwaltungsverfahrens. Daraufhin reichte der Rechtsanwalt des Beschwerdeführers beim Verwaltungsgericht Klage gegen die Entscheidung des TLfDI ein.

Im Rahmen des gerichtlichen Verfahrens wurden zwischen dem TLfDI und dem Rechtsanwalt des Beschwerdeführers zahlreiche Schriftsätze ausgetauscht. Im Zuge dieses Schriftwechsels prüfte der TLfDI den Sachverhalt erneut eingehend und blieb auch nach dieser erneuten tiefgreifenden Prüfung bei seiner, bereits im Verwaltungsverfahren dargelegten, datenschutzrechtlichen Auffassung, dass das MVZ nicht gegen den Schutz von personenbezogenen Daten verstoßen hatte. Der Rechtsanwalt des Beschwerdeführers vertrat weiterhin die Auffassung, dass die Übermittlung der Aufnahmediagnose durch das MVZ an dessen Rechtsanwalt gegen den Schutz personenbezogener Daten verstieß. Das Verwaltungsgericht beraumte schließlich einen mündlichen Verhandlungstermin an, in dem sowohl der Rechtsanwalt des Beschwerdeführers als auch der TLfDI die jeweiligen Argumente für ihre Auffassung vortrugen. Der Rechtsanwalt des Beschwerdeführers beantragte, den Bescheid des TLfDI zum Abschluss des Verwaltungsverfahrens aufzuheben und den Sachverhalt gegebenenfalls erneut zu prüfen; der TLfDI beantragte, die Klage abzuweisen. Das Gericht teilte mit, dass es den beiden Parteien des Rechtsstreits seine Entscheidung schriftlich zustellen werde, deutete jedoch bereits an, dass es die Argumentation das TLfDI rechtlich für plausibel und nachvollziehbar halte.
Kurze Zeit später stellte das Verwaltungsgericht dem TLfDI sein Urteil zu. Das Gericht wies die Klage ab und legte die Kosten dem Kläger, das heißt, dem Beschwerdeführer auf. Das Gericht stellte fest, dass der Bescheid des TLfDI im Verwaltungsverfahren, mit dem der TLfDI keinen Verstoß gegen den Schutz von personenbezogenen Daten des Beschwerdeführers festgestellt hatte, rechtmäßig war und den Beschwerdeführer nicht in seinen Rechten verletzte. Das Gericht legte weiterhin dar, dass in der getroffenen Entscheidung des TLfDI im Verwaltungsverfahren keine Ermessensfehler festzustellen sind und der Bescheid somit sowohl formell als auch materiell rechtskonform ist. Diesbezüglich stützte sich das Gericht in seinen Ausführungen umfassend auf die Argumentation des TLfDI zur Frage der Erforderlichkeit personenbezogener Daten zur Durchsetzung von Rechtsansprüchen in gerichtlichen Verfahren.
Weiterhin führte das Verwaltungsgericht aus, dass die Grenze der Erforderlichkeit bei Ausnahmen vom Verbotsgrundsatz der Verarbeitung personenbezogener Daten wegen ihrer Bedeutung für die rechtsstaatliche Durchsetzung von Ansprüchen nicht so streng anzulegen sei. Zwar dürfen diese Anforderungen nicht schrankenlos ausgedehnt

werden, jedoch verstoße nicht jeder Tatsachenvortrag, der sensible Daten einer betroffenen Person beinhalte, allein deswegen gegen Art. 9 Abs. 1 DS-GVO, weil dieser Vortrag vom Gericht als unerheblich bewertet werde. Insofern sei erst bei einer willkürlichen, bewussten Offenlegung von sensiblen Daten, die mit dem Streitgegenstand in keinerlei Verbindung mehr stehen, der Tatbestand der Ausnahmeklausel nicht mehr gegeben.

3.7 Besteht ein Auskunftsrecht nach Art. 15 der Datenschutz-Grundverordnung zwischen Internetforumsmitgliedern?

Auch Privatpersonen können sich nicht immer der Anwendbarkeit der DS-GVO entziehen. Die „Haushaltausnahme“ nach Art. 2 Abs. 2 Buchstabe c) DS-GVO führt zwar dazu, dass Privatpersonen in ihrem Privatleben die strengen Vorgaben der Datenschutzgesetze in der Regel nicht einhalten müssen. Allerdings handeln auch Privatpersonen öfter im Anwendungsbereich der DS-GVO als man denkt, wie das nachfolgende Beispiel zeigt.

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichte im Berichtszeitraum eine Beschwerde eines ehemaligen Internetforumsmitgliedes über einen anderen Internetforumsteilnehmer wegen nicht erteilter Auskunft nach Art. 15 Datenschutz-Grundverordnung (DS-GVO).
Der Beschwerdeführer brachte gegenüber dem TLfDI vor, dass ein anderes Mitglied im Forum einen Aufruf gestartet habe mit der Bitte, dass andere Forumsmitglieder Informationen zu und über den Beschwerdeführer, innerhalb des Themas, per privater Nachricht, per E-Mail oder auch telefonisch weiterleiten mögen. Der Beschwerdeführer beklagte eine mögliche Sammlung und Weitergabe seiner personenbezogenen Daten seitens des Aufrufstarters. Aus diesem Grund hat er den Aufrufstarter zu einer Auskunft über die Verarbeitung seiner personenbezogenen Daten gemäß Art. 15 DS-GVO aufgefordert. Dieser Auskunftspflicht sei dieser jedoch nicht nachgekommen.
Nach Feststellung der örtlichen Zuständigkeit musste der TLfDI prüfen, ob die DS-GVO im vorliegenden Fall Anwendung findet oder eine Ausnahme von der Anwendbarkeit der DS-GVO gemäß Art. 2 Abs. 2 Buchstabe c) DS-GVO („Haushaltsausnahme“) vorliegt. Im Beschwerdefall handelte es sich um zwei Privatpersonen, welche sich nach Angabe des Beschwerdeführers auch persönlich kennen.

Art. 2 Abs. 2 Buchstabe c) DS-GVO schließt die Anwendbarkeit der Datenschutz-Grundverordnung dann aus, wenn die Verarbeitung personenbezogener Daten „durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten“ stattfindet. Der Begriff der Haushaltsausnahme ist grundsätzlich restriktiv (sprich: streng, eng) auszulegen. Die Datenverarbeitung muss nicht zwingend den familiären Kreis der Beteiligten im engeren Sinne widerspiegeln. Der Begriff familiär umfasst, unabhängig von Ehe, Kindschaft und Verwandtschaft, jede Beziehung, die eine vergleichbare persönliche Nähe aufweist und von der Verkehrsanschauung als familiär angesehen wird. Dies gilt für Lebenspartnerschaften oder ein eheähnliches Zusammenleben und je nach Nähe der Beziehung sogar für Wohngemeinschaften. Er umfasst jedoch nicht den Freundeskreis, mit dem der Datenverarbeiter nicht familienförmig zusammenlebt (Rossnagel in Simitis Datenschutzrecht DSGVO mit BDSG, 1. Auflage 2019, Art. 2 Rn. 25). Auch muss die Datenverarbeitung nicht nur rein persönlicher oder familiärer Natur sein, sondern ebenso „öffentlichkeitsfeindlich“, um unter die Ausnahme fallen zu können. Mit Blick auf die unter Erwägungsgrund 18 DS-GVO erwähnte sozialen Netze (hier: Forum) ist daher eine differenzierte Betrachtung im Hinblick der Zugriffsmöglichkeiten geboten.

Findet die Datenverarbeitung innerhalb eines rein privaten und begrenzten Empfängerkreises statt, erfüllt dies die Voraussetzungen der „Haushaltsausnahme“. Jedoch greift sie nicht für die Veröffentlichung von Informationen an einen unbestimmten Personenkreis (Kühling/Buchner, DS-GVO Kommentar, 2017, Art. 2 Rn. 25). Somit führen Veröffentlichungen auf einer Internetseite, die prinzipiell von jedermann aufrufbar sind, zur Anwendbarkeit der DS-GVO.

Der Aufruf im Forum, Informationen innerhalb des Themas und für spätere juristische Zwecke bereitzustellen, eröffnet somit doppelt die Voraussetzungen, um die DS-GVO zur Anwendung zu bringen. Jegliche gewerbliche, politische oder sonstige weitergehende Zwecksetzung über die rein private hinaus ist, sobald sie objektiv erkennbar wird, ausnahmeschädlich (Paal/Pauly, Datenschutz-Grundverordnung, 2. Auflage 2018, Art. 2 DS-GVO, Rn. 17 Satz 3). Somit ist die weitere Nutzung der durch den Verantwortlichen gesammelten Daten durch Personen in Ausübung ihrer beruflichen Tätigkeit (sprich: juristischer Beistand) nicht von der Haushaltsausnahme gedeckt und damit ausnahmeschädlich. Auch der unbestimmte Personenkreis von Forumsmitgliedern, die durch die Veröffentlichung im Forum Zugang zu

diesen Informationen hatten, widersprach dem Charakter nach einer Datenverarbeitung zu ausschließlich persönlichen oder familiären Zwecken (Europäischer Gerichtshof C-101/01, 6. November 2003, Rn. 47).
Der Verantwortliche war verpflichtet, der Auskunftspflicht unverzüglich, spätestens aber innerhalb eines Monats, nachzukommen (Erwägungsgrund 59, Satz 3 DS-GVO). Nach Ablauf dieser Frist läge bei einer Nichtauskunft ein Datenschutzverstoß vor. Somit war für den vorliegenden Fall entscheidend, ob und wann der Auskunftsantrag an den Verantwortlichen genau erging. Das Stellen eines Auskunftsantrages gemäß Art. 15 DS-GVO gegenüber dem Verantwortlichen zum genannten Termin konnte der Beschwerdeführer dem TLfDI jedoch nicht glaubhaft belegen, daher führte das Beschwerdevorbringen im konkreten Fall nicht zum Erfolg.

3.8 Wohnmobilstellplatz unter Dauerbeobachtung

Eine Videoüberwachung in Bereichen, welche überwiegend Freizeitgestaltungen dienen, stellt einen erheblichen Eingriff in die Rechte und Freiheiten der betroffenen Personen dar. Die Verantwortlichen sollten daher im Vorfeld genau prüfen, ob der Einsatz einer Videoüberwachung überhaupt gerechtfertigt werden kann und in welchem Umfang sie geschehen darf.

Dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) wurde eine Videoüberwachung auf einem Wohnmobilstellplatz gemeldet, welche nicht den datenschutzrechtlichen Vorgaben entsprechen sollte. Der TLfDI wandte sich daher an den Betreiber des Wohnmobilstellplatzes. Dieser teilte mit, dass insgesamt sechs Videokameras auf dem Gelände betrieben werden. Aufgrund der übersandten Aufnahmen war festzustellen, dass der gesamte Platz durch den Verantwortlichen überwacht wurde. Zum Teil wurden Bereiche auch doppelt abgebildet. Es handelte sich um einen eher kleinen Wohnmobilstellplatz, sodass die Anzahl der Kameras bereits als umfangreich zu betrachten war. Die Videoüberwachung erfolgte als sogenanntes Monitoring (Beobachtung) am Tag, nachts wurden die Aufnahmen mittels Bewegungsmelder aufgezeichnet. Die einzelnen Sequenzen wurden für 48 Stunden gespeichert und dann automatisch gelöscht. Hinweisschilder waren an den Zugängen zu dem Gelände angebracht. Der Betreiber des Stellplatzes wies auch auf der Website

des Unternehmens auf die bestehende Videoüberwachung hin. Zudem wurde den einzelnen Gästen beim Anmieten des Stellplatzes ebenfalls nochmals ein Hinweis auf die Videoüberwachung erteilt. Insoweit wurde nach Auffassung des Verantwortlichen von jedem Stellplatzmieter durch den Verantwortlichen eine Einverständniserklärung eingeholt.
Während des Verwaltungsverfahrens wurden mehrere Zwecke für die betriebene Videoüberwachung benannt, unter anderem die Zuordnung der reservierten Stellflächen zum jeweiligen Mieter, Verhinderung von Verunreinigung durch Müll, Zigarettenkippen, Hundekot, Verhinderung von Zechprellerei, Erkennen von Gefahren (Mülltonnenbrand nach Brandstiftung, Fahrerflucht nach Schadenverursachung an Fahrzeugen, Diebstahl), Vandalismus und sonstige Kriminalität auch in der Nachbarschaft und die Wahrnehmung des Hausrechts.
Die hier betriebene Videoüberwachung konnte entgegen der Auffassung des Verantwortlichen nicht auf eine Einwilligung nach Art. 6 Abs. 1 Satz 1 Buchstabe a) Datenschutz-Grundverordnung (DS-GVO) gestützt werden, da es an der notwendigen Freiwilligkeit der Einwilligungserklärung nach Art. 7 DS-GVO der betroffenen Personen gefehlt hatte. Es bestand hier keine Möglichkeit der Betroffenen, einen nicht überwachten Stellplatz in Anspruch zu nehmen. Dass andere Wohnmobilstellplätze in der Umgebung keine Videoüberwachung durchführen und somit Ausweichmöglichkeiten bestehen würden, führt nicht zur Wirksamkeit der gegenüber dem Verantwortlichen erteilten „Einwilligungserklärungen“. Der Verantwortliche muss hier eigene Ausweichmöglichkeiten zur Verfügung stellen um eine entsprechende Freiwilligkeit der Einwilligungserklärung zu gewährleisten.
Somit war die Videoüberwachung nach Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO zu beurteilen. 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.
Es handelt sich somit um eine dreistufige Prüfung. Eine Videoüberwachung zur Gefahrenabwehr kann dann ein berechtigtes Interesse darstellen, wenn konkrete Tatsachen für eine objektiv begründbare Gefahrenlage vorliegen. Insoweit muss durch den Kamerabetreiber

eine konkrete Gefährdung nachgewiesen werden, die über das allgemeine Lebensrisiko hinausgeht (BVerwG, Urteil vom 27. März 2019, Az.: 6 C 2.18, Rn. 28). 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 (Datum, Vorfall, Schadenshöhe) oder durch Nennung von polizeilichen Tagebuchnummern beziehungsweise staatsanwaltschaftlichen Aktenzeichen erfolgen. Eine Gefahrenlage kann sich auch daraus ergeben, dass – mit zeitlichem Zusammenhang – vergleichbare Vorfälle oder Übergriffe in der unmittelbaren Nachbarschaft stattgefunden haben. Daher sollten vor dem Einsatz und auch während des Einsatzes einer Videoüberwachung etwaige Vorkommnisse genau dokumentiert und etwaige Strafanzeigen aufbewahrt werden. Auch hier besteht die sogenannte Rechenschaftspflicht des Verantwortlichen nach Art. 5 Abs. 2 DS-GVO gegenüber der Aufsichtsbehörde. Der Verantwortliche muss nachweisen können, dass die Verarbeitung rechtmäßig erfolgt. Im vorliegenden Fall wurde seitens des Verantwortlichen nur pauschal zu den Vorkommnissen Stellung genommen. Konkrete Angaben zu bestimmten Gefahren konnten nicht gemacht werden. Es wurde immer wieder zu einer generellen Gefährlichkeit der Umgebung vorgetragen. Daher wurde seitens des TLfDI ein Amtshilfeersuchen bei der zuständigen Polizeiinspektion gestellt, welche keinen Kriminalitätsschwerpunkt in der Umgebung festmachen konnte, jedoch sind mehrere Straftaten in der näheren Umgebung zum Wohnmobilstellplatz vorgekommen, sodass der TLfDI von einer konkreten Gefährdungslage ausgegangen ist.
Dennoch ergaben sich im Rahmen der Erforderlichkeit Bedenken hinsichtlich der Videoüberwachung, da für den überwiegenden Teil der genannten Zwecke mildere Maßnahmen, wie zum Beispiel der Einbau einer Zufahrtsschranke, Hinterlegung von Kaution, Kontrollgänge vor der Abreise, Zuordnung der Stellplätze über Nummerierungen et cetera möglich waren.
Zudem ging der TLfDI hinsichtlich der Erfassung der einzelnen Stellplätze der Wohnmobile von einem Überwiegen der Interessen der betroffenen Personen im Hinblick auf die berechtigten Interessen des Verantwortlichen aus. Es muss eine einzelfallorientierte Interessenabwägung durchgeführt werden, das heißt es ist anhand des konkreten Sachverhalts zu beurteilen, wie gewichtig die mit der Videoüberwachung verfolgten Interessen des Verantwortlichen sind und inwieweit diese durch die Videoüberwachung tatsächlich gefördert werden. Zum

anderen ist anhand des konkreten Einzelfalls zu prüfen und unter Berücksichtigung der vernünftigen Erwartungen des Betroffenen zu gewichten, inwieweit die Überwachung in schutzwürdige Interessen, Grundrechte und Grundfreiheiten eingreift und welche möglichen Folgen für Betroffene daraus resultieren können. Bei der Auslegung des Begriffs „vernünftige Erwartungen“ ist entscheidend, ob ein objektiver Dritter vernünftigerweise erwarten kann, in der konkreten Situation überwacht zu werden. Ob vernünftige Erwartungen bestehen, beurteilt sich daher danach, ob die Videoüberwachung in bestimmten Bereichen der Sozialsphäre typischerweise akzeptiert ist oder eventuell wegen eines Beziehungszusammenhangs sogar verlangt wird oder nicht.

Die Stellplatzmieter suchen einen Campingplatz zum Zwecke der Freizeitgestaltung auf und verhalten sich auch demgemäß ungezwungen. Caravan- oder Wohnmobilstellplätze sind gerade darauf ausgerichtet, dass sich dort Besucher auch außerhalb ihrer Fahrzeuge mit eigens hierfür mitgebrachten Sitzgelegenheiten zur Erholung und Kommunikation aufhalten. Auch die Überwachung der Zugänge zu den einzelnen Wohnmobilen ist ähnlich der Überwachung der Zugänge zu Wohnungen oder Hotelzimmern zu bewerten. Eine solche Überwachung stellt einen erheblichen Eingriff in die Privatsphäre der einzelnen Personen dar. Diese können erwarten, in sensiblen Bereichen der Freizeitgestaltung nicht überwacht zu werden.

Vorliegend wurde der Eingriff noch dadurch verstärkt, dass die betroffenen Personen keine Möglichkeit hatten, dieser Überwachung auszuweichen, da der Platz vollständig überwacht wurde. Hinzu tritt, dass während der Rezeptionszeiten ein ständiges Monitoring und somit eine ständige Beobachtung der Personen ermöglicht wurde. Die Überwachung wäre nur zum Schutz von gleichwertigen Rechtsgütern gerechtfertigt gewesen, was hier jedoch durch die Ausführungen des Verantwortlichen nicht dargelegt wurde. Insbesondere ist die Überwachung der Stellplätze nicht mit den genannten Bagatellschäden wie der Verunreinigung durch Zigarettenkippen oder Hundekot zu rechtfertigen.

Da der Verantwortliche weiterhin an der bisherigen Überwachung festhielt, wurde seitens des TLfDI ein Bescheid nach Art. 58 Abs. 2 Buchstabe f) DS-GVO erlassen, in dem die Überwachung der einzelnen Stellplätze der Wohnmobile untersagt wurde. Dieser ist jedoch noch nicht bestandskräftig, da durch den Verantwortlichen gegen den

Bescheid des TLfDI Klage vor dem Verwaltungsgericht erhoben wurde.

3.9 Webcam-Aufnahmen eines öffentlichen Platzes – nicht mit Personenbezug!

Betreiber von Webcams, die diese zu touristischen Zwecken einsetzen, also zum Beispiel die Wetterlage oder etwaige Sehenswürdigkeiten abbilden, sollten darauf achten, dass es sich dann um sogenannte Übersichtsaufnahmen handelt. Es muss sichergestellt werden, dass keinerlei Personenbezug hergestellt werden kann. Dies gilt insbesondere, wenn die Aufnahmen im Internet verbreitet werden.

Im Berichtszeitraum wurde der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) auf eine Videoüberwachung mittels einer Webcam aufmerksam gemacht, welche einen großen öffentlichen Marktplatz einer bekannten thüringischen Stadt abbildete. Auf dem Platz finden unter anderem auch traditionelle Märkte wie der Weihnachtsmarkt statt. Umliegend befinden sich die Touristinformation, verschiedene Gastronomiebetriebe und sonstige (Wohn-)Gebäude. Verantwortlich für die hier betriebene Videoüberwachung war nicht die Gemeinde, auch wenn die Aufnahmen den öffentlichen Marktplatz abbildeten. Die Webcam-Aufnahmen waren auf der Webseite eines Unternehmens abrufbar. Das Unternehmen ist somit datenschutzrechtlich Verantwortlicher im Sinne des Art. 4 Nr. 7 Datenschutz-Grundverordnung (DS-GVO) hinsichtlich der dort verarbeiteten personenbezogenen Daten und deren Inhalte. Die Aufnahmen waren mit einer einminütigen Aktualisierung auf der Webseite des Verantwortlichen einzusehen. Es wurden mittels der Videoaufnahmen Personen erkennbar abgebildet, die sich auf dem Marktplatz aufhielten. Ihre Tätigkeiten waren ebenfalls nachvollziehbar.
Der TLfDI wandte sich an den Verantwortlichen und teilte diesem mit, dass die Einstellungen der Webcam-Aufnahmen für datenschutzrechtlich unzulässig erachtet werden, da keine Rechtsgrundlage eine solche Verarbeitung rechtfertigt. Im Bereich der Videoüberwachungen durch nicht-öffentliche Stellen kommt als einzige Rechtsgrundlage Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO in Betracht. Danach ist die Verarbeitung zulässig, wenn diese zur Wahrung der berechtigten Interessen des Verantwortlichen erforderlich ist und die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Personen nicht

überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.
Im Fall der Verantwortlichkeit der Gemeinde kämen als Rechtsgrundlagen § 30 Thüringer Datenschutzgesetz oder § 26 Thüringer Gesetz über die Aufgaben und Befugnisse der Ordnungsbehörden in Betracht. Der TLfDI ging hier vom Überwiegen der Interessen der von der Webcam erfassten betroffenen Personen auf dem Marktplatz aus. Diese werden hier im Rahmen ihrer Freizeitgestaltung erfasst, was einen erheblichen Eingriff in die Rechte der betroffenen Personen darstellt. Die Personen verweilen in den umliegenden Cafés zum Kommunizieren und Essen. Auch der Platz selbst wird als Treffpunkt zum Kommunizieren und Verweilen genutzt. Ebenfalls wurde das „Bummeln“ durch die Markstände vollständig überwacht. Zudem finden dort Feste und traditionelle Märkte statt. Gerade dann dürfen die betroffenen Besucher erwarten, nicht durch eine Kamera überwacht zu werden und rechnen nicht damit, dass diese Aufnahmen im Internet verbreitet werden. Dritten ist es dort möglich, die digitalen Aufnahmen weltweit abzurufen, zu kopieren und unbegrenzt zu speichern. Zudem wird eine Vielzahl von Personen durch die Webcam erfasst. Das berechtigte Interesse des Verantwortlichen, die Webcam zu touristischen und werblichen Zwecken für das eigene Unternehmen zu betreiben, kann einen solch schweren Eingriff in die Rechte der Passanten und Marktbesucher nicht rechtfertigen.
Im Hinblick auf die Rechtmäßigkeit der Verarbeitung durch die Gemeinde ergeben sich insoweit keine anderen Erwägungen.
Der Verantwortliche stellte die Webcam-Aufnahmen nach Einschreiten des TLfDI sofort ein. Er bat jedoch darum mitzuteilen, inwieweit es datenschutzrechtlich möglich ist, eine Webcam zu touristischen Zwecken zu betreiben, ohne dass eine Verletzung der Rechte der betroffenen Personen erfolgt.
Grundsätzlich ist der Einsatz von Übersichtskameras beziehungsweise Webcams zu den vorgenannten Zwecken dann möglich, wenn kein Bezug zu Personen ermöglicht wird. Das bedeutet, dass Personen und Kraftfahrzeuge nur schemenhaft erkennbar sein dürfen. Dies kann durch entsprechende Kamerapositionierung, fehlende Zoommöglichkeit und eine niedrige Bildauflösung erreicht werden. Zudem muss die Bildübertragung so eingestellt sein, dass ein Bezug oder ein Rückschluss zum Verhalten einzelner Personen über einen längeren Beobachtungszeitraum nicht mehr möglich ist. Auf eine dauerhafte Bildübertragung sollte daher verzichtet werden und stattdessen sollten

Einzelbilder dargestellt werden. Weitere Hinweise hierzu sind in der seitens der Aufsichtsbehörden des Bundes und der Länder erstellten Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen vom 17. Juli 2020 zu finden. Diese ist auf der Website des TLfDI unter https://www.tlfdi.de/datenschutz/videoueberwachung/ abrufbar.
Der Verantwortliche passte die Webcam-Einstellungen hinsichtlich der Auflösung entsprechend den Vorgaben des TLfDI an, sodass ein Personenbezug ausgeschlossen werden konnte. Zudem wurde der Zeitraum des Uploads der einzelnen Bildsequenzen auf 15 Minuten angehoben.
Dennoch wurde der Verantwortliche hinsichtlich der bis zur Abschaltung unzulässigen Webcam-Aufnahmen seitens des TLfDI nach Art. 58 Abs. 2 Buchstabe b) DS-GVO verwarnt, da hier für einen Zeitraum von knapp zwei Jahren eine unzulässige Überwachung eines öffentlichen Platzes erfolgt war und somit ein erheblicher Eingriff in die Rechte der betroffenen Personen vorlag.

3.10 Campingplatz Kfz-Kennzeichenerfassung

In Thüringen werden in Parkhäusern und auf Parkplätzen immer mehr Kfz-Kennzeichenerfassungssysteme eingesetzt, sodass sich der TLfDI in den letzten Jahren auch mit gehäuften Meldungen und Beschwerden in Bezug auf solche Systeme auseinandersetzen musste. Letztendlich muss jedes System anhand einer Einzelfallbetrachtung geprüft und beurteilt werden. Jedoch können auch grundsätzliche Vorgaben zur Orientierung gemacht werden.

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) erhielt einen Hinweis hinsichtlich des Einsatzes eines Kfz-Kennzeichenerfassungssystems auf einem Campingplatz an einem Thüringer See. Der TLfDI wandte sich zunächst schriftlich an das verantwortliche Unternehmen. Da nach der schriftlichen Übersendung noch Fragen hinsichtlich des Systems offen waren, wurde eine Vor-Ort-Kontrolle durchgeführt.
Das Unternehmen betreibt im Bereich der Zu- und Abfahrt des Campingplatzes eine Schrankenanlage mit einem Kfz-Kennzeichenerfassungssystem. Vor der Schrankenanlage befindet sich eine großzügige Wendemöglichkeit für die Besucher. Da Kfz-Kennzeichen aufgrund des möglichen Rückschlusses auf den Fahrzeughalter personenbezogene Daten darstellen, handelt es sich um eine Verarbeitung dieser

Daten im Sinne des Art. 4 Nr. 2 Datenschutz-Grundverordnung (DS-GVO), wenn diese durch Bildaufnahmen erhoben und im System gespeichert werden. Es bedarf nach dem Grundsatz der Rechtmäßigkeit (Art. 5 Abs. 1 Buchstabe a) DS-GVO) einer Rechtsgrundlage für die Vornahme dieser Verarbeitung. In Bezug auf die Dauerparker beziehungsweise die Mieter von Parkplätzen kann die Verarbeitung auf Art. 6 Abs. 1 Satz 1 Buchstabe b) DS-GVO gestützt werden, da ohne die Hinterlegung des Kennzeichens die Vertragserfüllung des Anmietens eines Stellplatzes beim Einsatz eines solchen Systems nicht möglich ist. Bei Tagesmietern oder Tagesgästen, Kurzzeitparkern und Lieferanten kann die Verarbeitung des Kennzeichens nicht auf diese Rechtsgrundlage gestützt werden, da mit diesen im Vorfeld kein Mietvertrag über einen Wohnmobilstellplatz oder Bungalow geschlossen wurde, der auch die entsprechende Parkgebühr für die Parkdauer auf dem Campingplatz beinhaltet.
Bei nichtöffentlichen Stellen kann für die Prüfung eines solchen Systems auch Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO die Rechtsgrundlage für die Verarbeitung darstellen. Danach ist die Verarbeitung personenbezogener Daten rechtmäßig, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder die 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.
Zunächst muss also ein berechtigtes Interesse zum Betreiben eines solchen Systems seitens des Verantwortlichen bestehen. Als Zweck gab das Unternehmen im konkreten Fall unter anderem die Optimierung des Durchfahrtsbetriebes, die Zufahrtskontrolle und die Effektivierung des Parkgebührenbezahlvorgangs an. Es sollten Rückstaus an hochfrequentierten Tagen vermieden werden. Zudem sollte aufgrund der Zählung der Fahrzeuge durch das System eine Überfüllung erkannt werden, sodass die Zufahrtsstraße und die Straßen auf dem Gelände für die Rettungsfahrzeuge freigehalten werden können. Hierin sind ohne weiteres berechtigte Interessen zu sehen.
Neben dem Bestehen eines berechtigten Interesses muss eine Erforderlichkeitsprüfung durchgeführt werden, in der auch der räumliche und zeitliche Umfang der Verarbeitung zu beurteilen ist. Während der Vor-Ort-Kontrolle konnte durch die Einsichtnahme in die Kameraaufnahmen festgestellt werden, dass das Kennzeichen und ein Teil der

Motorhaube in der Aufnahme sichtbar waren. Eine Erfassung der Insassen des Fahrzeugs erfolgte nicht. Hinsichtlich des räumlichen Umfangs der Überwachung bestanden daher keine Bedenken. In zeitlicher Hinsicht konnte keine Einschränkung erfolgen, da das Befahren des Geländes 24 Stunden möglich ist.
Im Rahmen der durchzuführenden Interessenabwägung ist bei der Prüfung zu berücksichtigen, dass durch die Speicherung der Ein- und Ausfahrzeiten ein Profil hinsichtlich der Aufenthaltsdauer beziehungsweise wann sich wie lange sich auf dem Platz aufgehalten wurde, erstellt werden könnte. Um diesem Umstand zu begegnen, bedarf es eines dem Grundsatz der Datenminimierung und Speicherbegrenzung (Art. 5 Abs. 1 Buchstabe c) und e) DS-GVO entsprechenden Löschkonzepts. Das Unternehmen hat ein solches Konzept in seinem System hinterlegt. Die Kennzeichen der Tagesgäste beziehungsweise Kurzzeitparker werden unmittelbar nach der Ausfahrt, also nachdem bezahlt wurde, gelöscht. Kennzeichen von Lieferanten werden nach 45 Minuten entfernt. Die Kennzeichen von Besuchern der Dauerparker werden spätestens fünf Tage nach der Einfahrt beziehungsweise, falls diese vorher aus dem Gelände ausfahren, dann gelöscht, da diese bezahlen müssen. Die Kennzeichen der Dauercamper werden für die Dauer des bestehenden Vertrages gespeichert. Insoweit bestanden aufgrund des erstellten Löschkonzepts keine Bedenken im Rahmen der Interessenabwägung, da hier eine dauerhafte Überwachung der Aufenthaltszeiträume nicht mehr möglich war. Längere Speicherungen der Ein- und Ausfahrzeiten würden zu diesem Umstand führen und ein Bewegungsprofil ermöglichen, was zu einem Überwiegen der Interessen der betroffenen Personen führen würde. Das verantwortliche Unternehmen hatte ausreichende technische und organisatorische Maßnahmen getroffen, unter anderem bestanden klare Zugriffsregelungen, die Verarbeitung der Kennzeichen erfolgt auf passwortgeschützten Arbeitsplatzrechnern, die Speicherung erfolgt in einem verschlossenen Serverschrank und das Gebäude, in dem sich die gesamte Technik befindet, wurde mittels Alarmanlage gesichert. Aufgrund dieser Maßnahmen wurden die Risiken für die Rechte und Freiheiten der betroffenen Personen minimiert, sodass die Interessenabwägung in diesem Fall zugunsten des Verantwortlichen ausging. Im Rahmen der Interessenabwägung wurde auch berücksichtigt, dass den betroffenen Personen ausreichend Möglichkeit gegeben wurde, dem Bereich auszuweichen, indem vor der Schranke ein großer Wendebereich eingerichtet wurde.

Bemängelt wurde durch den TLfDI jedoch, dass auf die Kfz-Kennzeichenerfassung mittels Hinweisbeschilderung zunächst nicht hingewiesen wurde. Hier sind die Informationen nach Art. 13 DS-GVO zu erteilen. Insoweit ist es für die Verantwortlichen möglich, das Muster des Hinweisschildes für die Videoüberwachung, welches auf der Website des TLfDI unter https://www.tlfdi.de/datenschutz/videoueberwachung/ abrufbar ist, zu verwenden. Es handelt sich hier um ein vorgelagertes Hinweisschild, welches an den Zugängen zu dem videoüberwachten Bereich beziehungsweise wie hier vor dem Erfassen des Kfz-Kennzeichens anzubringen ist. Dann verbleibt den betroffenen Personen noch die Möglichkeit, der Kennzeichenerfassung auszuweichen. Die ausführliche Information kann dann an der Rezeption oder Kasse erteilt werden.
Das verantwortliche Unternehmen passte die Hinweisbeschilderung vollumfänglich an, sodass seitens des TLfDI keine weiteren Maßnahmen mehr zu treffen waren.
Im Rahmen der Kennzeichenerfassung trifft den Verantwortlichen zudem die Pflicht des Führens des Verzeichnisses von Verarbeitungstätigkeiten nach Art. 30 Abs. 1 DS-GVO. Möglicherweise ist je nach Fallkonstellation auch eine Datenschutz-Folgenabschätzung durchzuführen.
Zusammenfassend sollten nachfolgende Kriterien bei der Ausgestaltung des Einsatzes eines Kfz-Kennzeichenerfassungssystems bei der Rechtmäßigkeitsprüfung berücksichtigt werden:

- ausreichend Ausweichmöglichkeit für Personen, deren Erfassung nicht erforderlich ist
- Hinweisbeschilderung vor dem Bereich der Schranken, um ein Ausweichen zu ermöglichen
- nur das Kennzeichen darf erfasst werden, die Insassen sind nicht mit abzubilden
- ein angemessenes Löschkonzept
- umfangreiche technische und organisatorische Maßnahmen, welche die Sicherheit der Daten gewährleisten (Standard-Datenschutz-Modell-SDM) https://www.tlfdi.de/datenschutz/technischer-und-organisatorischer-datenschutz/das-standard-datenschutz-modell-sdm/.

3.11 Waldspaziergang unter Beobachtung

Die Inbetriebnahme einer Wildkamera, durch die neben der Überwachung des Tierbestandes auch die Erfassung und Identifizierung von Personen möglich ist, stellt einen erheblichen Eingriff in das allgemeine Persönlichkeits- und Selbstbestimmungsrecht der videoüberwachten Personen dar. Eine solche Videoüberwachung ist nur zulässig, sofern die Interessen des Kamerabetreibers gegenüber dem Persönlichkeitsrecht der betroffenen Personen überwiegen und keine milderen Mittel zur Erreichung des beabsichtigten Zwecks der Videoüberwachung zur Verfügung stehen.

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) erlangte von der Staatsanwaltschaft Kenntnis, dass ein Jäger eine Videoüberwachungsanlage an einer Futterstelle, einer sogenannten Kirrung, installiert hatte. Mithilfe der angebrachten Kamera konnte der Betreiber nicht nur den Wildtierbestand, sondern auch vorbeigehende Waldbesucher erfassen. Im Rahmen des von der Staatsanwaltschaft abgegebenen Ordnungswidrigkeitenverfahrens hatte der Jäger auch die Möglichkeit zur Stellungnahme im Rahmen seiner Anhörung. Er teilte darin mit, dass die videoüberwachte Kirrung abseits der Waldwege liege und ausgeschlossen sei, dass ein Waldbesucher zufällig zu dieser gelangen könne. Ferner habe er als Jäger ein berechtigtes Interesse an der Installation der Kameras aufgrund einer Jagd- und Hegeverpflichtung bezüglich des dort lebenden Wildes. Unter Berücksichtigung dieser Äußerung prüfte der TLfDI, ob der Jäger gegen die Grundsätze für die Verarbeitung, einschließlich der Bedingungen für die Einwilligung, gemäß den Artikeln 5, 6 und 7 Datenschutz-Grundverordnung (DS-GVO) verstoßen hatte.
Beim Erfassen von Personen mittels Videotechnik, seien es Videos oder Einzelbilder, handelt es sich um eine Verarbeitung von personenbezogenen Daten. Eine Ausnahme vom Anwendungsbereich der DS-GVO ist nicht gegeben, weswegen für eine solche Verarbeitung die Vorgaben der DS-GVO eingehalten werden müssen.
Trotz des Umstandes, dass es sich bei der Kirrung um eine jagdliche Einrichtung handelt, die von dem allgemeinen Betretungsrecht nach § 6 Abs. 7 Nr. 4 Thüringer Waldgesetz ausgenommen ist, handelt es sich um einen Bereich des Waldes, der trotz eines Betretungsverbotes faktisch für die Öffentlichkeit zugänglich ist. So ist für einen jagdun-

kundigen Waldbesucher bei Fehlen von Hinweis- oder Verbotsschildern oder durch erkennbare Abgrenzungen ein gesetzliches Betretungsverbot bei einer Kirrung nicht erkennbar (vergleiche Oberverwaltungsgericht Saarland, Urteil vom 14. September 2017 – 2 A 197/16).

Bei der Erfassung von öffentlich zugänglichen Bereichen mittels einer Videoüberwachung müssen die berechtigten Interessen der von den Videoaufnahmen betroffenen Personen berücksichtigt werden. Diesen Personen steht ein Recht auf informationelle Selbstbestimmung als besondere Ausprägung des allgemeinen Persönlichkeitsrechts zu. Das allgemeine Persönlichkeitsrecht aus Art. 2 Abs. 1 Grundgesetz (GG) in Verbindung mit Art. 1 Abs. 1 GG vermittelt nämlich jedem einen Anspruch auf Achtung und Entfaltung seiner Persönlichkeit. Es umfasst auch die Freiheit vor unerwünschten Videoaufnahmen – Art. 6 Abs. 2 und 3 Thüringer Verfassung. Vorliegend kam eine solche Beeinträchtigung des Persönlichkeitsrechts auch für Personen in Betracht, die den Wald zur Erholung nutzen oder Pilze, Beeren und Kräuter abseits der Wege sammeln.

Ein Erlaubnistatbestand für eine Datenverarbeitung mit der oben beschriebenen Kamera findet sich in der DS-GVO nur in Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO, soweit die Kamera zur Wahrnehmung des berechtigten Interesses des Jägers erforderlich war und nicht die Interessen oder Grundrechte und Grundfreiheiten der von der Videoüberwachung betroffenen Personen zum Schutz ihrer personenbezogenen Daten überwogen. Die berechtigten Interessen können hierbei ideeller, wirtschaftlicher oder rechtlicher Natur sein. Bei dem vom Kamerabetreiber benannten Interesse, der Jagdausübung, handelt es sich im Unterschied zu sonstigen Freizeitgestaltungen nicht nur um ein privates, sondern auch um ein öffentliches Interesse. Nach § 1 Abs. 1 Satz 1 Bundesjagdgesetz ist das Jagdrecht die ausschließliche Befugnis, auf einem bestimmten Gebiet wildlebende Tiere, die dem Jagdrecht unterliegen, zu hegen, auf sie die Jagd auszuüben und sie sich anzueignen.

Die im vorliegenden Fall vorgenommene Ausrichtung der Kamera überschritt jedoch den benannten Zweck der Jagd- und Hegeverpflichtung, da mit der installierten Wildkamera Aufnahmen von Personen angefertigt werden konnten, die in keiner Verbindung oder Beziehung zu der benannten Verpflichtung eines Jägers stehen. Zwar hat ein Jäger ein berechtigtes Interesse an der Verwendung einer Wildkamera, um seiner Jagd- und Hegeverpflichtung nachzugehen, jedoch besteht

eine Rechtmäßigkeit für eine Videoüberwachungsanlage nur, wenn die Interessen oder Grundrechte und Grundfreiheiten der von der Videoüberwachung betroffenen Personen zum Schutz ihrer personenbezogenen Daten nicht überwiegen. So besteht die Erforderlichkeit einer Videoüberwachung nur dann, wenn der beabsichtigte Zweck nicht genauso gut mit anderen Mitteln erreicht werden kann, welche in die Rechte der Betroffenen weniger eingreifen und dabei wirtschaftlich und organisatorisch zumutbar sind. Als mildere Mittel, um den vorbezeichneten Zweck zu erreichen, hätte die Kamera vorliegend so installiert werden können, dass von Waldbesuchern lediglich die Beine aufgenommen werden. Auch eine Bildauflösung, die zwar die Tierarten erkennen lässt, aber keine Rückschlüsse auf Personen zulässt, war denkbar. Weiterhin hätte bei der Installation der Kamera vom Betreiber geprüft werden müssen, auf welche Betriebszeiten und Erfassungsbereiche die Überwachung eingeschränkt werden kann. Eine anlassbezogene Überwachung ist einer dauerhaften Überwachung vorzuziehen. So hätte die Wildaufzeichnung zum Zweck der Jagdausübung in der Morgen- und Abenddämmerung sowie bei Nacht gewährleistet werden können. Auch hätten bestimmte Bereiche oder Personen, die für den Zweck der Überwachung nicht von Interesse sind, irreversibel ausgeblendet, geschwärzt oder verpixelt werden müssen, wenn sich die Ausrichtung der Kamera nicht verändern lässt. Im vorliegenden Fall war festzustellen, dass die Videoüberwachung nicht auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt war, da mildere Mittel zur Verfügung standen, welche weniger in die Grundrechte und Grundfreiheiten der betroffenen Personen eingegriffen hätten. Des Weiteren überwogen die Interessen der von der Videoüberwachung betroffenen Personen, da diese den Wald zur Erholung aufsuchen und hier nicht damit rechnen, von einer Videokamera gefilmt zu werden. Es erfolgte somit eine unrechtmäßige Datenverarbeitung über personenbezogene Daten. Aufgrund des damit gegebenen Verstoßes gegen die Grundsätze für die Verarbeitung von personenbezogenen Daten, einschließlich der fehlenden Bedingungen für die Einwilligung, gemäß Artikel […] 6 DS-GVO wurde nach Art. 83 Abs. 5 Buchstabe a) DS-GVO eine Geldbuße gegen den Kamerabetreiber verhängt.

Gegen den vom TLfDI erlassenen Bußgeldbescheid legte der Kamerabetreiber Rechtsbehelf ein. Im Berichtszeitraum wurde mit Urteil des Amtsgerichts die Unrechtmäßigkeit der Datenverarbeitung bestätigt.

3.12 Videoüberwachung in Supermarkt

Eine Videoüberwachung in Supermärkten ist nicht immer datenschutzrechtlich zulässig. Auch die Videoüberwachung in den Supermärkten wird durch den TLfDI geprüft. Dabei prüft der TLfDI im Rahmen einer Einzelfallbetrachtung ganz genau, ob die Interessen der Marktinhaber/-innen am Schutz ihres Eigentums vor Diebstählen im Einzelfall das Recht auf informationelle Selbstbestimmung der betroffenen Kunden überwiegen. In der Regel ist die Videoüberwachung auf diejenigen Waren zu beschränken, die schwerpunktmäßig gestohlen werden.

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) prüfte im Rahmen seiner behördlichen Tätigkeit die Videoüberwachung in einem kleineren Thüringer Supermarkt. Installiert waren dort insgesamt 14 Videokameras, die verschiedene Bereiche erfassen. Insbesondere die Verkaufsfläche wurde umfangreich überwacht. Die Aufnahmen der Videoüberwachung wurden für 72 Stunden gespeichert. Daneben war eine Live-Beobachtung der Videoaufnahmen durch den Marktleiter am Monitor möglich, fand jedoch nicht durchgehend statt. Zweck der Videoüberwachung war nach den Angaben des Marktleiters im Wesentlichen die Verhinderung von Diebstählen und die Beweissicherung.
Der TLfDI wandte sich mit mehreren Auskunftsverlangen an den Marktinhaber, um die Sach- und Rechtslage hinsichtlich der Videoüberwachung umfassend zu prüfen. Der Marktleiter teilte hierzu unter anderem mit, dass die Zahl der Ladendiebstähle hoch sei. Die Videoüberwachung sei erforderlich um den Markt zu schützen. Ohne eine Videoüberwachung sei man „blind“ gegenüber Eigentumsdelikten.
Die Zulässigkeit einer Videoüberwachung von nicht-öffentlichen Stellen richtet sich grundsätzlich nach Art. 6 Abs. 1 Satz 1 Buchstabe f) Datenschutz-Grundverordnung (DS-GVO). Danach ist die Verarbeitung von personenbezogenen Daten zulässig, soweit sie 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.
Wird eine Videoüberwachung von einem Verantwortlichen zu dem Zweck betrieben, sein Eigentum vor Diebstählen zu schützen, so stellt

dies grundsätzlich ein berechtigtes Interesse des Verantwortlichen dar. In diesem Fall muss der Verantwortliche jedoch das Vorliegen einer konkreten Gefahrenlage gegenüber dem TLfDI nachweisen, weil nur bei Vorliegen einer konkreten Gefahr seine Interessen an der Überwachung die Interessen der Kunden und Mitarbeiter daran, nicht überwacht zu werden grundsätzlich überwiegen können. Im Fall des Marktes trug der Marktleiter umfangreich zu Diebstählen von Waren im Markt in den letzten Monaten vor. Hierzu wurde ein Logbuch vorgelegt, aus dem die einzelnen Vorkommnisse in dem Markt hervorgingen. Zudem wurden auch polizeiliche Anzeigen erstattet. Der TLfDI ging daher von einer konkreten Gefährdung des Marktes aus.
In einem zweiten Schritt war sodann die Erforderlichkeit der Videoüberwachung für den verfolgten Zweck zu prüfen. Hierzu muss die Videoüberwachung geeignet sein und es darf kein anderes, gleich wirksames Mittel zur Verfügung stehen. Vor der Installation einer Videoüberwachungsanlage muss sich ein Verantwortlicher mit alternativen Sicherheitsmaßnahmen auseinandersetzen. Wenn diese weniger in die Rechte der betroffenen Personen eingreifen und gleich geeignet sind, die Zwecke der Überwachung zu erreichen, müssen sie vorrangig gewählt werden. Gerade im Supermarktbereich gibt es zahlreiche Möglichkeiten, die Waren vor Diebstahl zu schützen. So können etwa besonders hochpreisige Waren mit Alarmetiketten versehen oder in abschließbaren Vitrinen aufbewahrt werden. Es ist auch möglich, einen Ladendetektiv zu beauftragen. Im vorliegenden Fall konnte der Marktinhaber aber glaubhaft machen, dass solche alternativen Sicherungsmöglichkeiten hier nicht gleich effektiv seien.
Schließlich war im Rahmen des Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO eine einzelfallorientierte Interessenabwägung durchzuführen, das heißt, es war anhand des konkreten Sachverhalts zu beurteilen, wie gewichtig die mit der Videoüberwachung verfolgten Interessen des Verantwortlichen sind und inwieweit diese durch die Videoüberwachung tatsächlich gefördert werden. Zum anderen war zu prüfen und unter Berücksichtigung der vernünftigen Erwartungen der Betroffenen zu gewichten, inwieweit die Überwachung in schutzwürdige Interessen, Grundrechte und Grundfreiheiten eingreift und welche möglichen Folgen für Betroffene daraus resultieren können. Ob vernünftige Erwartungen bestehen, beurteilt sich danach, ob die Videoüberwachung in bestimmten Bereichen der Sozialsphäre typischerweise akzeptiert wird oder nicht.

Anhand dieses Maßstabs war daher das Recht auf informationelle Selbstbestimmung der betroffenen Kunden aus Art. 8 Abs. 1 und 2 der EU-GR-Charta gegen das Interesse des Marktinhabers am Schutz seines Eigentums abzuwägen. Dabei fiel die Abwägung im vorliegenden Fall zugunsten der Rechte der betroffenen Kunden aus.
Zu berücksichtigen war insbesondere, dass die Videoüberwachung mittels der 14 Videokameras einen erheblichen Eingriff in das Recht auf informationelle Selbstbestimmung der betroffenen Kunden darstellt. Videoüberwacht wurde ein Großteil der Ladenfläche. Erfasst wurden sämtliche Kunden, auch diejenigen, welche sich rechtstreu verhielten und sich während ihres Einkaufs nichts zu Schulden kommen ließen. Sie waren während ihres gesamten Einkaufs der Videoüberwachung ausgesetzt und hatten aufgrund des Umfangs der Videoüberwachung kaum eine Möglichkeit, dieser auszuweichen. Eine permanente und sehr umfassende Überwachung eines Raumes stellt eine deutlich weitergehende Beeinträchtigung dar, als eine Überwachung, die nur Teilbereiche erfasst.
Zwar gehört Warendiebstahl auf Verkaufsflächen im Einzelhandel zum unternehmerischen Risiko und eine Überwachung zumindest bestimmter Bereiche entspricht den vernünftigen Erwartungen der betroffenen Personen. Der TLfDI vertritt hierzu aber die Auffassung, dass eine Videoüberwachung auf diejenigen Bereiche zu beschränken ist, in denen schwerpunktmäßig Waren gestohlen werden und die den Großteil der wirtschaftlichen Schäden der Marktinhaber ausmachen. Dies sorgt für einen gerechten Ausgleich der gegenläufigen Interessen von Marktinhabern und Kunden. Die Marktinhaber haben so weiterhin die Möglichkeit ihr Eigentum mittels einer Videoüberwachung zu schützen und den redlichen Kunden bleibt zumindest für Teilbereiche ihres Aufenthalts im Markt eine Videoüberwachung erspart.
Im zu entscheidenden Fall waren die schwerpunktmäßig gestohlenen Waren nach den Angaben des Marktinhabers alkoholische Getränke und Aktionsartikel einer bestimmten Marke. Der TLfDI erachtete es daher für sachgerecht, die Videoüberwachung auf die Bereiche mit diesen Waren zu beschränken.
Eine andere Gewichtung der Interessen ergab sich auch nicht aufgrund des Umfangs der dem Marktinhaber entstandenen wirtschaftlichen Schäden durch Ladendiebstähle. Der Marktinhaber erzielt einen jährlichen Umsatz von mehreren Millionen Euro. Dem gegenüber entstehen durch die Ladendiebstähle Schäden in relativ geringer Höhe. Damit steht fest, dass jährlich nur ein verhältnismäßig kleiner Betrag des

Gesamtumsatzes durch die Ladendiebstähle verloren geht. Die finanziellen Einbußen des Marktes stehen damit außer Verhältnis zu der nahezu umfassenden Videoüberwachung der betroffenen Kunden durch den Markt. Aus finanzieller Hinsicht muss auch hingenommen werden, dass nicht jegliche finanziellen Risiken abgewendet werden können, vor allem nicht auf Kosten des Rechts auf informationelle Selbstbestimmung der betroffenen Kunden.
Neben den Interessen der Kunden sind auch die Interessen der Beschäftigten des Marktes im Rahmen der Interessenabwägung zu berücksichtigen. Insbesondere Bereiche, in denen sich Beschäftigte dauerhaft aufhalten, um ihrer Arbeitstätigkeit nachzukommen, wie zum Beispiel im Kassenbereich, sind von der Überwachung auszunehmen. Dies wurde durch die Verantwortlichen durch entsprechende Schwärzung des Bereichs vorgenommen.
Weiterhin ließ der TLfDI den Umstand in die Abwägung einfließen, dass die Videoüberwachung in ihrer konkreten Ausgestaltung nur teilweise geeignet ist, Diebstähle zu verhindern beziehungsweise begangene Diebstähle festzustellen. So wurde zum einen nur ein gewisser Teil der Diebstähle über die Videokameras bemerkt, da überwiegend ein sogenanntes Blackbox-Verfahren und keine durchgehende Live-Beobachtung durchgeführt wurde. Viele Diebstähle werden auch durch aufmerksame Kunden beobachtet und den Mitarbeitern des Marktes zur Anzeige gebracht. Außerdem wurden nach den Angaben des Marktes 30 Straftaten durch die Videokameras beobachtet, aber nur 12 Diebstähle mittels der Videoüberwachung aufgeklärt
Der TLfDI erließ daher einen Bescheid nach Art. 58 Abs. 2 Buchstabe d) und f) DS-GVO. Nach dieser Vorschrift kann der TLfDI eine vorübergehende oder endgültige Beschränkung der Verarbeitung einschließlich eines Verbots der Verarbeitung verhängen und den Verantwortlichen anweisen, Verarbeitungsvorgänge auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit der Verordnung zu bringen. In dem Bescheid wurde die Abschaltung derjenigen Kameras angeordnet, die nicht die Bereiche mit den schwerpunktmäßig gestohlenen Waren erfassen. Die Entscheidung ist noch nicht bestandskräftig, da der Verantwortliche Klage erhoben hat.

4. Vorträge und Veranstaltungen



Lernen Schulung Training - Pixabay

4.1 Vorträge und Veranstaltungen

Der TLfDI informiert! Der TLfDI ist unterwegs! – Höhepunkt im Berichtszeitraum war die Großveranstaltung zu „KI und Schule“ am 13. September 2023 im Augustinerkloster zu Erfurt. Der TLfDI und das Thüringer Institut für Lehrerfortbildung, Lehrplanentwicklung und Medien (ThILLM) setzten zudem ihre Zusammenarbeit im Rahmen ihres Kooperationsvertrages mit ihrer regelmäßigen virtuellen Vortragsreihe zum Thema „Datenschutz beim digitalen und häuslichen Lernen“ für Schulleitungen und nunmehr auch für Berufsschulleitungen fort. Auch die (unentgeltlichen) Vorlesungen des TLfDI an der Rechtsfakultät der Friedrich-Schiller-Universität (FSU) in Jena zur „Einführung in das Datenschutzrecht“ standen den Studierenden im Wintersemester 2022/2023 und im Sommersemester 2023 in Präsenz des TLfDI zur Verfügung. Teilnehmen konnten ab dem Wintersemester 2022 nun auch Studierende der Wirtschaftswissenschaften und des Lehramts. Für das Lehramt steht derzeit auch die Modernisierung der Curricula zum Thema „Datenschutzrecht“ zur Disposition.

Großveranstaltung zu „KI und Schule“
270 Gäste, darunter knapp **einhundert** Schülerinnen und Schüler, sowie zahlreiche Thüringer Schulleiterinnen und Schulleiter, waren der Einladung des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) zu seiner Tagung zu „KI und Schule“ in die Augustinerkirche zu Erfurt gefolgt – denn hier reichte dann der

Platz für alle. **ChatGPT** ist in aller Munde. Wie ChatGPT funktioniert, haben wir mit „Hausaufgaben“ aus dem Publikum direkt vor Ort getestet. Unsere Fragen beschäftigten sich unter anderem mit der Künstlichen Intelligenz (**KI)** als Werkzeug zur Förderung des Unterrichts: **Was macht KI mit den Schulen? Können die Schülerinnen und Schüler das verarbeiten? Woran orientieren sie sich? Was sagen die Lehrerinnen und Lehrer? Wie muss sich Schule umorientieren? Wie wird der Datenschutz beim Einsatz von KI in der Schule tangiert?** Mit unseren prominenten Gästen haben wir die Antworten auf die oben genannten Fragen gesucht.
Als Vortragende konnten der BfDI, Prof. Ulrich Kelber, und der Staatssekretär des Bundesbildungsministeriums, Dr. Jens Brandenburg, für Grußwort und Keynote, Hendrik Haverkamp – Koordinator für Digitalität am Evangelisch Stiftischem Gymnasium Gütersloh, Frau Prof. Jana Dittmann und Dr. Robert Altschaffel von der Uni Magdeburg, Prof. Dr. Petra Grimm als Ethikerin, Prof. Dr. Dirk Labudde von der Hochschule Mittweida und Prof. Dr. Enkelejda Kasneci von der Technischen Universität München (TUM) gewonnen werden. Nachzulesen sind die einzelnen Präsentationen unter: https://www.tlfdi.de/wir/veranstaltungen/.
Mit Blick auf die neuen Herausforderungen durch KI hält der TLfDI eine Anpassung der Lehrerausbildung weiterhin für dringend notwendig. Die Ausbildung von angehenden Lehrerinnen und Lehrern in den Bereichen Medienkompetenz, digitale Kompetenz und Recht finde so gut wie nicht statt, so das wiederholte Fazit des TLfDI. Er mahnt im Nachgang der Veranstaltung zur Vorsicht, KI bei Hausaufgaben einzubeziehen. Er könne nicht empfehlen, den Schülern die Arbeit mit KI aufzugeben, wenn die Schüler dafür personenbezogene Daten eingeben müssten, weil bis heute nicht klar ist, was mit diesen Daten passiert. Text-Quellen hierzu unter: https://www.tlfdi.de/presse/presse-echo/



Save_the_Date_PM_13092023.pdf (tlfdi.de)

Vorlesungen des TLfDI an der Rechtsfakultät der Friedrich-Schiller-Universität (FSU) in Jena

Die Vorlesungen zur „Einführung in das Datenschutzrecht" standen den Studierenden wieder in Präsenz des TLfDI zur Verfügung. Teilnehmen konnten ab dem Wintersemester 2022 nun auch Studierende der Wirtschaftswissenschaften und vor allem der Erziehungswissenschaften. Inzwischen können mit einer Klausur auch Creditpoints für das Examen erworben werden. Für das Lehramt steht derzeit auch die Modernisierung der Curricula zum Thema „Datenschutzrecht" zur Disposition.

Thüringer Landesbeauftragter
für den Datenschutz und die Informationsfreiheit

Einführung in das Datenschutzrecht - „DS-GVO: Kenntnis statt Angst!“



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

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

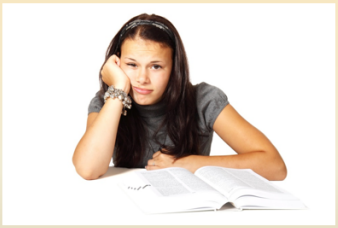
Sommersemester 2023 Rechtswissenschaftliche Fakultät - FSU-Jena 1

Videokonferenzreihe zum Thema Datenschutz für pädagogische Führungskräfte

Datenschutz beim häuslichen Lernen

Thüringer Landesbeauftragter
für den Datenschutz und die Informationsfreiheit

Datenschutz beim digitalen und häuslichen Lernen



TLfDI, Dr. Lutz Hasse

27.09.2023 Schulleiterinnen und Schulleiter 1

Die Videokonferenzreihe mit dem ThILLM „Datenschutz beim digitalen und häuslichen Lernen“ wurde mit sechs Fortbildungsveranstaltungen auch für die Berufsschulleiter und einer zusätzlichen Veranstaltung für die Landeselternsprecher erweitert. Links für Lehrkräfte finden Sie unter: https://www.tlfdi.de/datenschutz/schule-1/links-fuer-lehrkraefte-und-schueler/.

Podium und Vorträge:
Der TLfDI beteiligte sich wieder als Referent auf verschiedenen Podien der Bildung, so unter anderem bei der Learntec in Düsseldorf und der Frankfurter Buchmesse.
Es gab weitere Vorträge bei den Parlamentariern im Thüringer Landtag sowie im Bundestag in Berlin und der ständigen Konferenz der Kultusminister der Länder in der Bundesrepublik Deutschland (KMK) zu Datenschutz und Bildung im Zeitalter der KI.
Auch beim Verband der Wirtschaft Thüringens (VWT), dem Thüringer Beamtenbund und Tarifunion (tbb) und dem Blinden- und Sehbehindertenverband Thüringen e. V. (BSVT) wurde bei den entsprechenden Veranstaltungen durch den TLfDI via Podiumsdiskussion und Präsentationen beraten und informiert.
Der TLfDI betreute auch diverse Seminarfacharbeiten der Schülerinnen und Schüler in verschiedenen Schulen und Schulformen Thüringens. Wir bereicherten den 8. Datenschutztag der Karl-Volkmar-Stoy-Schule in Jena mit unseren Präsentationen, und das bereits zum achten Mal in Folge. Fortsetzung folgt!

Aktualisierung der Gesetztes-Broschüre des TLfDI (DS-GVO; BDSG, ThürDSG)



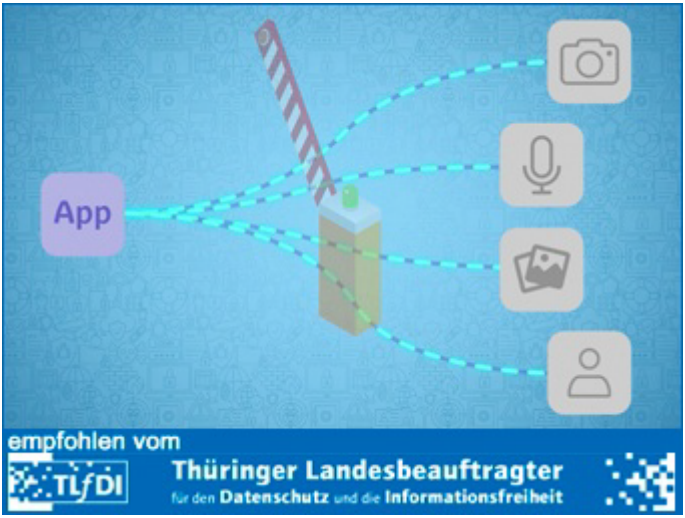
Nachzuschlagen unter:
https://www.tlfdi.de/fileadmin/tlfdi/Infothek/Gesetzesbroschuere_08.2023.pdf

8. Auflage: Aktualisierung der Handreichung „Digitale Selbstverteidigung“



Nachzulesen unter: https://www.tlfdi.de/fileadmin/tlfdi/datenschutz/Wir_ueber_uns/Infomaterial/Digitale_Selbstverteidigung_8.Auflage.pdf

Persönliche Daten auf dem Smartphone schützen
(Online) Erklärfilm des TLfDI



https://www.schulportal-thueringen.de/media/detail?tspi=16475

Pressearbeit:



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

Der TLfDI beantwortete mehr als **40 Presseanfragen** von Journalistinnen und Journalisten sowie verschiedenen Redaktionen. Er gab **diverse Interviews** bei Funk und Fernsehen, veröffentlichte **14 Pressemitteilungen**. und war am **Tag der offenen Tür 2023** im Landtag mit einem Info-Stand und seinem Team vertreten.

5. Entschließungen und Beschlüsse



Konferenz Erde Welt - Pixabay

5.1 Notwendigkeit spezifischer Regelungen zum Beschäftigtendatenschutz! Rechtsprechung des Europäischen Gerichtshofs hat Auswirkungen auf zahlreiche deutsche Vorschriften im Beschäftigungskontext

Entschließung
der Konferenz der unabhängigen Datenschutzaufsichtsbehörden
des Bundes und der Länder
am 11. Mai 2023

Der Europäische Gerichtshof (EuGH) hat am 30. März 2023 in der Rechtssache C-34/21 über die Anforderungen an eine europarechtskonforme Umsetzung des Beschäftigtendatenschutzrechts in Hessen entschieden. In seinem Urteil formuliert der EuGH hohe Anforderungen an nationale Vorschriften, die auf der Grundlage der Öffnungsklausel des Artikels 88 der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung – DS-GVO) erlassen werden. Die Entscheidungsgründe legen nahe, dass die Vorschrift des § 23 Absatz 1 Satz 1 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes und § 86 Absatz 4 des Hessischen Beamtengesetzes diese Anforderungen nicht erfüllen.

Die Entscheidung des EuGH ist bundesweit von großer Bedeutung, weil Gesetzgeber aufgrund der Feststellungen des EuGH, soweit noch nicht geschehen, prüfen müssen, ob bestehende Regelungen zum Beschäftigtendatenschutz in Deutschland den Vorgaben von Artikel 88 DS-GVO entsprechen.
Zum einen dürfen diese Regelungen nicht nur die Bestimmungen der DS-GVO wiederholen, sondern es muss sich bei ihnen um spezifischere Vorschriften der Mitgliedstaaten handeln (siehe Artikel 88 Absatz 1 DS-GVO). Zum anderen müssen diese inhaltlich den Vorgaben des Artikels 88 Absatz 2 DS-GVO entsprechen. Danach müssen die mitgliedstaatlichen Vorschriften selbst Maßgaben zum Schutz der Rechte und Freiheiten der Beschäftigten sowie geeignete und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person enthalten.
Nationale Regelungen im Beschäftigtenkontext, die nicht den Vorgaben der DS-GVO entsprechen, müssen unangewendet bleiben – so der EuGH. In diesen Fällen gelten aufgrund des Anwendungsvorrangs des Unionrechts unmittelbar die Bestimmungen der DS-GVO.
Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hatte bereits in ihrer Entschließung vom 29. April 2022, „**Die Zeit für ein Beschäftigtendatenschutzgesetz ist „Jetzt'!"**, festgestellt, dass die bestehende bundesrechtliche Regelung im Beschäftigtenkontext nicht hinreichend praktikabel, normenklar und sachgerecht ist und als Generalklausel weite Interpretationsspielräume eröffnet. Auch der vom Bundesministerium für Arbeit und Soziales (BMAS) eingesetzte unabhängige, interdisziplinäre Beirat zum Beschäftigtendatenschutz ist in seinem Bericht aus Januar 2022 zu dem Schluss gelangt, dass neben weiteren Maßnahmen ein eigenständiges Beschäftigtendatenschutzgesetz notwendig ist.
Anlässlich der EuGH-Entscheidung hält es die DSK für notwendig, über die vorgenannte Entschließung hinaus, den Gesetzgeber auf die daraus resultierenden inhaltlichen Anforderungen an datenschutzrechtliche Regelungen ausdrücklich hinzuweisen.
Die DSK fordert daher den Gesetzgeber erneut auf, ein Beschäftigtendatenschutzgesetz zu schaffen. Sie begrüßt, dass das Bundesministerium für Arbeit und Soziales (BMAS) und das Bundesministerium des Innern und für Heimat (BMI) mit den Arbeiten für ein Beschäftigtendatenschutzgesetz begonnen haben

Das Urteil des EuGH vom 30. März 2023 in der Rechtssache C-34/21 ist abrufbar unter: https://curia.europa.eu/juris/liste.jsf?language=de&num=C-34/21
Die Entschließung der DSK vom 29. April 2022 „Die Zeit für ein Beschäftigtendatenschutzgesetz ist ‚Jetzt'!" ist abrufbar unter:
https://www.datenschutzkonferenz-online.de/entschliessungen.html
Der Bericht des unabhängigen, interdisziplinären Beirats zum Beschäftigtendatenschutz ist abrufbar unter:
ttps://www.bmas.de/SharedDocs/Downloads/DE/Arbeitsrecht/ergebnisse-beirat-beschaeftigtendatenschutz.pdf?__blob=publicationFile&v=6

5.2 Verfassungsrechtliche Anforderungen bei automatisierter Datenanalyse durch Polizei und Nachrichtendienste beachten!

Entschließung
der Konferenz der unabhängigen Datenschutzaufsichtsbehörden
des Bundes und der Länder
am 11. Mai 2023

Mit Urteil vom 16. Februar 2023 hat das Bundesverfassungsgericht verfassungsrechtliche Weichen für den behördlichen Einsatz von automatisierten Datenanalysen/-auswertungen gestellt (- 1 BvR 1547/19 - und - 1 BvR 2634/20 -). Das Bundesverfassungsgericht hat entschieden, dass das Gewicht des mit der Datenanalyse verbundenen Grundrechtseingriffs insbesondere durch Art und Umfang der zu verarbeitenden Daten und die zugelassene Methode der Datenanalyse bestimmt wird. Ein besonderes Eingriffsgewicht aufgrund von Art und Umfang der Daten ist regelmäßig gegeben, wenn viele Daten zu Personen in die Datenanalyse eingehen, die selbst keinen Anlass für polizeiliche Maßnahmen gegeben haben. Das trifft beispielsweise auf Datenbestände aus Funkzellenabfragen und aus der Vorgangsbearbeitung zu. Funkzellenabfragen betreffen alle Personen, die in der Funkzelle mit ihrem Mobilgerät eingebucht sind. Datenbestände insbesondere aus Vorgängen der Strafverfolgung enthalten regelmäßig auch Daten von Opfern und Zeugen. Besonderes Eingriffsgewicht aufgrund der Methode der Datenanalyse können insbesondere die Verwendung lernfähiger Systeme – Künstliche Intelligenz („KI“) –, aber auch komplexe Formen des Datenabgleichs mit nicht lernfähigen Systemen haben. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) sieht ihre Forderungen aus ihrer Entschließung vom 3. April 2019 „Hambacher Erklärung zur Künstlichen Intelligenz“ in dem Urteil bestätigt.
Die DSK, deren Mitglieder in dem Verfahren angehört wurden, betont, dass die im Bereich der Polizei und Nachrichtendienste vorhandenen allgemeinen Vorschriften den Besonderheiten komplexer Analysemethoden nicht ausreichend Rechnung tragen. Dies gilt jedenfalls für solche Analysemethoden, die mit intensiven Eingriffen in die Grundrechte der betroffenen Personen verbunden sein können. Hierfür bedürfte es eigener verhältnismäßig ausgestalteter Rechtsgrundlagen. Der Gesetzgeber wäre dann in der Pflicht, die wesentlichen

Grundlagen selbst durch spezifische gesetzliche Vorschriften vorzugeben, um insbesondere Art und Umfang der Daten und die Verarbeitungsmethoden zu begrenzen.
Aufsichtsbehördlichen Erfahrungen entsprechend werden im Bereich der Strafverfolgung und der Gefahrenabwehr auch komplexe Formen der Datenanalyse eingesetzt, mitunter Systeme und Komponenten, die auf maschinellem Lernen basieren. Gerade polizeiliche Ermittlungen und nachrichtendienstliche Beobachtung können mit intensiven Grundrechtseingriffen verbunden sein. Daher ist die Beachtung verfassungsrechtlicher Anforderungen an das Handeln von Polizei und Nachrichtendiensten besonders dringlich.
Die Konferenz appelliert an die in Bund und Ländern politisch Verantwortlichen, den sich aus dem Urteil ergebenden gesetzgeberischen Handlungsbedarf zu prüfen. Erachten sie den Einsatz komplexer Datenanalysemethoden für erforderlich, müssen hierfür klare Rechtsgrundlagen und geeignete Rahmenbedingungen geschaffen werden, mittels derer der Grundrechtsschutz betroffener Personen sichergestellt wird. Die vorhandenen gesetzlichen Bestimmungen sind in der Praxis in verfassungskonformer Weise anzuwenden.

5.3 Geplante Chatkontrolle führt zu einer unverhältnismäßigen, anlasslosen Massenüberwachung!

Entschließung
der Konferenz der unabhängigen Datenschutzaufsichtsbehörden
des Bundes und der Länder
am 17. Oktober 2023

Die EU-Kommission beabsichtigt, technische Verfahren zur Überwachung der elektronischen Kommunikation zu ermöglichen, deren erklärtes Ziel es ist, Darstellungen von Kindesmissbrauch im Internet vorzubeugen bzw. aufzudecken. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden (Datenschutzkonferenz) weist darauf hin, dass die von der EU-Kommission vorgesehene Wahl der Mittel äußerst zweifelhaft ist, denn hierdurch wären massenweise zum Teil sehr sensible Informationen sämtlicher Nutzender, die E-Mails oder andere Nachrichten in Online-Diensten austauschen, unterschiedslos und verdachtsunabhängig von einer Überwachung betroffen
Im Mai 2022 hat die Kommission einen Vorschlag für eine Verordnung zur Festlegung von Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern vorgelegt. Der Vorschlag sieht unter anderem vor, dass Anbieter von E-Mail- oder Online-Diensten zur Nachrichtenübermittlung dazu verpflichtet werden, sexuellen Kindesmissbrauch im Internet aufzudecken. Dazu müssen die Anbieter Maßnahmen ergreifen, um die Verbreitung von bekannten oder neuen Darstellungen sexuellen Kindesmissbrauchs oder die Kontaktaufnahme zu Kindern anhand bestimmter Indikatoren zu erkennen.
Ohne Zweifel besteht die Notwendigkeit, Kinder vor sexuellem Missbrauch zu schützen und entsprechende Straftaten aufzudecken. Die Ziele der geplanten Verordnung an sich stehen also nicht infrage. Gleichwohl sind die staatlich angeordnete Kontrolle und Überwachung von Kommunikation in der umfassenden Form, die in dem Verordnungsentwurf vorgesehen ist, von unverhältnismäßigem Ausmaß. Es wird eine Vielzahl von Nutzenden mit einer erheblichen Menge sehr persönlicher Informationen aus sämtlichen Lebensbereichen von den Überwachungsmaßnahmen betroffen sein – und zwar unabhängig davon, ob überhaupt der Verdacht einer Straftat besteht. Der gewählte Ansatz bedeutet, dass die Anbieter sämtliche über bzw. mit ihren Diensten verarbeiteten Daten auf die genannten Inhalte hin überprüfen

müssen. Je nachdem, um welche Art von Diensten es sich handelt, werden dabei Verkehrs-, Inhalts- und Standortdaten sowie sämtliche Inhalte der über einen Dienst abgewickelten zwischenmenschlichen Kommunikation überwacht – auch komplette Inhalte von E-Mails und Chats.
Die Verpflichtung soll auch dann gelten, wenn die Dienste eine Ende-zu-Ende verschlüsselte Kommunikation anbieten. De facto bedeutet dies eine Abkehr von der Ende-zu-Ende-Verschlüsselung, die sich in den letzten Jahren als notwendige Vorbedingung privater Kommunikation weitgehend etabliert hat. Damit die Maßnahmen gemäß dem Verordnungsentwurf umgesetzt werden können, müsste nämlich die Ende-zu-Ende-Verschlüsselung aufgebrochen werden.
Daraus folgt, dass Technologien wie Ende-zu-Ende-Verschlüsselung nicht mehr zuverlässig zur Verfügung stehen werden, sondern nur noch unter dem Vorbehalt, dass der anbietende Dienst die Verschlüsselung umgehen kann. Das läuft dem Ziel der Verschlüsselung zuwider, die ausdrücklich die Sicherheit und die Vertraulichkeit der Kommunikation von Nutzenden, einschließlich Kindern, wie der Verordnungsentwurf selbst feststellt, gewährleisten soll. Es ist ein Bruch der Vertraulichkeit elektronischer Kommunikation mit nicht absehbaren Folgen für die Kommunikationsfreiheit als eines der demokratiesichernden Grundrechte schlechthin. Damit wird diese Vertraulichkeitsmaßnahme nicht nur gegenüber den Anbietern nutzlos, sondern es erhöht sich auch generell das Risiko von Schwachstellen, die missbräuchlichen Zugriffen Tür und Tor öffnen. In einer Zeit, in der Sicherheitslücken in IT-Systemen vermehrt und in großem Stil für illegale Zwecke ausgenutzt werden, sollten Schwächungen des Schutzes vermieden werden, statt absichtlich Bruchstellen in den technischen Infrastrukturen einzubauen.
Die vorgesehene anlasslose Massenüberwachung greift fundamental in die Grundrechte auf Achtung des Privat- und Familienlebens, der Vertraulichkeit der Kommunikation und zum Schutz personenbezogener Daten ein. Vor dem Hintergrund der anstehenden Beratungen im Rat der Europäischen Union warnt die Datenschutzkonferenz davor, den Wesensgehalt dieser Grundrechte anzutasten, und appelliert an den EU-Gesetzgeber, bei der Regulierung von Maßnahmen zur Bekämpfung schwerster Kriminalität die Grenzen der Rechtsstaatlichkeit einzuhalten und insbesondere Erforderlichkeit und Verhältnismäßigkeit zu wahren.

5.4 Datenschutz in der Forschung durch einheitliche Maßstäbe stärken

Entschließung
der Konferenz der unabhängigen Datenschutzaufsichtsbehörden
des Bundes und der Länder
am 23. November 2023

Medizinische Forschungsprojekte werden in Deutschland häufig nicht nur in einem Bundesland durchgeführt. Vielmehr sind zunehmend verschiedene Forschungseinrichtungen aus unterschiedlichen Ländern daran beteiligt (z. B. länderübergreifende Verbundforschung, multizentrische Studien). Je nach Forschungsstandort sind unterschiedliche datenschutzrechtliche Anforderungen zu beachten. Dies erschwert nicht nur die Forschung, sondern wirkt sich auch nachteilig auf den Datenschutz für die betroffenen Personen aus. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) fordert den Bundesgesetzgeber und die Landesgesetzgeber daher auf, durch aufeinander abgestimmte gesetzliche Regelungen auf hohem Datenschutzniveau den Datenschutz in der länderübergreifenden Forschung zu stärken. Hierfür hat sie Eckpunkte erarbeitet. Im Einzelnen:
In vielen Ländern enthalten verschiedene Landesgesetze, die beispielsweise die Datenverarbeitungen durch Krankenhäuser und Behörden des öffentlichen Gesundheitsdienstes betreffen, konkrete Befugnisse der jeweiligen Stellen zur Verarbeitung von Gesundheitsdaten zu Forschungszwecken, die den allgemeinen Vorgaben vorgehen. Diese gesetzlichen Regelungen stellen unterschiedliche datenschutzrechtliche Anforderungen. Bei länderübergreifender Forschung müssen von den Verantwortlichen die jeweils für sie geltenden Gesetze angewandt werden. Unterschiede bestehen insbesondere in Bezug auf die Zulässigkeit der Datenverarbeitung (gesetzliche Grundlage oder Einwilligung mit jeweils unterschiedlichen Anforderungen), die Definition von Schutzbereichen (u. a. Patientinnen und Patienten, Angehörige) und zulässige Zwecke der Verarbeitung. Die rechtliche Bewertung und Umsetzung der jeweils geltenden Rechtsgrundlage führte in der Vergangenheit zu einem gesteigerten Beratungsbedarf und zu Unsicherheiten bei den Forschenden und Rechtsanwendern. Auch ergeben sich aus unterschiedlichen Regelungen Herausforderungen für

eine transparente und verständliche Informationserteilung nach Artikel 13 und 14 der Datenschutz-Grundverordnung (DSGVO).
Das Bundesgesundheitsministerium hat mit dem Gesetzentwurf eines Gesundheitsdatennutzungsgesetzes (GDNG) eine Vereinheitlichung der forschungsrelevanten Rechtsgrundlagen vorgeschlagen. Geplant ist insoweit eine Rechtsgrundlage für die „Weiterverarbeitung von Versorgungsdaten zur Qualitätssicherung, zur Förderung der Patientensicherheit und zu Forschungszwecken“ durch eine Gesundheitseinrichtung für die bei ihr rechtmäßig gespeicherten Daten.
Das Verhältnis dieser geplanten Neuregelungen zu den Landeskrankenhausgesetzen ist jedoch unklar. Mit der Gesetzgebungskompetenz der Länder für den Bereich der Krankenhäuser hat sich der Gesetzentwurf nicht auseinandergesetzt. Daher bestehen erhebliche Zweifel, dass mit diesem Gesetzentwurf eine rechtssichere und tragfähige Neuregelung erreicht wird, die die länderübergreifende Forschung erleichtert.
Die DSK hat in ihrer Stellungnahme zum GDNG-Gesetzentwurf vom 14.08.2023 hierauf hingewiesen und weiteren Korrekturbedarf aufgezeigt.[2]
In dieser Stellungnahme und in der „Petersberger Erklärung“ vom 24.11.2022 hat die DSK wichtige Hinweise für gesetzliche Neuregelungen formuliert.[3] Sie beschreiben wesentliche Anforderungen zur datenschutzkonformen Verarbeitung von Gesundheitsdaten in der wissenschaftlichen Forschung, insbesondere zu den Rechtsgrundlagen und den besonderen Einwirkungsmöglichkeiten für betroffene Personen.
Um eine weitgehende Nutzung von Gesundheitsdaten zu Forschungszwecken im Einklang mit den Grundrechten zu normieren, sind konkrete Garantien und Maßnahmen gesetzlich festzulegen. Es gilt der Grundsatz: Je höher der Schutz der betroffenen Personen durch geeig-

[2] Die Stellungnahme der DSK vom 14.08.2023 zum Entwurf eines Gesetzes zur verbesserten Nutzung von Gesundheitsdaten (Gesundheitsdatennutzungsgesetz – GDNG – Stand 03.07.2023) ist abrufbar unter https://datenschutzkonferenz-online.de/media/st/23_08_14_DSK_Stellungnahme_GDNG-E.pdf.

[3] Die Entschließung der DSK vom 24.11.2022 (Petersberger Erklärung) ist abrufbar unter: https://www.datenschutzkonferenz-online.de/media/en/20221124_en_06_Entschliessung_Petersberger_Erklaerung.pdf.

nete Garantien und Maßnahmen, desto umfangreicher und spezifischer können die Daten zu Forschungszwecken genutzt werden.[4] Abhängig von den jeweils verarbeiteten Datenarten – z. B. personenbezogenen Daten (Art. 4 Nr. 1 DSGVO), Gesundheitsdaten (Art. 4 Nr. 15 DSGVO) oder genetische Daten (Art. 4 Nr. 13 DSGVO) – bedarf es eines angemessenen Schutz- und Vertrauensniveaus und spezifischer Regelungen für die Verarbeitungen in den jeweiligen Bereichen der Forschung.
Für besondere Forschungsgegenstände, bei denen eine ausreichende Anonymisierung nicht immer gewährleistet werden kann (etwa für radiologische Bilddaten), sollten spezifische Regelungen getroffen werden, um einen angemessenen Schutz der Grundrechte der betroffenen Personen sicherzustellen, z. B. durch zusätzliche technische und organisatorische Maßnahmen.
Darüber hinaus sind die Regelungen des Art. 9 Abs. 2 lit. j i. V. m. Art. 89 Abs. 1 DSGVO zu beachten. Insbesondere müssen im Gesetz selbst angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person festgelegt werden. Diese Festlegung der spezifischen Anforderungen darf nicht an die Verantwortlichen delegiert werden. Die Umsetzung darf sich auch nicht in generalklauselartigen oder in solchen Regelungen erschöpfen, die die DSGVO ohnehin für die Datenverarbeitung vorsieht, wie etwa die Betroffenenrechte nach Art. 15 ff. DSGVO oder Maßnahmen nach Art. 32 DSGVO. Stattdessen müssen konkrete Maßnahmen benannt werden.
Angemessene und spezifische Maßnahmen in diesem Sinne können etwa sein:

- Vorgaben für die Datenschutz-Folgenabschätzung (z. B. Betrachtungstiefe, Aufgabenzuweisungen für die Durchführung),
- die Schaffung weiterer, über die in Art. 15 ff. DSGVO hinausgehender Betroffenenrechte (z. B. spezifische Widerspruchsrechte, Vernichtung von Bioproben),
- die Festlegung angemessener Sperrfristen, die den betroffenen Personen ermöglichen, ihre Rechte auszuüben, bevor mit ihren Daten geforscht werden darf (z. B. bei einem Widerspruchsrecht),

[4] Vgl. Empfehlung Nr. 2 der Petersberger Erklärung.

- die Einbindung einer unabhängigen Treuhandstelle insbesondere zur Verschlüsselung, Anonymisierung oder Pseudonymisierung der Daten,
- die Einrichtung von Datenintegrationszentren oder Forschungsplattformen, soweit konkrete, der DSGVO entsprechende Anforderungen an deren Ausgestaltung formuliert werden,
- die Verpflichtung beteiligter Stellen zur Verschwiegenheit und die Schaffung korrespondierender Prozessrechte wie ein Beschlagnahmeverbot und Zeugnisverweigerungsrechte,
- konkrete Festlegungen zur Ausgestaltung und Gewährleistung der Datenminimierung.

Diese Aufzählung ist nicht abschließend. Es ist die Aufgabe des Gesetzgebers, die Risiken zu erkennen, die mit einer Verarbeitung von Gesundheitsdaten verbunden sind, sie zu benennen und ihnen angemessene Schutzmaßnahmen für die Rechte und Interessen der betroffenen Personen gegenüberzustellen.
Die DSK weist darauf hin, dass medizinische personenbezogene Daten in bestimmten Fallkonstellationen dem absoluten Schutz des Kernbereichs privater Lebensgestaltung unterliegen.
Die Verarbeitung solcher menschenwürderelevanter Daten kann selbst zu Forschungszwecken nicht auf Grundlage einer gesetzlichen Regelung legitimiert werden.
Schließlich ist eine uneingeschränkte Datenschutzaufsicht in dem sensiblen Bereich der Verarbeitung von Gesundheitsdaten zu garantieren. Diese bietet Schutz für die betroffenen Personen. Etwaig bestehende Einschränkungen der Befugnisse der Datenschutzaufsichtsbehörden hinsichtlich der Verhängung von Bußgeldern und des Vollzugs gegenüber öffentlichen Stellen sind zumindest im Anwendungsbereich entsprechender Regelungen aufzuheben.
Die DSK setzt sich für die Schaffung eines hohen Datenschutzniveaus in der medizinischen Forschung durch eine aufeinander abgestimmte zeitnahe rechtsklare und systematische Neustrukturierung der entsprechenden rechtlichen Regelungen ein. Sie appelliert an die Gesetzgeber des Bundes und der Länder, durch klarstellende Regelungen einen wirksamen Kernbereichsschutz sicherzustellen.
Die Datenschutzaufsichtsbehörden bieten an, in Wahrnehmung ihrer Beratungsfunktion die Gesetzgeber vor und bei entsprechenden Gesetzesvorhaben zu unterstützen.

5.5 Rahmenbedingungen und Empfehlungen für die gesetzliche Regulierung medizinischer Register

Entschließung
der Konferenz der unabhängigen Datenschutzaufsichtsbehörden
des Bundes und der Länder
am 22./23. November 2023

Das Vorhaben der Bundesregierung, für die ausgesprochen heterogene Vielfalt medizinischer Register einen allgemeinen Rahmen und eine einheitliche Basis zu schaffen, um Daten im öffentlichen Interesse nutzen zu können, ist aus datenschutzrechtlicher Perspektive nachvollziehbar. Allerdings muss sichergestellt sein, dass auch im konkreten Anwendungsfall die datenschutzrechtlichen Vorgaben eingehalten werden und das Grundrecht auf Datenschutz stets gewährleistet ist. Sowohl für die Befüllung der Register als auch für die registerinterne Verarbeitung und die Bereitstellung sowie die mögliche Nutzung der Daten durch Dritte sind die spezifischen datenschutzrechtlichen Voraussetzungen für die Verarbeitung von Gesundheitsdaten, insbesondere aus Art. 9, 25, 32 und ggf. Art. 89 Abs. 1 DSGVO, maßgeblich.

Es gibt eine Vielzahl medizinischer Register in Deutschland in unterschiedlichen Strukturen und Formen. Wenige sind spezialgesetzlich geregelt oder basieren auf allgemeinen gesetzlichen Grundlagen. Die meisten stützen sich zur Datenverarbeitung auf Einwilligungen: verschiedene stammen aus abgeschlossenen Forschungsvorhaben, andere werden auf Patienteninitiative oder von Fachgesellschaften zu bestimmten Erkrankungen betrieben; nicht alle werden noch aktiv genutzt.

Anknüpfend an die Festlegungen im Koalitionsvertrag „Mehr Fortschritt wagen“ vom November 2021 (S. 83), wonach neben einem Gesundheitsdatennutzungsgesetz auch ein Registergesetz im Einklang mit der DSGVO geschaffen werden soll, sieht die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) Anlass, ergänzend zu ihren bisherigen Forderungen und Empfehlungen die datenschutzrechtlichen Anforderungen und Bedingungen für die Regulierung einer Datenverarbeitung in medizinischen Registern zu präzisieren. Soweit die Datenverarbeitung den Zwecken

wissenschaftlicher Forschung dient, gelten daneben die Hinweise in der „Petersberger Erklärung“ der DSK aus dem November 2022.[5]
Die DSK begrüßt, dass durch das vom Bundesministerium für Gesundheit (BMG) beauftragte Gutachten zur Weiterentwicklung medizinischer Register[6] ein nahezu vollständiger Überblick[7] über die vorhandenen Register und die darin enthaltenen Daten vorliegt. Zugleich schließt sich die DSK der darin enthaltenen Empfehlung an, durch die nun geplante Gesetzgebung ein entsprechendes Registerverzeichnis zu verstetigen und dauerhaft öffentlich zugänglich zu gestalten. Die DSK befürwortet insbesondere die Überlegungen zur Schaffung einer Zentralstelle für medizinische Register, die das Registerverzeichnis führen und die eine Auditierung und Zuordnung medizinischer Register je nach vorhandener Qualitätsstufe (im Gutachten als „Reifegrad“ bezeichnet) verantworten soll. Aufgrund der Aufgaben der Zentralstelle für medizinische Register, die maßgeblich für die weitere Verarbeitung der in den medizinischen Registern enthaltenen Daten sind, hält es die DSK für geboten, hiermit eine unabhängige Körperschaft des öffentlichen Rechts zu betrauen. Dieser Zentralstelle könnte zudem eine besondere Funktion als Ansprechpartner und Lotse für die betroffenen Personen sowie bei der Erfüllung der Betroffenenrechte zukommen.
Die DSK teilt das aus dem Koalitionsvertrag erkennbare Anliegen, durch die gesetzliche Regelung die bislang heterogene Registerlandschaft zu strukturieren und zum Aufbau fachlich qualitätsgesicherter Register beizutragen. Entsprechend den Ausführungen im Gutachten bietet es sich an, bei der Zuordnung der Register je nach Qualitätsstufe zu verschiedenen Kategorien die Datenqualität, die Datenstruktur und die Standards bei der Verarbeitung zu berücksichtigen.
Insbesondere folgende Rahmenbedingungen sind aus datenschutzrechtlicher Sicht bei der gesetzlichen Regulierung medizinischer Register vorzusehen:

[5] Entschließung der DSK „Petersberger Erklärung zur datenschutzkonformen Verarbeitung von Gesundheitsdaten in der wissenschaftlichen Forschung“ vom 24. November 2022.

[6] Gutachten zur Weiterentwicklung medizinischer Register zur Verbesserung der Dateneinspeisung und -anschlussfähigkeit, TMF – Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V. und BQS – Institut für Qualität und Patientensicherheit, 29. Oktober 2021.

[7] Unter dem Link: https://registersuche.bqs.de/search.php sind ca. 400 Register gelistet.

- Werden personenbezogene Daten an die Register übermittelt und von diesen erhoben, die nicht unmittelbar für das Register, sondern zu einem anderen Zweck erhoben worden sind, bedarf es hierfür – soweit dies nicht durch Einwilligungen gedeckt ist – klarer gesetzlicher Festlegungen zu den Voraussetzungen der zweckändernden Datenverarbeitung, die den Anforderungen aus Art. 6 Abs. 4 DSGVO entsprechen.
- Es sind rechtsklare und verhältnismäßige Regelungen über die Aufbewahrungsdauer und Löschfristen der Registerdaten unter der Maßgabe der Grundsätze der Datenminimierung und Speicherbegrenzung zu treffen.
- Eine Befugnis zur Übermittlung von personenbezogenen Gesundheitsdaten an das Register, zu deren Speicherung im Register sowie zu deren Übermittlung an Dritte unter Verzicht auf eine vorherige Einbindung der betroffenen Person bedarf mindestens der medizinisch-fachlichen Erforderlichkeit für einen der in Art. 9 Abs. 2-4 DSGVO genannten Zwecke, der gesetzlichen Definition der zu verarbeitenden personenbezogenen Daten und bei Forschungszwecken dienenden Registern eines allgemeinen, voraussetzungslosen Widerspruchsrechts.
- Bei der Festlegung von Voraussetzungen für eine datenschutzkonforme Verarbeitung von Registerdaten, insbesondere den Anforderungen für die Übermittlung an und Erhebung durch die Register, die weitere Verarbeitung der Daten in den Registern und deren Bereitstellung für Dritte, sowie einer Definition der zu verarbeitenden Einzelangaben, sind außer den Maßgaben der Öffnungsklauseln nach Art. 9 Abs. 2 DSGVO und ggf. den Garantien nach Art. 89 Abs. 1 DSGVO auch die Vorgaben des Grundrechts auf Datenschutz zu berücksichtigen. Insbesondere müssen sich wesentliche Grundrechtseinschränkungen unmittelbar aus dem Gesetz ergeben.
- Bei den gesetzlichen Regelungen sollte die Rechtmäßigkeit der Datenverarbeitung abhängig von dem jeweiligen Zweck differenziert festgelegt werden. Eine Nutzung zur wissenschaftlichen Forschung erfordert beispielsweise andere Bedingungen als eine Auswertung zu Zwecken einer – gesetzlich jeweils näher zu bezeichnenden – Qualitätssicherung. Dies muss berücksichtigt werden.
- Die DSK hält es für erforderlich, dass mit der gesetzlichen Regulierung der medizinischen Register auch Vorgaben zu technisch-

organisatorischen Maßnahmen standardisiert und harmonisiert festgelegt werden. Damit wird das dem Risiko angemessene Schutzniveau für die Verarbeitungen verdeutlicht und eine effektive Datenschutzaufsicht ermöglicht. Insbesondere bei besonderen Risiken, wie zum Beispiel einem Remotezugriff auf Gesundheitsdaten über digitale Portale, wird dem Gesetzgeber empfohlen, im Rahmen einer sog. gesetzlichen Datenschutz-Folgenabschätzung (DSFA) globale Risiken der Registersysteme zu ermitteln und so geeignete technische und organisatorische Maßnahmen zur Minimierung dieser Risiken bereits im Gesetz zu regeln. Dies kann die Verantwortlichen zwar nicht vollständig von einer eigenen DSFA entlasten, trägt aber zur Schaffung einheitlicher Mindeststandards bei.

- Die DSK empfiehlt, durch die gesetzlichen Regelungen digitale Methoden u.a. für das Einwilligungsmanagement und die Ausübung der Betroffenenrechte zu fördern sowie – beispielsweise durch Portale – eine Partizipation der Betroffenen zu ermöglichen.
- Die DSK hält es grundsätzlich für tragfähig, für qualitätsgesicherte Register ein Zulassungsverfahren vorzusehen mit dem Ziel, dass für bestimmte im Registerverzeichnis entsprechend gelistete Register bestehende oder noch zu schaffende gesetzliche Datenverarbeitungsbefugnisse herangezogen werden können. Dabei ist hinsichtlich der einzelnen Verarbeitungsschritte der Übermittlung an das Register, der Erhebung und der Bereitstellung der Daten durch das Register sowie der Verwendung bei der weiteren Nutzung der Registerdaten zu differenzieren.
- Für die Register sollten regelmäßig unabhängige Vertrauensstellen vorgesehen werden. Diese könnten eine zentrale Rolle bei der Anonymisierung und Pseudonymisierung von Gesundheitsdaten vor der Bereitstellung für Forschende und bei der Verwaltung bereichsspezifischer Kennzeichen als einheitliche Identifikatoren spielen.
- Im Zulassungsverfahren sollten relevante Aspekte des Datenschutzes (z. B. die Rechtsgrundlagen und die Gewährleistung der Betroffenenrechte) und der Informationssicherheit geprüft werden. Die DSK empfiehlt, die Festlegung des Zulassungsverfahrens mit ihr abzustimmen, um die technisch-organisatorischen Maßnahmen und die datenschutzrechtlichen Prinzipien – wie

Verschlüsselung, Pseudonymisierung, Erforderlichkeitsgrundsatz, Anonymisierung, Nutzung synthetischer Daten – bei der Datenerhebung, bei der Verarbeitung innerhalb des Registers und bei der Bereitstellung der Daten durch das Register zu gewährleisten. Zugleich sollte für die Zulassung ein Verfahren vorgesehen werden, mit dem die Einhaltung der Qualitätsstandards sowie die Angemessenheit des Schutzniveaus in regelmäßigen Abständen wiederholt geprüft und nachgewiesen wird.

- Im Zulassungsverfahren sollten auch das Verfahren, das Schutz- und Vertrauensniveau der Schnittstellen und die Voraussetzungen geprüft werden, mit denen ein Register Daten an Dritte bereitstellt oder übermittelt. Nutzungsanträge und -bewilligungen sollten aus Transparenzgründen vom Register und von der für den Nutzungsantrag zuständigen Stelle veröffentlicht werden.
- Zur Verminderung von Risiken und zur datenschutzkonformen Auswertung von Daten sollte in der gesetzlichen Regelung die Nutzung geeigneter technischer und organisatorischer Methoden einschließlich der dezentralen Speicherung und Verarbeitung gefordert werden.
- Es wird empfohlen, gesetzlich festzulegen, welche datenschutzrechtliche Rolle den beteiligten Stellen für welche Verarbeitungsvorgänge zukommt, d.h. ob eine eigene oder gemeinsame Verantwortlichkeit oder eine Auftragsverarbeitung vorliegt.
- Der datenschutzrechtliche Grundsatz der Zweckbindung nach Art. 5 Abs. 1 lit. b DSGVO steht der Verknüpfung von Datensätzen grundsätzlich entgegen. Sofern für Zwecke der wissenschaftlichen Forschung Datensätze verknüpft werden sollen, bedarf es im Hinblick auf das Grundrecht auf Datenschutz einer besonderen Rechtfertigung, die sich in der Regel aus einem öffentlichen Interesse und einem gesellschaftlichen Nutzen ergeben soll. Wegen der sich aus einer Verknüpfung ergebenden Risiken sollte sie nur anlassbezogen und temporär zulässig sein.
- Bei der Verwendung einheitlicher Identifikatoren sollten bereichsspezifische Kennzeichen eingesetzt werden. Im Bereich der Datenverarbeitung durch medizinische Register wäre ein spezifisches datenschutzfreundliches Identifikationssystem für den Gesundheitsbereich denkbar: So könnten beispielsweise aus einer bereits vorhandenen Krankenversichertennummer nicht rückrechenbare, bereichsspezifische Pseudonyme für die Register je-

weils gesondert durch geschützte Verfahren gebildet und gespeichert werden, die sich nur über eine zentrale Vertrauensstelle zuordnen ließen. Soweit die Zentralstelle für medizinische Register auch datenschutzrechtliche Aspekte prüft, sollte das Verhältnis zu den Datenschutzaufsichtsbehörden unter Beachtung der Vorgaben der DSGVO gesetzlich geklärt werden.

5.6 Zur datenschutzrechtlichen Bewertung von Zugriffsmöglichkeiten öffentlicher Stellen von Drittländern auf personenbezogene Daten

Beschluss
der Konferenz der unabhängigen Datenschutzaufsichtsbehörden
des Bundes und der Länder
am 31. Januar 2023

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder bewertet Zugriffsmöglichkeiten öffentlicher Stellen von Drittländern auf personenbezogene Daten, die nach Art. 28 DSGVO im Auftrag im EWR verarbeitet werden, datenschutzrechtlich wie folgt:

1. Die Gefahr allein, dass – etwa über gesellschaftsrechtliche Weisungsrechte – die Drittlands-Muttergesellschaft eines EWR-Unternehmens dieses anweisen könnte, oder dass öffentliche Stellen von Drittländern unmittelbar EWR-Unternehmen anweisen könnten, personenbezogene Daten in ein Drittland zu übermitteln, genügt nicht, um eine Übermittlung in ein Drittland i.S.d. Art. 44 ff. DSGVO anzunehmen.[8], [9]
2. Allerdings kann eine solche Gefahr dazu führen, dass solchen Rechtsvorschriften unterliegenden Auftragsverarbeitern die Zuverlässigkeit im Sinne von Art. 28 Abs. 1 DSGVO fehlt, soweit nicht diese – oder auch der Verantwortliche – technische und/oder organisatorische Maßnahmen ergriffen haben, die hinreichend Garantien dafür bieten, dass der Auftragsverarbeiter seinen Pflichten nachkommt, insbesondere was das Unterlassen von Verarbeitungen personenbezogener Daten ohne oder gegen die Weisung des Verantwortlichen angeht, im Speziellen auf der Grundlage von Verpflichtungen aus drittstaatlichem Recht.[10]
3. Soweit das Risiko besteht, dass eine Norm oder Praxis, die nach EU-Recht unzulässige Verarbeitungen personenbezogener Daten

[8] Bericht der AG „Microsoft-Onlinedienste“, Kap. 3.2.3.4. b) iv., Rn. 983 ff.; Kap. 3.2.3.5., Rn. 1131 ff

[9] Eine solche Gefahr kann aber Anhaltspunkt sein, um zu prüfen, ob eine Übermittlung in ein Drittland i.S.d. Art. 44 ff. DSGVO geplant ist, die beispielsweise Informationspflichten nach Art. 13, 14 DSGVO auslöst.

[10] Bericht der AG „Microsoft-Onlinedienste“, Kap. 3.2.3.5., Rn. 1135 ff.

verlangen kann, auch auf EWR-Tochtergesellschaften von Drittlands-Unternehmen anwendbar ist, genügt die Verarbeitung durch eine EWR-Tochtergesellschaft als Auftragsverarbeiter für sich genommen nicht, um eine Zuverlässigkeit im Sinne von Art. 28 Abs. 1 DSGVO zu erreichen.[11] Soweit eine Norm oder Praxis eines Drittlands die abstrakte Gefahr einer nach EU-Recht unzulässigen Übermittlung personenbezogener Daten aus dem EWR in ein Drittland durch eine als Auftragsverarbeiter tätige Stelle in dem EWR – z.B. die EWR-Tochtergesellschaft eines Drittlands-Unternehmens – begründet, sind an die Sorgfalt der Zuverlässigkeitsprüfung im Sinne von Art. 28 Abs. 1 DSGVO besonders hohe Anforderungen zu stellen, die dieser Gefahr Rechnung tragen.

4. Dies erfordert zunächst eine Bewertung sämtlicher Umstände des Einzelfalls, ob der Auftragsverarbeiter und/oder die von ihm verarbeiteten Daten unter diese drittstaatliche Norm oder Praxis fallen und wenn ja, ob der Auftragsverarbeiter dennoch hinreichend Garantien dafür bietet, dass es nicht zu Verarbeitungen kommt, die nach den Maßstäben der DSGVO bzw. des anwendbaren mitgliedstaatlichen Rechts unzulässig sind.
   Dabei sind insbesondere die folgenden Punkte zu berücksichtigen:
   - das Ergebnis einer Prüfung hinsichtlich einer extraterritorialen Anwendbarkeit des Drittlands-Rechts und einer ggf. darüber hinausgehenden praktischen extraterritorialen Anwendung,
   - bei einer extraterritorialen Anwendbarkeit und/oder Anwendung: das Ergebnis einer Prüfung, ob das Recht oder die Praxis des Drittlands die Verpflichtungen aus dem Auftragsverarbeitungsvertrag beeinträchtigen könnten (in Anlehnung an die Empfehlungen 01/2020 des Europäischen Datenschutzausschusses)
   - das Risiko, dass die Drittlands-Muttergesellschaft eines EWR-Tochterunternehmens dieses anweisen könnte, personenbezogene Daten in ein Drittland übermitteln (Prüfung der Erkenntnisse zur Rechtslage/-praxis),

[11] Bericht der AG „Microsoft-Onlinedienste“, Kap. 3.2.3.4. b) v., Rn. 1011 ff.

- ob der Auftragsverarbeitungsvertrag nach europäischen Maßstäben unzulässige Verarbeitungen auf der Grundlage von Drittlands-Recht erlaubt,
- etwaige Zusicherungen der Drittlands-Muttergesellschaft und des EWR-Unternehmens zum Umgang mit kollidierenden Anforderungen des Rechts eines Drittstaates und der EU,
- eine Bewertung der Rechtslage und -praxis des Drittlands, ob derartige Zusicherungen auch tatsächlich eingehalten werden können,
- eine Bewertung aller weiteren Aspekte, ob derartige Zusicherungen auch tatsächlich eingehalten werden,
- etwaige in der Vergangenheit festgestellte Datenschutzverstöße,
- die Schwere und Wahrscheinlichkeit einer Sanktionierung von Zuwiderhandlungen nach EU-Recht und dem Recht des Drittlands sowie
- der Ausschluss unzulässiger Übermittlungen durch geeignete technische und organisatorische Maßnahmen.

Bietet der Auftragsverarbeiter nach dieser Prüfung keine hinreichenden Garantien, sind die Risiken der europarechtswidrigen Datenverarbeitung durch technische und/oder organisatorische Maßnahmen auszugleichen, die genau diejenigen Defizite der Rechtslage oder -praxis des drittstaatlichen Rechts ausgleichen, die zu der mangelnden Zuverlässigkeit des Auftragsverarbeiters geführt haben.[12] Für die Frage, welche Maßstäbe an diese Maßnahmen zu stellen sind, können Verantwortliche die Empfehlungen 01/2020 des Europäischen Datenschutz-ausschusses heranziehen, wobei jedoch zu beachten ist, dass diese Empfehlungen für den Kontext von Datenübermittlungen in Drittländer konzipiert worden sind,[13] sodass abweichende Bewertungen der Eignung bestimmter Maßnahmen nicht ausgeschlossen sind. Soweit eine Verarbeitung personenbezogener Daten im Auftrag den Zugriff des Auftragsverarbeiters auf Klardaten erfordert, ist in entsprechender Anwendung des Anwendungsfalls 6 des Anhangs 2 der Empfehlungen 01/2020 besonders kritisch zu prüfen, wie den

[12] Bericht der AG „Microsoft-Onlinedienste“, Kap. 3.2.3.4. b) v., Rn. 1025 ff.; Kap. 3.2.3.5., Rn. 1142 f.

[13] Bericht der AG „Microsoft-Onlinedienste“, Kap. 3.2.3.4. b) v., Rn. 1042 ff.; Kap. 3.2.3.5., Rn. 1146 ff.

Anforderungen des Art. 28 Abs. 1 DSGVO ausreichend Rechnung getragen werden kann.[14]

5. Der Verantwortliche muss in der Lage sein, den Nachweis zu führen, dass ein Auftragsverarbeiter die Anforderungen aus Art. 28 Abs. 1 und ErwG 81 DSGVO an Fachwissen, Zuverlässigkeit und Ressourcen erfüllt.[15]

Die DSK wird sich auf der Grundlage dieses Beschlusses für eine weitere Behandlung dieser Fragestellung im Europäischen Datenschutzausschuss (EDSA) einsetzen.

[14] Bericht der AG „Microsoft-Onlinedienste“, Kap. 3.2.3.4. b) v., Rn. 1053 ff.; Kap. 3.2.3.5., Rn. 1149 ff.

[15] Bericht der AG „Microsoft-Onlinedienste“, Kap. 3.2.3.4.b) v., Rn. 996 ff; Leitlinien 07/2020 des Europäischen Datenschutzausschusses zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ in der DSGVO, Rn. 94.

5.7 Bewertung von Pur-Abo-Modellen auf Websites

Beschluss
der Konferenz der unabhängigen Datenschutzaufsichtsbehörden
des Bundes und der Länder
am 22. März 2023

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) beschließt im Zusammenhang mit sogenannten Pur-Abo-Modellen auf Websites:

1. Grundsätzlich kann die Nachverfolgung des Nutzendenverhaltens (Tracking) auf eine Einwilligung gestützt werden, wenn alternativ ein trackingfreies Modell angeboten wird, auch wenn dies bezahlpflichtig ist. Die Leistung, die Nutzende bei einem Bezahlmodell erhalten, muss jedoch erstens eine gleichwertige Alternative zu der Leistung darstellen, die diese durch eine Einwilligung erlangen. Zweitens muss die Einwilligung alle in der Datenschutz-Grundverordnung (DS-GVO) normierten Wirksamkeitsvoraussetzungen, d. h. insbesondere die in Art. 4 Nr. 11 sowie Art. 7 DS-GVO aufgeführten Erfordernisse, erfüllen.[16]
2. Ob die Bezahlmöglichkeit – also z. B. ein Monats-Abo – als eine gleichwertige Alternative zur Einwilligung in das Tracking zu betrachten ist, hängt insbesondere davon ab, ob den Nutzenden gegen ein marktübliches Entgelt ein gleichwertiger Zugang zu derselben Leistung eröffnet wird. Ein gleichwertiger Zugang liegt in der Regel vor, wenn die Angebote zumindest dem Grunde nach die gleiche Leistung umfassen.
3. Nehmen Nutzende das Angebot im Rahmen eines „trackingfreien“ Abonnements wahr und erteilen keine zusätzliche Einwilligung, dürfen gemäß § 25 Abs. 1 des Gesetzes über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei Telemedien (TTDSG) nur Speicher- und Auslesevorgänge erfolgen, die für den von ihnen ausdrücklich gewünschten Telemediendienst unbedingt erforderlich sind. Nachfolgende Verarbeitungen personenbezogener Daten sind nur dann zulässig,

[16] In diesem Zusammenhang wird auch auf die Leitlinien 05/2020 des Europäischen Datenschutzausschusses verwiesen: EDSA, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679, Version 1.1, angenommen am 20.05.2020, Rn. 37 f., https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_de.pdf.

wenn die Anforderungen der DS-GVO, insbesondere die gesetzlichen Erlaubnistatbestände gemäß Art. 6 Abs. 1 DS-GVO und, je nach Einzelfall, Art. 9 DS-GVO, erfüllt sind. Diesbezüglich wird auf die allgemeinen Ausführungen in der Orientierungshilfe der DSK für Anbieter von Telemedien (OH Telemedien 2021, Version 1.1) Bezug genommen.

4. Die Wirksamkeit von Einwilligungen von Nicht-Abonnentinnen und Nicht-Abonnenten ist bei den sogenannten Pur-Abo-Modellen sicherzustellen. Soweit mehrere Verarbeitungszwecke vorliegen, die wesentlich voneinander abweichen, müssen die Anforderungen an die Freiwilligkeit dahingehend erfüllt werden, dass Einwilligungen granular erteilt werden können. Dies bedeutet unter anderem, dass Nutzende die Möglichkeit haben müssen, die einzelnen Zwecke, zu denen eine Einwilligung eingeholt werden soll, selbst und aktiv auswählen zu können (Opt-in). Nur wenn Zwecke in einem sehr engen Zusammenhang stehen, kann eine Bündelung von Zwecken in Betracht kommen. Eine pauschale Gesamteinwilligung in insoweit verschiedene Zwecke kann nicht wirksam erteilt werden.
5. Darüber hinaus müssen die Einwilligungen den sonstigen Anforderungen der DS-GVO gerecht werden, insbesondere auch jenen an Transparenz, Verständlichkeit und Information für die betroffenen Personen aus Art. 4 Nr. 11 und Art. 7 Abs. 2 DS-GVO (vgl. hierzu die Orientierungshilfe der DSK für Anbieter von Telemedien (OH Telemedien 2021, Version 1.1).

Stichwortverzeichnis

Abrechnung 3.5
Adressdatei 2.7
Adresse 2.14, 2.13
Amtsarzt 2.15
Anordnung 3.12
App 2.4
Arbeitgeber 2.6, 1.18, 1.17
Arbeitskreis Datenschutz-/Medienkompetenz 1.9
Arbeitskreis Schulen und Bildungseinrichtungen 1.9
Arbeitsmedizin 3.3
Arbeitsunfähigkeit 1.17
Archivzwecke 1.18
Arzt 3.5, 3.3, 2.15, 1.17, 1.5
ärztliches Attest 2.15
Asset-Deal 3.1
Aufnahmediagnose 3.6
Aufruf 3.7
Auftragsdatenverarbeitung 1.4
Auftragsverarbeitung 2.4, 1.7
Auftragsverarbeitungsvertrag 2.17
aus Österreich 2.2
Auskunft 2.9
Auskunfts- und Recherchesystemen ComVor-Index 3.4
Auskunftsanspruch 2.12, 1.19
Auskunftspflicht 3.7
Auskunftsrecht 1.5
Auto 2.5
Automobilbranche 1.8
Beamter 2.6
berechtigte Interessen 3.8
Beschäftigte 2.8, 2.6, 2.3, 2.1, 1.18, 1.17
Bescheid 2.16
besondere Kategorien von personenbezogenen Daten nach Art. 9 DS-GVO 2.3
betriebliches Eingliederungsmanagement 3.3
Bewegungsmelder 3.8
Bewerber 2.6

Bildungsmesse didacta 1.9
Blackbox-Verfahren 3.12
Blindkopie 1.16
Blutspendedienst 3.2
Brief 3.4
bring your own device (BYOD) 1.9
Broschüre 4.1, 1.10
Bundesamt für Sicherheit in der Informationstechnik (BSI) 1.8
Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (BfDI) 1.11
Bundesdatenschutzgesetz (BDSG), Änderung 1.6
Bußgeld 3.11, 1.19
Bußgeldbescheid 3.4, 3.3
Bußgeldverfahren 3.3
Buttersäure-Brandanschlag 2.2
Campingplatz 3.10
ChatGPT 1.20, 1.9, 1.3
Chatprogramm 1.3
Cloud 1.13
Cloud, souveräne 1.7
Corona-Impfstatus 1.18
Corona-Virus 2.14
Cyberkriminalität 1.8
Datenschutzbeauftragter 1.12
Datenschutzbeauftragter, kommunaler 1.15
Datenschutz-Folgenabschätzung 3.10, 1.15
Datenübermittlung 1.2
Datenübertragbarkeit 1.7
Dauerparker 3.10
Diagnose 3.3
Diebstahl 3.12
Dienstanweisung zum Einsatz einer IT-Anwendung zum Zweck der Alarmierung 2.1
Diensthandys 2.1
Digitale Selbstverteidigung 1.10
Digital-Gesetz 1.11
Digitalisierung 1.11
Download 2.16
Drittstaatentransfers 1.7
Drohne 1.13

Durchsuchungsbeschluss....2.2
Einwilligung..... 3.8, 3.6, 3.3, 3.2, 3.1, 2.14, 2.10, 2.9, 2.3, 2.1, 1.16
elektronische Patientenakte....1.11
Eltern....2.10, 2.9
E-Mail....2.16, 2.12, 1.17, 1.16
E-Mail-Adresse....2.8, 1.16
Ende-zu-Ende-Verschlüsselung....2.12
E-Rezept....1.11
Ermessensfehler....3.6
Europäischer Datenschutzausschusses (EDSA)....1.20
Europäischer Gerichtshof (EuGH)....1.19, 1.1
EU-US Data Privacy Framework....1.2
Expert Subgroups....1.20
Formular....2.15
Forschung....2.14, 1.11
Forschungsdaten....1.11
Forschungsdatenzentrum Gesundheit....1.11
Forschungsgeheimnis....1.11
Foto....2.10, 2.9
Freiwilligkeit....3.8, 3.2
Freizeitgestaltung....3.8
Futterstelle....3.11
Gefahren für die öffentliche Sicherheit und Ordnung....2.1
Gefahrenlage....3.8
Geheimschutzbeauftragter....1.12
Geldwäschebeauftragter....1.12
gematik....1.11
Gemeinde....3.9
gemeinsame Verantwortlichkeit....1.19
gerichtliche Überprüfung....1.19
Geschäftsstelle....1.6
Gesetz zur Regelung des Transfusionswesens (TFG)....3.2
Gesundheitsamt....2.14, 1.18
Gesundheitsdaten 3.6, 3.5, 3.3, 3.2, 2.15, 2.11, 2.3, 1.18, 1.11, 1.5
Gesundheitsversorgung....1.11
Grundschule....2.11
Grundstückseigentümer....3.1
Hacker-Angriff....1.8
Handreichung....1.4
Handy-/Telefonnummern....2.1

Haushaltsprivileg 3.7
Hinweis auf die Videoüberwachung 3.8
Hinweisbeschilderung 3.10
Hinweisschild 1.13
Hochschule 2.16, 2.15
Homepage 2.10
ICD-Code 2.15
Identitätsprüfung 3.2
Identitätssicherung 3.2
Infektionsschutzgesetz 2.11
Information der Betroffenen 2.7
Informationsgesellschaft 1.9
Informationspflicht 3.2, 2.14, 2.11, 1.13
INPOL 3.4
Insolvenzverfahren 3.1
Insolvenzverwalter 3.1
Instagram 2.17
Interessenabwägung 3.10
Interessenkonflikt 1.12
International Bank Account Number (= IBAN) 2.7
Internetforum 3.7
Interview 4.1
IT-Sicherheit 1.8
IT-Sicherheitsbeauftragter 1.12
Jagdrecht 3.11
Jäger 3.11
Kassenärztliche Vereinigung Thüringen (KVT) 3.5
Kennzeichenerfassung 2.4
Kfz-Kennzeichen 2.5
Kfz-Kennzeichenerfassungssystem 3.10
Kinder 2.11, 2.9
Kindergarten 2.11, 2.9
Kirrung 3.11
Kita App 2.9
Klage 3.6
Klassenfoto 2.10
Klingelkamera 1.13
Kommune 2.7, 1.15, 1.14
Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) 1.11, 1.6

Kontaktdaten 2.8, 2.7
Kontoinhaber 2.7
Kopie 2.12, 1.5
Kopierschablone 3.2
Kosten 1.5
Krankenhaus 3.6, 1.18
Krankenkasse 3.5, 1.11
Krebsfrüherkennungsrichtlinie 2.13
Kreditwirtschaft 1.19
Kultusministerkonferenz (KMK) 1.9
Kundendaten 2.2
Künstliche Intelligenz (KI) 1.9, 1.8, 1.3
Kurzzeitparker 3.10
Landeskriminalamt 2.2
Landespolizeiinspektion 3.4
Landesregierung 2.3
Läuse 2.11
Leitungsebene 1.12
Lieferanten 3.10
Live-Beobachtung 3.12
Löschkonzept 3.10
Löschung 2.9
Mammographie-Screening 2.13
Marktplatz 3.9
Medizinisches Versorgungszentrum (MVZ) 3.6
Meldedaten 2.13
Melderegister 2.13
Meldung nach Art. 33 DS-GVO 2.16
Meta 1.20
Microsoft 365 ..... 1.4
Mitarbeiterexzess 3.4
Mitwirkungspflicht 1.14
Mobile Device Management 1.9
Monitoring (Beobachtung) 3.8
Notfalldatensatz 3.5
öffentliche Stelle 1.12
Öffentlichkeitsarbeit 4.1
OpenAI 1.3
Open-Source-Software 1.7
Opt-Out 1.11

Ordnungsbehörde 2.5
Ordnungswidrigkeit 2.5
Ordnungswidrigkeitenverfahren 3.11
Organisationshoheit 2.8
Pachtvertrag 3.1
Parkplatz 3.10
Parkplatzanlage 2.4
Patient 3.5, 1.11, 1.5
Patientenquittung 3.5
Personalakten 2.3
Personalausweiskopie 3.2
Personalverwaltung 1.17
Personen des öffentlichen Interesses 2.3
Polizei 3.4, 2.1
Polizeibeamte 2.1
Postenaffäre 2.3
Presseanfrage 4.1
Profiling 1.19
Prüfungsunfähigkeit 2.15
Pseudonymisierung 2.3, 1.11
Rechenschaftspflicht 3.8, 1.19
Rechenzentrum 1.7
Recht auf Kopie 1.19
Rechtsanspruch 3.6
Registrierung 3.2
Rollenkonflikt 1.12
Schadenersatzansprüche 1.14
Schranke 2.4
Schrankenanlage 3.10
Schrems II 1.2
SCHUFA 1.19
Schulden 2.6
Schule 2.17, 2.11, 2.10
Schüler 4.1, 2.17, 2.10
Schwerpunkt 1.1
Scoring-Verfahren 1.19
Selbstzertifizierung 1.2
Seminarfacharbeit 2.17
Sicherheitsgefühl 1.14
Social Media Plattformen 2.17

Sozialdaten 1.11
Sozialgeheimnis 1.11
Speicherdauer 3.12, 1.13
Speicherfristen 2.4
Statistik 1.1
Stellplatz 3.10
Strafanzeige 3.4
Straftat 2.2
Strafzettel 2.5
Studierende 2.16
Supermarkt 3.12
Tagesgäste 3.10
Tauglichkeitsgutachten 3.3
telefonische Anfrage 2.8
Thüringer Institut für Lehrerfortbildung, Lehrplanentwicklung und Medien 4.1
Thüringer Landesrechenzentrum 2.13
Thüringer Landtag 2.3
Thüringer Ministerium für Arbeit, Soziales, Gesundheit, Frauen und Familie (TMASGFF) 1.18
Thüringer Ministerium für Inneres und Kommunales (TMIK) 2.1
Thüringer Rechnungshof 2.3
TikTok 1.20
Toilettenanlage 1.14
Tonaufnahme 1.13
Transparenzgebot 1.4
Transparenzpflichten 1.7
Transportverschlüsselung 2.12
Türkamera 1.13
Übermittlungssperre 2.13
Umfrage 2.1, 1.15
Untersagungsbescheid 3.8
Untersuchungsausschuss 2.3
Unzuständigkeit 2.2
USA 1.2
US-Datenschutzprüfungsgericht 1.2
US-Nachrichtendienste 1.2
Veranstaltung 4.1
Verletzung des Schutzes personenbezogener Daten 2.7
Vermögensverhältnisse 2.6

Verschlüsselung 2.12
Verschwiegenheitserklärung 2.7
Vertraulichkeit 2.12
Verwaltungsgericht 3.6
Verwarnung 3.9, 3.2, 3.1, 2.16, 2.14, 2.10, 2.9, 2.6
Videokamera 3.8, 2.4
Videoüberwachung 3.12, 3.11, 3.9, 3.8, 1.14, 1.13
Vier-Augen-Prinzip 2.16
Vorlesung 4.1
Vor-Ort-Kontrolle 3.10
Vorträge 4.1
Waldbesucher 3.11
Warnung 2.3
Webcam 3.9
Webseite 3.9
Widerspruchsrecht 2.13
Windschutzscheibe 2.5
Wohnmobilstellplatz 3.8
www.youngdata.de 1.9
Zentrale 2.8
Zentrale Stelle Mammographie-Screening 2.13
Zufahrtskontrolle 3.10
Zugriffsmöglichkeit 2.1