TLfDI

Thüringer Landesbeauftragter
für den Datenschutz und die Informationsfreiheit

2024

7. Tätigkeitsbericht zum Datenschutz nach der DS-GVO

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:	November 2025

7. Tätigkeitsbericht zum Datenschutz nach der DS-GVO:

des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit

Berichtszeitraum: 1. Januar 2024 bis 31. Dezember 2024
Zitiervorschlag: 7. TB DS-GVO LfDI Thüringen

Der 7. Tätigkeitsbericht DS-GVO steht im Internet unter der Adresse www.tlfdi.de zum Abruf bereit.

Erfurt, im November 2025

Tino Melzer

Thüringer Landesbeauftragter für den Datenschutz
und die Informationsfreiheit

Inhaltsverzeichnis

Vorwort

Liebe Leserinnen und Leser dieses Tätigkeitsberichts,

mit dem vorliegenden siebten Tätigkeitsbericht seit Inkrafttreten der Datenschutz-Grundverordnung (DS-GVO) wird der Zeitraum vom 1. Januar bis 31. Dezember 2024 abgedeckt. Das Berichtsjahr war für mich in Thüringen von besonderen Entwicklungen geprägt – organisatorisch wie rechtlich.

Am 2. Februar 2024 wurde ich als der neue Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) gewählt und am 1. März in das Amt eingeführt. Diese personelle Veränderung markiert zugleich den Beginn einer Phase der Erneuerung und der Neuausrichtung im Hinblick auf die Schwerpunkte der Aufsichtsarbeit, die Kommunikation mit den Bürgerinnen und Bürgern sowie die Zusammenarbeit mit verantwortlichen öffentlichen und nicht-öffentlichen Stellen.

Das Berichtsjahr 2024 stand im Zeichen einer fortschreitenden Digitalisierung sämtlicher Lebensbereiche, deren Dynamik durch neue technische Entwicklungen – insbesondere im Bereich der künstlichen Intelligenz – erheblich zugenommen hat. Diese Innovationen versprechen zum einen Effizienz und Nutzerfreundlichkeit – digitale Dienste sind heute auch für Menschen ohne besondere Vorkenntnisse leicht zugänglich. Gleichwohl zeigt sich, dass dieser Fortschritt stabile rechtliche und datenschutzkonforme Grundlagen benötigt. Datenschutz ist in diesem Zusammenhang nicht allein integraler Bestandteil moderner digitaler Verwaltung und digitaler Gesellschaft, letztere ist auch ohne Datenschutz als ein Garant des nötigen Grundrechtsschutzes nicht zu denken.

Die europäische Digitalrechtsgesetzgebung bildet hierbei einen wichtigen Rahmen, um die gemeinsamen Werte und Potenziale der Europäischen Union zu sichern und weiterzuentwickeln. Während auf europäischer Ebene erhebliche Fortschritte erzielt wurden, bleibt die Umsetzung auf Bundesebene teilweise hinter den Erwartungen und Erfordernissen zurück. Eine größere Kohärenz der Rechtsakte ist un-

erlässlich; dort, wo sie fehlt, gilt es, diese Defizite offen anzusprechen und Lösungen zu suchen.
Von hoher Bedeutung waren im Berichtszeitraum zudem zahlreiche Entscheidungen des Gerichtshofs der Europäischen Union, die den datenschutzrechtlichen und institutionellen Rahmen weiter konkretisieren. Besonders hervorzuheben ist die Entscheidung zur Zuständigkeit der Aufsichtsbehörden für die datenschutzrechtliche Aufsicht über die Parlamente. Zu den sich daraus ergebenden besonderen Herausforderungen zählt auch, die verfassungsrechtliche Stellung der Parlamentarier im Rahmen der Aufsicht zu berücksichtigen. Auch erwähnt werden muss die Entscheidung zum Ermessen der Aufsichtsbehörde. Diese ist zwar verpflichtet jede eingehende Beschwerde zu prüfen, ihr steht aber ein Ermessen zu in Hinblick auf die Frage, ob und wenn ja, welche Maßnahmen sie bei einem festgestellten Verstoß ergreifen möchte.
Das Jahr 2024 war von einer deutlichen Zunahme an Aufgaben des TLfDI geprägt. Mit dem Zuwachs an Aufgaben aus Rechtsprechung und Rechtsakten kommen aber auch neue Herausforderungen. Die personelle Ausstattung des TLfDI ist bereits für das bisherige Beschwerdeaufkommen zu knapp bemessen. Für die Aufsichtsarbeit in Thüringen ergibt sich daraus die Notwendigkeit eine Vielzahl fachlicher Verfahren effizient zu gestalten – ein Zustand, der nicht im Interesse der Bürger oder der Wirtschaft sein kann.
An den Thüringer Gesetzgeber richtet sich die Bitte, den begonnenen Weg der Verwaltungsdigitalisierung konsequent und unter Beachtung verfassungsrechtlicher Grundsätze fortzusetzen. Hierzu gehört ebenfalls der Datenschutz sowie eine handlungsfähige Aufsichtsbehörde. Ebenso ist die Wahrung föderaler Entscheidungsstrukturen als Grundpfeiler der Deutschen Staatsorganisation von Bedeutung. Etwaige Kompetenzverlagerungen – etwa im Zusammenhang mit der Verschiebung von Zuständigkeiten in den Bund – sind kritisch zu überdenken. Es droht dann der Verlust von Bürgernähe der Datenschutzaufsicht sowie der Fähigkeit zur lokalen Wirtschaftsberatung.
Datenschutz bedeutet zugleich Mitgestaltung. Der TLfDI strebt gemeinsam mit der Landesverwaltung an, praktikable und rechtssichere Lösungen zu entwickeln. Über die Umsetzung des in der DS-GVO skizzierten Lastenheftes dürfte nunmehr neun Jahre nach in Kraft treten und sieben Jahre der Geltung Einigkeit bestehen; jedenfalls ist aus Sicht des TLfDI hierrüber nicht mehr zu diskutieren. Bei Fragen die

sich aus diesen Aufgaben allerdings ergeben sowie künftige Herausforderungen, wird beim TLfDI jedoch stets Gesprächsbereitschaft bestehen. Neue Formate wie Podcasts oder die Reihe „TLfDI on Tour“ sollen den Informationsaustausch mit Verwaltung, Wirtschaft und Öffentlichkeit erweitern soweit es die Kapazitäten der Behörde zukünftig zulassen.

Wie immer lag ein Schwerpunkt im Jahr 2024 im Bereich der immer noch zunehmenden Nutzung privater Videoüberwachungstechnik. Aber auch im Bereich der öffentlichen Stellen beschäftigte sich der TLfDI im Berichtszeitraum viel mit Videotechnik. Ein dominantes Thema etwa war die Videoüberwachung des Angers in Erfurt. Diese Thematik wird die Aufsicht auch in den kommenden Jahren weiter begleiten.

Im Bereich Bildung und Schule wurde die Arbeit des Arbeitskreises „Schulen und Bildung“ fortgeführt. Auch hier bleibt es ein wesentliches Ziel, Gesetzgebungs- und Digitalisierungsprozesse frühzeitig zu begleiten und Datenschutzaspekte frühzeitig einzubinden. Nur so können datenschutzrechtliche Herausforderungen rechtzeitig erkannt und sachgerechte Lösungen entwickelt werden.

Das Berichtsjahr 2024 verdeutlicht, dass Datenschutz fortlaufende Anpassungen an technologische Entwicklungen erfordert. Während sich die technologieneutrale Ausrichtung der DS-GVO bewährt hat, zeigt die Erfahrung, dass man als Verantwortlicher „ständig dranbleiben“ muss. Der Schutz personenbezogener Daten bleibt Grundlage zur Verwirklichung von Grundrechten, insbesondere im digitalen Raum und damit Grundpfeiler einer stabilen digitalen und demokratischen Gesellschaft.

Last but not least gilt mein Dank den Mitarbeiterinnen und Mitarbeitern des TLfDI für ihre engagierte Arbeit sowie für die Unterstützung während meines Amtsantritts. Ohne ihr Fachwissen und ihren Einsatz wäre die erfolgreiche Wahrnehmung unserer Aufgaben nicht möglich.

Bleiben Sie informiert und fragen Sie nach,

Ihr Tino Melzer

1. Themengebiete

© Cevahir - Datenaustausch - fotolia.com

1.1 Schwerpunkte im Berichtszeitraum einschließlich Statistik

Die Entwicklung des Datenschutzrechts in Europa hat erhebliche Auswirkungen auf die Tätigkeit des TLfDI. Die KI-Verordnung ist in Kraft, allerdings sind die Zuständigkeiten in diesem Bereich noch nicht abschließend geklärt. Im Zuge der Digitalisierung in allen Lebensbereichen gewinnt KI zugleich eine immer größere Bedeutung, was datenschutzrechtliche Fragen aufwirft.

Die Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz – KI-Verordnung) regelt den Einsatz Künstlicher Intelligenz (KI) weltweit. Die Anforderungen an die Anbieter differieren je nach dem mit dem Einsatz verbundenen Risiko.

In vielen Bereichen ist Künstliche Intelligenz unter bestimmten Bedingungen anwendbar, in bestimmten Bereichen mit besonders hohem Risiko aber gesetzlich verboten. Die Vorgaben der KIVO gelten nicht sofort nach dem Inkrafttreten. Vielmehr sind Übergangsfristen zwischen sechs und 36 Monaten vorgesehen. Die Datenschutz-Grundverordnung (DS-GVO) wird durch die Bestimmungen der KI-Verordnung nicht ersetzt, sondern gilt weiterhin. Das hat zur Folge, dass die Anforderungen der DS-GVO eingehalten werden müssen, wenn personenbezogene Daten bei KI-Anwendungen verarbeitet werden. Die Benennung der Datenschutzbehörden als nationale Aufsichtsbehörden auch im Bereich der KI-Verordnung würde einen einheitlichen Regulierungsansatz ermöglichen und dazu beitragen, dass die Datenverarbeitungsvorschriften einheitlich ausgelegt werden (s. hierzu Beitrag Nr. 1.2).
Um den Einsatz von KI datenschutzrechtlich besser begleiten zu können, war der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) auch in der im Mai 2024 auf europäischer Ebene gegründeten Arbeitsgruppe *ChatGPT Taskforce* vertreten (vgl. Beitrag 1.3).
Ansonsten ist festzustellen, dass Art und Umfang der Auskunftserteilung nach Art. 15 DS-GVO in der Praxis immer noch Probleme bereiten (vgl. Beiträge 1.15 und 3.3).
Daneben gab es viele Einzelfälle aus unterschiedlichen Themenbereichen, von denen im Bericht eine Auswahl dargestellt ist. Bei den Beschwerden nimmt weiterhin die datenschutzrechtliche Prüfung von Videoüberwachung in verschiedensten Zusammenhängen einen gewissen Schwerpunkt ein.
Einige statistische Angaben:
Im Jahr 2024 gab es 19.042 Posteingänge beim TLfDI (Vorjahr 21.334).
Es wurden im Berichtsjahr 135 Bußgeldverfahren eröffnet, das sind gut 17 Prozent mehr als im Vorjahr. Davon endeten fünf Verfahren mit einem Bußgeldbescheid. Insgesamt wurden im Jahr 2024 beim TLfDI 38 Bußgeldbescheide erlassen, wovon 27 bis zum Ende des Berichtszeitraumes Rechtskraft erlangten. Die Höhe der insgesamt festgesetzten Bußgelder betrug 50.840 Euro, was eine Steigerung gegenüber dem Vorjahr um gut 61 Prozent bedeutet. Der TLfDI erließ einen Bußgeldbescheid nach Art. 83 Abs. 4 Datenschutz-Grundverordnung (DS-GVO). Weiterhin wurden 37 Bußgeldbescheide nach Art. 83 Abs. 5 DS-GVO erlassen. Wie auch in den Vorjahren richteten

sich die Bußgeldbescheide erneut schwerpunktmäßig gegen die Betreiber unbefugter Videoüberwachung. Gleichzeitig war mit acht Bußgeldbescheiden wieder ein leichter Anstieg von Verstößen im Polizeibereich zu verzeichnen.
Insgesamt gab es 330 Meldungen der Verletzung des Schutzes personenbezogener Daten nach Art. 33 DS-GVO. Dies stellt eine Steigerung im Vergleich zum Vorjahr um rund 10 Prozent dar. Im Berichtszeitraum gingen 468 Beschwerden nach Art. 77 Abs. 1 DS-GVO ein, also Eingaben von Personen, die sich gegen eine sie betreffende Datenverarbeitung durch Thüringer Stellen wandten, knapp 13 Prozent mehr als im Vorjahr. 163 davon richteten sich gegen Verantwortliche im öffentlichen Bereich und 305 gegen solche im nicht-öffentlichen Bereich.
Im Berichtszeitraum wurden insgesamt 43 Maßnahmen nach Art. 58 Abs. 2 DS-GVO ergriffen. Hiervon betrafen 18 Maßnahmen den öffentlichen Bereich und 25 den nicht-öffentlichen Bereich. In keinem Fall wurden die Verantwortlichen gewarnt, dass beabsichtigte Verarbeitungsvorgänge voraussichtlich gegen diese Verordnung verstoßen (Art. 58 Abs. 2 Buchstabe a) DS-GVO). 38 Verantwortliche wurden nach Art. 58 Abs. 2 Buchstabe b) DS-GVO verwarnt, hierbei betrafen dies 18 Verwarnungen im öffentlichen Bereich und 20 Verwarnungen im nicht-öffentlichen Bereich, da diese mit Verarbeitungsvorgängen gegen diese Verordnung verstoßen hatten. Zwei Verantwortliche aus dem nicht-öffentlichen Bereich wurden im Berichtszeitraum nach Buchstabe c) angewiesen, den Anträgen der betroffenen Person auf Ausübung der ihr nach dieser Verordnung zustehenden Rechte zu entsprechen. Vier Verantwortliche (hiervon zwei aus dem nicht-öffentlichen Bereich) wurden im Berichtszeitraum nach Buchstabe d) angewiesen, Verarbeitungsvorgänge auf eine bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit dieser Verordnung zu bringen. Hierbei gab es in einem Fall eine Kombination mit Art. 58 Abs. 2 Buchstabe g), also einer Berichtigung, Löschung oder Einschränkung der Verarbeitung. Eine vorrübergehende oder endgültige Beschränkung der Verarbeitung, einschließlich eines Verbots nach Buchstabe f), wurde gegenüber keinem Verantwortlichen verhängt. Bei keinem Verantwortlichen wurden Maßnahmen nach Buchstabe d) und f) in Kombination ergriffen.

1.2 EU KI-Verordnung und wer sind die Aufsichtsbehörden?

Seit 1. August 2024 ist die EU KI-Verordnung in Kraft. Doch wer sind die zukünftigen Marktüberwachungsbehörden in Deutschland? Viel Zeit bleibt nicht mehr, denn nach Inkrafttreten der KI-Verordnung muss in Deutschland innerhalb von zwölf Monaten eine behördliche Aufsichtsstruktur eingerichtet werden. Damit besteht dringender Handlungsbedarf für die Gesetzgeber in Bund und Ländern. Die Datenschutzaufsichtsbehörden von Bund und Länder haben vorgeschlagen, auch die Zuständigkeiten als Marktüberwachungsbehörden an sie zu übertragen, um so Synergieeffekte zu erreichen und Kompetenzen zu bündeln.

Am 1. August 2024 ist die europäische Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz) in Kraft getreten. Sie gilt ab dem 2. August 2026. Jedoch gelten einige Regelungen in dieser Verordnung bereits eher. Schon ab dem 2. Februar 2025 gelten die Kapitel I (Allgemeine Bestimmungen) und II (Verbotene Praktiken im KI-Bereich). So gilt beispielsweise auch Art. 4 der KI-Verordnung, wonach die Anbieter und Betreiber von KI-Systemen Maßnahmen ergreifen müssen, um nach besten Kräften sicherzustellen, dass ihr Personal und andere Personen, die in ihrem Auftrag mit dem Betrieb und der Nutzung von KI-Systemen befasst sind, über ein ausreichendes Maß an KI-Kompetenz verfügen, wobei ihre technischen Kenntnisse, ihre Erfahrung, ihre Ausbildung und Schulung und der Kontext, in dem die KI-Systeme eingesetzt werden sollen, sowie die Personen oder Personengruppen, bei denen die KI-Systeme eingesetzt werden sollen, zu berücksichtigen sind. Kapitel III Abschnitt 4 (Notifizierende Behörden und notifizierte Stellen), Kapitel V (KI-Modelle mit allgemeinem Verwendungszweck), Kapitel VII (Governance) und Kapitel XII (Sanktionen – mit Ausnahme des Artikels 101) sowie Artikel 78 (Vertraulichkeit) gelten ab dem 2. August 2025. Artikel 6 Absatz 1 KI-Verordnung (Einstufungsvorschriften für Hochrisiko-KI-Systeme) und die entsprechenden Pflichten für diese Systeme gelten ab dem 2. August 2027.

Diese Verordnung ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat. Sie zielt darauf ab, die verantwortungsvolle Entwicklung und Verwendung künstlicher Intelligenz in der EU zu fördern[1]. Zweck der Verordnung ist es, unter anderem die Einführung von menschenzentrierter und vertrauenswürdiger KI zu fördern und gleichzeitig ein hohes Schutzniveau in Bezug auf Gesundheit, Sicherheit und der in der Charta der Grundrechte der Europäischen Union („Charta“) verankerten Grundrechte, einschließlich Demokratie, Rechtsstaatlichkeit und Umweltschutz, sicherzustellen, den Schutz vor schädlichen Auswirkungen von KI-Systemen in der Union zu gewährleisten und gleichzeitig die Innovation zu unterstützen. In der gesamten Union soll so ein einheitliches hohes Schutzniveau sichergestellt werden, um eine vertrauenswürdige KI zu erreichen und Rechtssicherheit für Akteure sicherzustellen, die KI-Systeme entwickeln, einführen oder verwenden. Dabei geht die KI-Verordnung von einem risikobasierten Ansatz aus.

Die Verordnung definiert dabei auch klar in Art. 3 KI-Verordnung, was unter einem „KI-System“ und unter einem „Risiko“ zu verstehen ist: Ein „KI-System“ ist ein maschinengestütztes System, das für einen in unterschiedlichem Grade autonomen Betrieb ausgelegt ist und das nach seiner Betriebsaufnahme anpassungsfähig sein kann und das aus den erhaltenen Eingaben für explizite oder implizite Ziele ableitet, wie Ausgaben wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erstellt werden, die physische oder virtuelle Umgebungen beeinflussen können. Ein „Risiko“, so die Begriffsbestimmung, ist die Kombination aus der Wahrscheinlichkeit des Auftretens eines Schadens und der Schwere dieses Schadens.

Entsprechend dem Erwägungsgrund 26 KI-Verordnung ist es aber auch notwendig, bestimmte inakzeptable Praktiken im Bereich der KI zu verbieten und Anforderungen an Hochrisiko-KI-Systeme und Pflichten für die betreffenden Akteure sowie Transparenzpflichten für bestimmte KI-Systeme festzulegen. Diese Anforderungen, so Erwägungsgrund 66 der KI-Verordnung, sollten für Hochrisiko-KI-Systeme im Hinblick auf das Risikomanagement, die Qualität und Relevanz der verwendeten Datensätze, die technische Dokumentation und die Aufzeichnungspflichten, die Transparenz und die Bereitstellung von Informationen für die Betreiber, die menschliche Aufsicht sowie

[1] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401689

die Robustheit, Genauigkeit und Sicherheit gelten. Diese Anforderungen sind erforderlich, um die Risiken für Gesundheit, Sicherheit und Grundrechte wirksam zu mindern.
Hochrisiko-KI-Systeme gemäß Art. 6 Abs. 2 KI-Verordnung sind in der Anlage III der KI-Verordnung bereichsspezifisch aufgeführt.
Die KI-Verordnung weist auch auf die Gefahren von Verwendungsmöglichkeiten der KI-Systeme hin. Im Erwägungsgrund 28 der KI-Verordnung heißt es dazu: „Abgesehen von den zahlreichen nutzbringenden Verwendungsmöglichkeiten von KI kann diese Technologie auch missbraucht werden und neue und wirkungsvolle Instrumente für manipulative, ausbeuterische und soziale Kontrollpraktiken bieten. Solche Praktiken sind besonders schädlich und missbräuchlich und sollten verboten werden, weil sie im Widerspruch zu den Werten der Union stehen, nämlich der Achtung der Menschenwürde, Freiheit, Gleichheit, Demokratie und Rechtsstaatlichkeit sowie der in der Charta verankerten Grundrechte, einschließlich des Rechts auf Nichtdiskriminierung, Datenschutz und Privatsphäre sowie der Rechte des Kindes.“ Art. 20 KI-Verordnung regelt zudem auch, dass Anbieter von KI-Systemen, einschließlich KI-Systemen mit allgemeinem Verwendungszweck, die synthetische Audio-, Bild-, Video- oder Textinhalte erzeugen, sicherstellen müssen, dass die Ausgaben des KI-Systems in einem maschinenlesbaren Format gekennzeichnet und als künstlich erzeugt oder manipuliert erkennbar sind.
Doch wer kontrolliert eigentlich die ordnungsgemäße Umsetzung der KI-Verordnung? Die Datenschutzkonferenz (DSK), das Gremium der unabhängigen deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder, hatte bereits am 8. Mai 2024 in ihrer Pressemitteilung „Nationale Zuständigkeiten für die Verordnung zur Künstlichen Intelligenz (KI-VO)“ genau diese Frage problematisiert (https://datenschutzkonferenz-online.de/media/pm/2024_05_08_DSK_PM_KI_VO_Zustaendigkeiten.pdf). In ihrem entsprechenden Beschluss dazu heißt es: „Die Benennung der jeweiligen allgemeinen Marktüberwachungsbehörden in den Mitgliedsstaaten ist in der KI-VO nicht dediziert geregelt. Es finden sich nur vereinzelt Vorgaben, die bei der nationalen Bestimmung zu berücksichtigen sind. Für Deutschland muss – wie in anderen Mitgliedstaaten auch – in einem nationalen Umsetzungsgesetz festgelegt werden, welcher oder welchen unabhängigen nationalen Behörden die jeweiligen Zuständigkeiten zugewiesen werden (Art. 70 Abs. 1 KI-

VO). Dabei muss gleichzeitig auch eine hinreichende Bereitstellung aufgabengerechter zusätzlicher Ressourcen mitgedacht werden."
So empfahl die DSK unter anderem die Funktion der Marktüberwachungsbehörden dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) und den Landesdatenschutzbehörden zu übertragen, auch um so Synergieeffekte zu erreichen und Kompetenzen zu bündeln. Mit dem Hinweis: „Wird ein KI-System bundesweit als Produkt angeboten oder aus dem internen Gebrauch heraus zum externen Vertrieb auf den Markt gebracht, liegt die Zuständigkeit hierfür beim Bund. Insbesondere die Nutzung oder die Entwicklung von KI-Systemen für den internen Gebrauch durch Unternehmen und Behörden wird von den Landesdatenschutzbehörden beziehungsweise der Bundesdatenschutzbehörde in ihrer jeweiligen Zuständigkeit überwacht."
Die DSK hat in ihrer 108. Konferenz am 15. November 2024 zudem einen Arbeitskreis KI gebildet: „Ein Schwerpunkt der Konferenz betraf die Entwicklung und den Einsatz von Modellen und Systemen Künstlicher Intelligenz (KI). Diese will die DSK zielführend und konstruktiv begleiten. Zentrales Ziel soll dabei sein, Anforderungen und Handlungsempfehlungen zu entwickeln, um KI datenschutzkonform zu realisieren und einzusetzen. Um ihre bisherige Arbeit in diesem Bereich zu verstetigen, hat die DSK einen Arbeitskreis Künstliche Intelligenz gebildet. Dieser vereinigt technische und rechtliche Expertise aller in der DSK verbundenen Aufsichtsbehörden. Er soll die Entwicklungen und Wirkungen sowohl der KI-Technologien als auch der KI-Regulierung beobachten, konstruktiv-kritische Beiträge zu aktuellen Diskussionen um KI leisten und dazu beitragen, dass sich die Aufsichtstätigkeit innovationsfreundlich und risikospezifisch fortentwickeln kann."
„Für die nächste Zeit hat die DSK dem Arbeitskreis aufgegeben, sich mit der Erhebung und Vorbereitung von Trainingsdaten, dem Training mit personenbezogenen Daten, den Auswirkungen eines rechtswidrigen Trainings auf die Rechtmäßigkeit des Einsatzes eines KI-Modells sowie mit der Umsetzung von Betroffenenrechten zu befassen.", siehe https://www.datenschutzkonferenz-online.de/media/pm/2024-11-15_PM_108_DSK.pdf. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit hat in diesen Arbeitskreis auch zwei Mitarbeiter entsandt, um technisch und juristisch diese neuen Anforderungen aktiv mitzugestalten.

1.3 Zwischenbericht der *ChatGPT TaskForce*

Der Europäische Datenschutzausschuss hat eine spezielle Arbeitsgruppe *ChatGPT TaskForce* zur Förderung der Zusammenarbeit und zum Austausch von Informationen über mögliche Durchsetzungsmaßnahmen der Datenschutzbehörden eingesetzt. Diese Arbeitsgruppe, an der auch der TLfDI beteiligt ist, hat im Mai 2024 einen ersten Zwischenbericht veröffentlicht und benennt darin eine Reihe von datenschutzrechtlichen Problempunkten, die zu beachten sind.

Seit ChatGPT im November 2022 als Textgenerator und Chatbot durch die US-amerikanische Firma OpenAI einer breiten Bevölkerung zur Verfügung gestellt wurde, ist das Thema Künstliche Intelligenz (KI) auch in der breiten Öffentlichkeit angekommen. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit berichtete darüber bereits ausführlich in seinem 6. Tätigkeitsbericht 2023 unter Punkt 1.3. Der Europäische Datenschutzausschuss (englisch *European Data Protection Board, EDPB*), eine unabhängige europäische Einrichtung mit dem Ziel, die einheitliche Anwendung der Datenschutz-Grundverordnung (DS-GVO) sicherzustellen und die Zusammenarbeit zwischen den Datenschutzbehörden der EU zu fördern, nahm sich dem Thema an. So wurde 2023 geplant, eine spezielle Arbeitsgruppe *ChatGPT TaskForce* zur Förderung der Zusammenarbeit und zum Austausch von Informationen über mögliche Durchsetzungsmaßnahmen der Datenschutzbehörden einzusetzen. Denn relativ schnell wurde klar, dass bei Weitem nicht alle datenschutzrechtlichen Fragestellungen geklärt sind. Vor allem die Systemeigenschaft, dass offensichtlich Wissen im Textgenerator vorhanden ist, welches durch Anfragen preisgegeben wird, ist datenschutzrechtlich zu beleuchten. Es stellen sich Fragen dazu, welches Wissen überhaupt abrufbar ist. Sind darunter auch personenbezogen Daten, die nicht in der breiten Öffentlichkeit bekannt sind? Hat das System eventuell beim Lernen auch gelernt, Eigenschaften von Personen zu klassifizieren (wie zum Beispiel ob eine Person homosexuell ist oder nicht)? Wie zuverlässig sind Fakten in generierten Texten? Kurz: Welche Gefahren gehen tatsächlich von einem solchen Textgenerator aus, aber auch, welche Gegenmaßnahmen hat OpenAI implementiert, um Gefahren angemessen zu begegnen?
Im Mai 2024 hat die gegründete Arbeitsgruppe *ChatGPT Taskforce* einen Zwischenbericht veröffentlicht. Auch der TLfDI war als ein

Vertreter der deutschen Datenschutzaufsichtsbehörden involviert. Der Bericht ist unter https://www.edpb.europa.eu/system/files/2024-05/edpb_20240523_report_chatgpt_taskforce_en.pdf abrufbar.
In diesem Bericht werden Punkte aufgegriffen, die auch durch datenschutzrechtliche Verantwortliche innerhalb Thüringens beachtet werden müssen, die ChatGPT einsetzen.
Folgende Punkte wurden durch den Bericht aufgeworfen, die beim Einsatz von ChatGPT (aber auch bei anderen KI-Modellen) beachtet werden müssen:

- Rechtmäßigkeit der Verarbeitung (Rechtsgrundlage): Der Bericht unterteilt die Verarbeitung personenbezogener Daten in verschiedene Phasen. Während die Phasen der Datensammlung und des Trainings des Sprachmodells vor allen Dingen OpenAI betreffen, werden auch in der Nutzungsphase personenbezogene Daten verarbeitet (Eingaben mit Personenbezug, Ausgaben mit Personenbezug). Diese werden unter Umständen von OpenAI wiederum zu Trainingszwecken genutzt – ebenso wie zu Analysezwecken. Hierzu müssen Verantwortliche innerhalb Thüringens gültige Rechtsgrundlagen nachweisen können. Ausgangspunkt können hier Art. 6 Abs. 1 DS-GVO sowie Art. 9 Abs. 2 DS-GVO sein, aber auch spezialgesetzliche Regelungen.
- Verarbeitung nach Treu und Glauben (Art. 5 Abs. 1 Buchstabe a) DS-GVO): Es wird von einem System erwartet, dass die Datenverarbeitung im erwartbaren Rahmen durchgeführt wird. Der Bericht erwähnt insbesondere, dass das Risiko eines unerwarteten Verhaltens oder einer unerwarteten Verarbeitung nicht einfach auf den Nutzer übertragen werden kann. Verantwortliche müssen sich über Risiken, die sich aus dem Einsatz des Systems ergeben, im Klaren sein, sich im Vorfeld damit beschäftigen, eventuell getroffene Gegenmaßnahmen bewerten und dann erst die Nutzung des Systems zulassen (und regeln). Diese Prüfung darf nicht dem Nutzer allein übertragen werden.
- Informationspflichten: Verantwortliche, die ChatGPT lediglich einsetzen, müssen primär die Informationspflichten für die Nutzungsphase sicherstellen. Dies bedeutet in der Praxis, dass sie die Nutzer darüber aufklären müssen, welche personenbezogenen Daten zu welchen Zwecken bei der Nutzung verarbeitet werden. In diesem Rahmen gelten die Informationspflichten des Art. 13 DS-GVO.

- Richtigkeit (Art. 5 Abs. 1 Buchstabe d) DS-GVO): Der Bericht stellt für diesen Punkt fest, dass ChatGPT in seiner jetzigen Form Fakten beziehungsweise personenbezogene Daten nicht in jedem Fall korrekt wiedergeben kann. Auch eine Berichtigung von Fakten ist momentan nicht möglich – es gibt lediglich Unterdrückungsmechanismen, die als falsch gemeldete Ausgaben unterdrücken, aber nicht berichtigen. Allen Verantwortlichen innerhalb Thüringens sollte dieser Mangel bewusst sein. Mindestens sollten die Nutzer über diese Systemeigenschaft informiert sein, im Zweifel kann dies aber auch zur Unzulässigkeit des Systems führen.
- Betroffenenrechte: Diese betreffen das Recht auf Auskunft, Berichtigung (eher Sperrung), Löschung und so weiter, die in den Art. 15 bis 22 DS-GVO definiert sind. Betroffene (also zum Beispiel Nutzer) dürfen diese Rechte jederzeit wahrnehmen. Verantwortliche innerhalb Thüringens können bei Nutzung von ChatGPT diese Rechte selbst nicht unmittelbar bedienen, sondern müssen die Mittel nutzen, die OpenAI zur Verfügung stellt (siehe dazu Fußnote 32 des Berichtes). Als Verantwortliche müssen sie die Betroffenen auch darüber informieren, wie diese Rechte wahrnehmbar sind.

Insgesamt sollte Verantwortlichen und Nutzern bewusst sein, dass ChatGPT trotz der großen Beliebtheit und enormen Nachfrage noch eine neue Technologie ist, bei der neben dem unbestreitbaren Nutzen die Bedrohungssituation für Betroffene unklar ist. Grundsatzfragen, wie Informationen aus dem Sprachmodell wieder entfernt werden können, wie der Wahrheitsgehalt einer Ausgabe signalisiert oder gemessen werden kann oder wie ein Bürger überhaupt prüfen kann, ob Wissen über ihn im Sprachmodell gespeichert ist, bleiben unklar. Bei aller Euphorie sollte also nach wie vor eine gewisse Vorsicht bei der Nutzung behalten werden.

Aus Sicht der deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder gilt es, bei der Anwendung in Deutschland, die Datenschutz-Grundverordnung einzuhalten. Also für die Verarbeitungsprozesse von personenbezogenen Daten die Transparenz, Kontrolle und bestimmte Rechte von betroffenen Personen zu gewährleisten.

1.4 Die Datenschutzaufsicht im parlamentarischen Bereich – ein Urteil des Europäischen Gerichtshofs wirbelt Staub auf

Der Europäische Gerichthof entschied am 16. Januar 2024, dass die DS-GVO auch auf die parlamentarischen Untersuchungsausschüsse anwendbar ist. Aus den Ausführungen in dem Urteil sieht der TLfDI eine Übertragbarkeit auch auf andere Bereiche der parlamentarischen Tätigkeit des Thüringer Landtags, wenn dabei personenbezogene Daten verarbeitet werden. Eine Anwendbarkeit der DS-GVO hat zur Folge, dass die datenschutzrechtliche Aufsicht derzeit dem TLfDI obliegt, solange die Parlamentarische Datenschutzordnung des Thüringer Landtags den Anforderungen des Artikels 51 ff. DS-GVO noch nicht entspricht. Der EuGH sah durchaus das Konfliktpotenzial zwischen dem Verfassungsrecht und dem Unionsrecht und zeigte deshalb in seinem Urteil eine Lösungsmöglichkeit auf, indem gegebenenfalls mehrere Aufsichtsbehörden eingerichtet werden könnten.

In dem Vorlageverfahren (Österreichische Datenschutzbehörde, Aktenzeichen C-33/22) ging es vor dem Europäischen Gerichtshof (EuGH) um die Frage, ob die Datenschutz-Grundverordnung (DS-GVO) auch auf die parlamentarischen Untersuchungsausschüsse anwendbar ist und wer die Aufsicht über die Durchsetzung der DS-GVO gegenüber den Parlamenten ausübt.
Der EuGH stellte fest, dass „der Umstand, dass es sich […] beim Untersuchungsausschuss um ein Organ handelt, das unmittelbar und ausschließlich parlamentarisch tätig ist, nicht bedeutet, dass die Tätigkeit dieses Untersuchungsausschusses vom Anwendungsbereich der DS-GVO ausgenommen ist“ (Urteil des EuGHs vom 16. Januar 2024, Aktenzeichen: C-33/22 Rn. 40). Dies bekräftigte der Gerichtshof, in dem er ausführte, dass „sich die in Art. 2 Abs. 2 Buchstabe a) DS-GVO vorgesehene Ausnahme vom Anwendungsbereich dieser Verordnung ausschließlich auf Kategorien von Tätigkeiten, die aufgrund ihrer Natur nicht in den Anwendungsbereich des Unionsrechts fallen, und nicht auf Kategorien von Personen (privater oder öffentlich-rechtlicher Natur) und – für den Fall, dass der Verantwortliche eine Behörde ist – auch nicht darauf, dass die Aufgaben und Pflichten dieser Behörde unmittelbar und ausschließlich einer bestimmten hoheitlichen Befugnis zuzurechnen sind, wenn diese Befugnis nicht mit einer Tätigkeit einhergeht, die jedenfalls vom Anwendungsbereich des Unionsrechts ausgenommen ist, bezieht“ (Randnummer 41). Im Ergebnis

sind daher „Art. 16 Abs. 2 Satz 1 AEUV [= Vertrag über die Arbeitsweise der Europäischen Union] und Art. 2 Abs. 2 Buchstabe a) DS-GVO dahin auszulegen […], dass nicht angenommen werden kann, dass eine Tätigkeit allein deshalb außerhalb des Anwendungsbereichs des Unionsrechts liegt und damit der Anwendung der DS-GVO entzogen ist, weil sie von einem vom Parlament eines Mitgliedstaats in Ausübung seines Kontrollrechts der Vollziehung eingesetzten Untersuchungsausschuss ausgeübt wird“ (Randnummer 43).
Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) geht davon aus, dass aus den Ausführungen des EuGHs geschlossen werden kann, dass nicht nur die Verarbeitung von personenbezogenen Daten in Untersuchungsausschüssen, sondern auch andere parlamentarischen Tätigkeiten des Landtags unter die DS-GVO fallen. Diese Ansicht lässt sich auch auf das Urteil des EuGHs vom 9. Juli 2020 stützen (Aktenzeichen: C 272/19), in dem die Anwendbarkeit der DS-GVO auf die Tätigkeit des Petitionsausschusses des Hessischen Landtags bejaht wurde.
Wenn die DS-GVO für den parlamentarischen Untersuchungsausschuss im Thüringer Landtag anzuwenden ist, gelten dementsprechend auch die Regelungen über die Datenschutzaufsicht (Zuständigkeit, Aufgaben, Befugnisse). Hierzu stellte der EuGH in seiner Entscheidung vom 16. Januar 2024 Folgendes fest: „Die Wirkungen des Grundsatzes des Vorrangs des Unionsrechts sind für alle Stellen eines Mitgliedstaats verbindlich, ohne dass dem insbesondere die innerstaatlichen Bestimmungen, auch wenn sie Verfassungsrang haben, entgegenstehen könnten“ (Randnummer 70). Der EuGH wies aber darauf hin, dass Art. 51 Abs. 1 DS-GVO jedem Mitgliedstaat einen Ermessensspielraum einräumt, „der es ihm ermöglicht, so viele Aufsichtsbehörden einzurichten, wie insbesondere aufgrund seiner verfassungsmäßigen Struktur erforderlich sind“ (Randnummer 69). Der Gerichtshof hat somit in seiner Entscheidung das Konfliktpotenzial zwischen dem Verfassungsrecht und dem Unionsrecht gesehen und eine Lösungsmöglichkeit aufgezeigt, indem gegebenenfalls mehrere Aufsichtsbehörden eingerichtet werden könnten.
Eine Datenschutzaufsicht beim Landtag müsste folglich den Anforderungen in den Artikeln 51 ff. DS-GVO entsprechen. Dazu gehören unter anderem die Unabhängigkeit der Stelle (Art. 52 DS-GVO), die Wahl durch das Parlament sowie die erforderliche Qualifikation, Erfahrung und Sachkunde insbesondere im Datenschutzrecht (Art. 53 DS-GVO), Regelungen nach Art. 54 DS-GVO und die Festlegung von

Aufgaben und Befugnissen (Artikel 57, 58 DS-GVO). Dies ist derzeit noch nicht der Fall.
Der TLfDI wandte sich daraufhin an den Thüringer Landtag, um die wesentlichen Aspekte des ergangenen Urteils darzustellen und dessen Schlussfolgerungen und Auswirkungen auf die parlamentarische Tätigkeit des Thüringer Landtags zu erörtern. Im Ergebnis bestand Einigkeit darüber, dass die Aufsicht nach der geltenden Rechtslage derzeit beim TLfDI liegt und er die aufsichtsrechtlichen Befugnisse unter Berücksichtigung der verfassungsrechtlichen Stellung des Thüringer Landtags und seiner Abgeordneten bis zu einer abschließenden Entscheidung des Landtags darüber wahrnimmt, wie die Aufsicht über den parlamentarischen Datenschutz mit den sich aus der DS-GVO ergebenen Anforderungen gestaltet werden muss.

1.5 Cyber-Sicherheitslage

Jährlich wird vom BSI zur „Lage der IT-Sicherheit in Deutschland“ ein Bericht veröffentlicht. Der Bericht für 2024 liegt seit Mitte November 2024 mit Stand Oktober 2024 vor: „Jedes Unternehmen, jede Behörde, jede wissenschaftliche oder soziale Einrichtung, jeder Einzelunternehmer – ganz Deutschland ist aufgerufen, eigene Angriffsflächen zu ermitteln und zu schützen.“

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist die Cybersicherheitsbehörde des Bundes. Es veröffentlicht jährlich einen umfassenden Bericht zur Lage der IT-Sicherheit in Deutschland. Der Bericht „Die Lage der IT-Sicherheit in Deutschland 2024“ liegt seit Mitte November 2024 mit Stand Oktober 2024 vor:
„Als die Cybersicherheitsbehörde des Bundes beobachtet das Bundesamt für Sicherheit in der Informationstechnik (BSI) kontinuierlich die Gefährdungslage der IT-Sicherheit in Deutschland. Im Fokus des BSI stehen die Erkennung von Cyberangriffen auf staatliche sowie öffentliche Institutionen, Unternehmen und Privatpersonen, aber auch Maßnahmen zur Prävention und Abwehr spezifischer Gefahren für die Verfügbarkeit, Unversehrtheit oder Vertraulichkeit der Kommunikationstechnik.“
Nachfolgend soll nur auf einige Themen aus dem BSI-Bericht eingegangen werden: Laut Bericht wurden im Berichtszeitraum täglich durchschnittlich 309.000 neue Schadprogramm-Varianten bekannt.

Das waren rund 26 Prozent mehr als im vergangenen Berichtszeitraum mit durchschnittlich täglich 250.000 neuen Schadprogramm-Varianten. Auch berichtet das BSI, dass Schadprogramme von kriminellen Angreifern in der Regel massenhaft und ungezielt verteilt werden. Anders seien sogenannte APT-Angriffe (APT=Advanced Persistent Threat). Die oft langfristig und mit großem Aufwand geplanten Angriffe haben einzeln ausgewählte, herausgehobene Ziele im Focus. „APT-Angriffe dienen also in der Regel nicht der kriminellen Gewinnerzielung, sondern der Beschaffung von Informationen über das Ziel und gegebenenfalls der Sabotage. Im aktuellen Berichtszeitraum waren nach Kenntnis de s BSI 22 verschiedene APT-Gruppen in Deutschland aktiv, deren Angriffe auf Behörden und Unternehmen insbesondere der auswärtigen Angelegenheiten, der Verteidigung sowie der öffentlichen Sicherheit und Ordnung zielten." Eine Liste dieser Gruppen sowie deren Ziele und Eigenschaften werden im Bericht aufgelistet.
„Jedes Unternehmen, jede Behörde, jede wissenschaftliche oder soziale Einrichtung, jeder Einzelunternehmer – ganz Deutschland ist aufgerufen, eigene Angriffsflächen zu ermitteln und zu schützen."
Weiterhin geht das BSI auch auf Schwächen von KI-Sprachmodellen und ihre Ursachen ein. So sieht das BSI insbesondere die mangelnde Erklärbarkeit, die Abhängigkeit von Trainingsdaten und durch die flexiblen Infrastrukturen begünstigte dynamische Entwicklung als Problem an und erläutert diese. Im Ergebnis kommt das BSI zur Einschätzung: „Der großflächige Einsatz von Sprachmodellen, die damit verbundene kommerzielle Dynamik und die prinzipiellen Unschärfen der Modelle können je nach Kritikalität des Einsatzes ein hohes IT-Sicherheitsrisiko mit sich bringen." Risiken sieht das BSI zum Beispiel bei:

- Phishing: Angreifer setzen Large Language Models (LLMs) ein, um Texte für Phishing-Nachrichten und Webseiten mit Täuschungsabsicht zu erzeugen sowie um Desinformation zu gestalten, die insbesondere vor Wahlen direkte und kurzfristige Auswirkungen haben kann. Auch können jetzt leistungsfähigere KI-Chatbots zum Phishing sowie zur Verbreitung von Desinformation verwendet werden. Diverse Angebote für entsprechende Dienste weisen auf eine rege Nutzung hin. Verbesserte und personalisierte Sprach- und Bildgenerierungen (Deepfakes) in hoher Qualität unterstützen sowohl Erpressungsversuche, wie zum Beispiel Sextortion, als auch die Kompromittierung öffentlich tätiger Personen.

- Technische Angriffsunterstützung: Mit Sprachmodellen kann lauffähiger Schadcode generiert oder iterativ verfeinert werden. Ihre Anwendung ist allerdings schwer nachweisbar.
- Cyberspionage: Sprachmodelle können Angreifern auch bei gezielten Angriffen nützlich sein. Beispielsweise kann ein mit zu vielen internen Daten trainierter Unternehmens-Chatbot Interna offenbaren.

Das BSI empfiehlt daher: „Die Auswirkungen damit einhergehender Bedrohungen sollten mittels Testen, zum Beispiel Pentesting, und der Betrachtung von Worst-Case-Szenarien im Rahmen einer Risikoanalyse eingeschätzt werden."
Weiterhin wird im BSI-Bericht unter anderem auch auf den am 19. Juli 2024 aufgetretenen weltweiten IT-Ausfall eingegangen: „In Deutschland wurden zahlreiche IT-Ausfälle gemeldet, auch bei KRITIS-Betreibern und meldepflichtigen Organisationen. Die IT-Ausfälle traten in Zusammenhang mit einem durchgeführten Update der EDR-Software Falcon auf." Dieser Programmierfehler hatte erhebliche Folgen: „Nach Angaben von Microsoft waren insgesamt circa 8,5 Millionen Windows-Systeme betroffen. Cyberkriminelle haben die IT-Ausfälle für unterschiedliche Formen von Phishing, Scam oder Fake-Webseiten ausgenutzt. Ab dem 21. Juli 2024 normalisierte sich die Lage wieder."
„Die Folgen der weltweiten IT-Störungen im Juli 2024 haben eindrucksvoll gezeigt, wie abhängig unsere digitalisierte Welt von funktionierenden IT-Systemen ist. Dieser Vorfall war ein ungewollter Beleg dafür, dass aufgrund der bestehenden Vernetzungen und damit einhergehenden Abhängigkeiten nur das intensive Zusammenspiel aller Beteiligten zielführend ist. In kürzester Zeit konnten die Ursache ausfindig gemacht, eine Problemlösung gefunden und Betroffene und Öffentlichkeit informiert werden."
Den gesamten Bericht „Die Lage der IT-Sicherheit in Deutschland 2024" finden Sie unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2024.pdf?__blob=publicationFile&v=4.

1.6 Untersuchungen zu Apple Mobile-Device-Management

Der TLfDI hat sich in diesem Berichtszeitraum vertieft mit Mobile-Device-Management-Systemen beschäftigt. Diese kommen zunehmend auch in öffentlichen Stellen wie beispielsweise Schulen zum

Einsatz. Um die Beratung fundiert leisten zu können, wurde Apple Mobile-Device-Management näher untersucht.

Durch die Digitalisierung der Gesellschaft und den enormen Fortschritt in der Miniaturisierung von Rechentechnik verändert sich auch die Art und Weise, mit welchen Hilfsmitteln die täglichen Aufgaben erledigt werden. So sind Smartphones und Tablets neben herkömmlichen Laptops nun integraler Bestandteil der Arbeitskultur – sei es in der Wirtschaft oder im öffentlichen Bereich, wie zum Beispiel in Schulen. Sobald auf diesen Geräten im Schul- oder Arbeitskontext personenbezogene Daten verarbeitet werden, gilt die Datenschutz-Grundverordnung (DS-GVO) und der Verantwortliche muss auch die Sicherheit der Verarbeitung nach Art. 32 DS-GVO auf diesen Geräten sicherstellen. Für feste Arbeitsplatzrechner oder Laptops gibt es dazu etablierte Administrationsvorgehen (siehe https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/cyber-sicherheitsempfehlungen_node.html).
Für Smartphones und Tablets funktioniert die herkömmliche Art der Administration nicht mehr, da es dort keinen klassischen Administrationsnutzer gibt. Für die private Nutzung ist dies auch durchaus ausreichend, aber für größere Organisationen, in denen die dienstlichen Geräte zentral verwaltet werden müssen, sind andere Werkzeuge nötig. Die Hersteller von Smartphones und Tablets haben dieses Problem erkannt und sogenannte Mobile-Device-Management-Lösungen (MDM) nachgerüstet. Diese ermöglichen eine zentrale Verwaltung von Geräten. Insbesondere während der Pandemie und im Rahmen des Digitalpaktes wurden auch in öffentlichen Stellen große Mengen Tablets beschafft.
Daher hat der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) beschlossen, sich technisch tiefgreifender mit dem Thema MDM auseinanderzusetzen. Eine vom TLfDI im Jahr 2024 gestartete Umfrage an Thüringer Schulen ergab, dass diese überwiegend das Apple MDM einsetzen. Dieses System und seine Konfigurationsmöglichkeiten wurden daraufhin im vorliegenden Berichtszeitraum vom TLfDI näher untersucht. Im Mittelpunkt dabei Sicherheitsmechanismen, Konfigurationsmöglichkeiten, Datenflüsse und damit verbundene Verarbeitungszwecke.

Ziel war es, den TLfDI künftig in die Lage zu versetzen, detaillierte Auskünfte vor allem über technische Fragestellungen zum Apple Mobile-Device-Management geben zu können. Aspekte wie Rollout-Modelle, Geräte-Profile, Anmeldevarianten, Einbindung beziehungsweise Deaktivierung von Cloud-Diensten wurden unter anderem dabei betrachtet. Die Auswertung der Untersuchungen ist im Berichtszeitraum noch nicht abgeschlossen. Es konnten zumindest datensparsame Konfigurationsmöglichkeiten getestet und untersucht werden, welche Kontrolle private Personen über vollständig gemanagte Geräte haben. In den vorläufigen Ergebnissen scheint damit eine datenschutzkonforme Nutzung möglich, diese ist aber noch nicht abschließend geklärt. Der TLfDI als Vorsitzender des Arbeitskreises Schule und Bildungseinrichtungen der Datenschutzkonferenz (DSK), dem Gremium der unabhängigen deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder, unterrichtete diesen bereits über die ersten Erkenntnisse. Der TLfDI wird zu diesem Thema zur gegebenen Zeit weiter berichten.

1.7 Entwicklungen zum Thema Microsoft 365 (inkl. EU Data Boundary)

Den TLfDI erreichen nach wie vor Anfragen zum Einsatz von Microsoft-Office-Produkten. An der Bewertung durch den TLfDI hat sich allerdings nichts geändert: Es ist grundsätzlich sehr schwierig einen datenschutzkonformen Einsatz nachzuweisen. Nach neueren Untersuchungen wird aber klar, dass dieses Problem sich auch auf die Offline-Produkte von Office erstrecken kann.

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) berichtet regelmäßig zum Thema Microsoft 365, zuletzt in Punkt 1.4 in seinem 6. Tätigkeitsbericht 2023. Die Datenschutzkonferenz (DSK), das Gremium der unabhängigen deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder, nahm damals am 24. November 2022 einen 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 gegen-

über 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."
Auch im Berichtsjahr 2024 war die Frage, ob weiterhin Microsoft 365 datenschutzrechtskonform betrieben werden kann. So erreichten den TLfDI zu dem Thema zum Beispiel eine Beschwerde zum Einsatz von Microsoft 365 im Schulbereich, eine Anfrage zur Zulässigkeit der Installation der Offline-Versionen (im Bereich der öffentlichen Verwaltung) der Software sowie ein Überprüfungswunsch des veränderten „Data Processing Addendums (DPA)", wie das Vertragswerk zur Auftragsverarbeitung von Microsoft bezeichnet wird, in Bezug auf das EU Data Boundary Projekt von Microsoft. Die Auftragsverarbeitung gilt für alle Online-Verarbeitungstätigkeiten von Microsoft, wie Videokonferenzen, Online-Kollaboration, OneDrive-Nutzung aber auch eher nicht sichtbare Verarbeitungen von zum Beispiel Diagnose- und Telemetriedaten oder die lokale Anmeldung über einen Active Directory Nutzeraccount. Alle Themen hängen in dem Sinn zusammen, dass zu klären ist, ob bei der Nutzung von Microsoft-Produkten der Online-Bereich überhaupt betroffen ist, das heißt, eine Verarbeitung von personenbezogenen Daten durch Microsoft überhaupt stattfindet (und damit das DPA gilt), und ob im Rahmen der online durchgeführten Verarbeitungen die Bedingungen des Art. 5 Abs. 2 Datenschutz-Grundverordnung (DS-GVO) nun erfüllbar sind. Um festzustellen, ob bei der Nutzung von Offline-Anwendungen, bei denen man in erster Linie keine Verarbeitung von Daten seitens Microsoft vermuten würde, doch eine Auftragsverarbeitung stattfindet (und damit das DPA anwendbar wäre), hat der TLfDI sich mit diesen Offline-Anwendungen (Word, Excel, PowerPoint) näher beschäftigt. Zunächst spielt hier die Aktivierung der Produkte eine Rolle. Um Microsoft 365 zu aktivieren, ist in der Regel ein Online-Account nötig. Entweder betreibt diesen ein einzelner Nutzer, der bei Microsoft registriert werden muss (mit Nutzername, E-Mail-Adresse, Passwort, Zahlungsmittel) oder der Nutzer ist Teil einer größeren Struktur (ein sogenannter Tennant), wobei diese Struktur auch online bei Microsoft registriert sein muss. Im Tennant werden Organisationsdetails (nicht personenbezogen) sowie die Nutzer und Rollen in der Organisation definiert (hier ist das Vorhandensein von Personenbezug sehr wahrscheinlich). Da bereits der Nutzer einen persönlichen Online-Account bei Microsoft

benötigt, um das Produkt lizensieren und nutzen zu können, greift das DPA bereits bei der Aktivierung des Produktes und kann nicht umgangen werden. An zweiter Stelle hat der TLfDI das Kommunikationsverhalten von Microsoft 365 untersucht (primär der Anwendungen Word, Excel und PowerPoint). Es ist festzustellen, dass auch diese Anwendungen mit zahlreichen Microsoft-Servern kommunizieren. Dies ist dann kein Problem, wenn dem Verantwortlichen klar ist, welche Datenkategorie zu welchen Verarbeitungszwecken im Auftrag durch Microsoft verarbeitet wird. Diese Information wird allein schon deshalb benötigt, um Betroffenen nach Art. 13 Abs. 1 Buchstabe c) sowie Abs. 2 Buchstabe b), e) und f) sowie Abs. 3 DS-GVO informieren zu können. Die Informationen von Microsoft zu Datenarten und Verarbeitungszwecken werden im DPA dargelegt (Abschnitt „Art der Datenverarbeitung; Eigentumsverhältnisse“). Zu Beginn des DPA werden aber auch „produktspezifische Bestimmungen“ mit in den Kreis der regelnden Dokumente aufgenommen (unter Abschnitt „Definitionen: DPA-Bestimmungen“ des DPA). Zusätzlich fordert Art. 5 Abs. 2 DS-GVO, dass der Verantwortliche, der Verarbeitungen in Auftrag gibt, Rechenschaft über diese Verarbeitungen abgeben kann – also genauer beschreiben kann, bei welchen Tätigkeiten welche Daten-Kategorien zu welchen Zwecken verarbeitet werden. Fallen bei Offline-Anwendungen Datentransfers auf, müssen diese im Sinne des Art. 5 Abs. 1 Buchstabe a) DS-GVO erklärbar sein. Welche Art von Daten bei der Nutzung von Offline-Anwendungen mit Microsoft ausgetauscht werden, ist aber nicht genauer festzustellen. Weder ist erkennbar, ob überhaupt personenbezogene Daten enthalten sind, noch, zu welchen Zwecken welche Kategorien an personenbeziehbaren Daten an die unterschiedlichen Microsoft-Server gesendet werden. Die Wahrscheinlichkeit ist damit zumindest hoch, dass bei Microsoft eine Verarbeitung personenbeziehbarer Daten stattfinden könnte und somit die Anwendung des DPA auch eröffnet ist, wenn „nur“ die Offline-Version der Software genutzt wird – sprich die installierten Apps auf dem Tablet, Smartphone oder auf dem Laptop. Das muss ein Verantwortlicher wissen! Damit gilt für diesen Fall auch unmittelbar das DPA und der unbestimmte Kreis von produktspezifischen „DPA-Bestimmungen“ sowie die Anforderungen an Art. 28 DS-GVO zur Auftragsverarbeitung.

Auch die Betrachtung des EU Data Boundary Projektes hilft nicht weiter. Dieses Projekt wurde im Rahmen des Schrems-II-Urteils von

Microsoft ins Leben gerufen, um festzulegen wann welche Kundendaten oder pseudonymisierten personenbezogenen Daten außerhalb der EU-Datengrenze übertragen werden. Doch zum einen umfasst dieses Vorhaben nicht alle Daten, die an Microsoft-Online-Dienste geschickt werden (siehe https://learn.microsoft.com/de-de/privacy/eudb/eu-data-boundary-learn?culture=de-de&country=de), und zum anderen hilft die EU Data Boundary nicht, die nötige Transparenz nach Art. 5 Abs. 2 DS-GVO herzustellen.
Ein Verantwortlicher hat somit zwei Möglichkeiten, Office Produkte einzusetzen: Einmal kann er die geforderte Rechenschaft nach Art. 5 Abs. 2 DS-GVO herstellen, indem er alle Formulierungen des DPA erläutern kann – insbesondere welche Datenarten zu welchen konkreten Verarbeitungszwecken unter welchen Rechtsgrundlagen im Auftrag durch Microsoft verarbeitet werden. Oder er unterbindet für lokal nutzbare Anwendungen alle Datenübertragungen zu Microsoft-Servern (mit Ausnahme der Produktaktivierung) und weist damit nach, dass die nicht erklärbaren Verarbeitungszwecke des DPA mangels Daten gar nicht stattfinden können. Dem TLfDI ist klar, dass beide Wege extrem aufwendig sind. Daher sollte Microsoft seine Vernetzungsstrategie überdenken, um Verantwortlichen ihre Rechenschaftspflicht zu erleichtern. Das Einhalten der Rechenschaftspflicht ist im Übrigen bei der übergroßen Menge an Open-Source-Alternativen sehr einfach möglich: Diese kommunizieren nämlich gar nicht mit irgendwelchen schwer erklärbaren Servern im Internet.

1.8 AK Schulen und Bildungseinrichtungen

Wenn der Arbeitskreis Schulen und Bildungseinrichtungen der Datenschutzaufsichtsbehörden der 16 Länder und des Bundes zu seiner jährlichen Tagung zusammentrifft, steht eine große Themenvielfalt auf der Tagesordnung. Für Thüringen, als Vorsitzland des Arbeitskreises, empfing zum ersten Mal der neue Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit, Tino Melzer, die Teilnehmer und Teilnehmerinnen in Erfurt.

Früher als gewöhnlich, nämlich bereits im September 2024, trafen sich die für den Bildungsbereich zuständigen Vertreter und Vertreterinnen der Datenschutzaufsichtsbehörden der Länder in Erfurt. Thüringen, das den Vorsitz des Arbeitskreises Schulen und Bildungsein-

richtungen innehat, hatte die Sitzung vom üblichen Termin im Dezember vorgezogen, sodass noch im laufenden Jahr einige Themen weiter vorangetrieben werden konnten. Insbesondere der Einsatz von digitalen Lernangeboten an den Schulen erfordert eine datenschutzrechtliche Orientierung für die Akteure vor Ort. Ein großer Anteil von Anfragen und Beschwerden bei den Aufsichtsbehörden in diesem Bereich ist auf den datenschutzkonformen Einsatz solcher Anwendungen gerichtet. Verschiedene Projekte streben dabei an, digitale Bildungsangebote für den Einsatz an Schulen auf unterschiedlichen Wegen sicher zu machen. Dafür bedarf es weiter der engen Abstimmung mit den jeweiligen Datenschutzaufsichtsbehörden und Bildungsministerien der Länder.

Die mittlerweile weit verbreitete Einführung von sogenannten Tablet-Klassen, die für die Schülerinnen und Schüler zumeist die verpflichtende Nutzung eines iPads zur Folge hat, ist Gegenstand einer technischen Untersuchung des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Das gemäß einer Umfrage an Thüringer Schulen am häufigsten verwendete Mobile Device Management (MDM) „JAMF“ wird dabei im Rahmen eines Projekts in einer Testumgebung untersucht. Zu diesem Thema fand ein reger Austausch der Aufsichtsbehörden statt, der auch im Rahmen einer Arbeitsgruppe weiterverfolgt wird.

Eine länderübergreifende Problematik stellt auch der Austausch von personenbezogenen Schülerdaten zwischen Schule und Schulsozialarbeit dar. Die Schulsozialarbeit ist in den vergangenen Jahren seit der Corona-Pandemie verstärkt in den Schulalltag einbezogen worden. Träger der Schulsozialarbeit sind jedoch in der Regel externe Institutionen, sodass ein Datenaustausch zwischen Schule und Schulsozialarbeit nur über eine entsprechende Einwilligung der Schülerinnen und Schüler beziehungsweise deren Sorgeberechtigten erfolgen kann. Hier fehlen in den Ländern zum Teil die rechtlichen Vorgaben, die eine notwendige Abstimmung zwischen Schule und Schulsozialarbeit verbindlich regeln, ohne den notwendigen Vertrauensschutz für die Schülerinnen und Schüler außer Kraft zu setzen.

Das Thema Videoüberwachung an Schulen war ebenfalls ein Diskussionspunkt auf der Tagesordnung, bei dem es um einen Meinungsaustausch zwischen den Aufsichtsbehörden ging. Mehrheitlich erteilten die Länder einem solchen Vorhaben, insbesondere während der Schulzeit, eine klare Absage. Wenngleich die Notwendigkeit, Vandalismus konsequent zu ahnden, nachvollziehbar ist, überwiegen klar die

schutzwürdigen Interessen der Kinder und Jugendlichen denen der Schule oder dem Schulträger nach Aufklärung und Verfolgung der Täter. Auch in Thüringen kann nach § 30 Thüringer Datenschutzgesetz die Verfolgung der Täter nie Hauptzweck der Videoüberwachung sein.
Einigkeit bestand hingegen bei der Frage, ob Prüflinge an Schulen und Hochschulen einen Anspruch auf Überlassung einer unentgeltlichen Kopie ihrer Abschluss- und Zwischenprüfungsarbeiten haben. Auch wenn dies in der Praxis noch nicht überall angekommen zu sein scheint, leitet sich der Anspruch aus Art. 15 Abs. 1 und Abs. 3 Satz 1 in Verbindung mit Art. 12 Abs. 5 Satz 1 Datenschutz-Grundverordnung zweifelsfrei her, wie auch Urteile des Bundesverwaltungsgerichts und des Europäischen Gerichtshofs bestätigt haben. Dabei haben die Prüflinge Anspruch auf eine Kopie ihrer Prüfungsleistung selbst sowie deren Bewertungen, die Prüfungsaufgaben sind hingegen nicht Bestanteil des Auskunftsanspruchs.
Mit vielen weiteren Themen und Abstimmungen war die arbeitsreiche zweitätige Sitzung geprägt von einem offenen und kollegialen Austausch, der auch die Zusammenarbeit in der Datenschutzkonferenz prägt. Mit Videokonferenzen, Informations- und Rundschreiben zu aktuellen Themen tauschen sich die Konferenzteilnehmer bis zur nächsten Sitzung im September 2025 fortlaufend aus.

1.9 Datenschützer mit Gemeinschaftsstand auf Europas größter Bildungsmesse didacta 2024 in Köln

Wenn es um die neuesten Trends, Methoden und Produkte in Sachen Bildung geht, ist die „didacta“ der *place to be*. Zur größten Fachmesse im Bildungsbereich in Europa war im Jahr 2024 erstmals auch der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit mit einem Gemeinschaftsstand mit anderen Landesdatenschutzbeauftragten vertreten und hat zahlreiche Besucher zum Datenschutz in Kindergärten, Schulen und Hochschulen beraten.

Dass Schulnoten nicht vor der Klasse verkündet und Lehrkräfte mit ihren Schülern nicht per WhatsApp kommunizieren sollen, dürfte mittlerweile bekannt sein. Doch im Bildungsbereich sind nicht zuletzt durch die zunehmenden digitalen Lernangebote immer komplexere datenschutzrechtliche Fragestellungen zu beachten. Um hier Lösungen aufzuzeigen und Lehrkräfte, Erzieher und andere Multiplikatoren

zu sensibilisieren, hatten sich die Datenschutzaufsichtsbehörden aus Thüringen, Hessen, Berlin und Baden-Württemberg zusammengetan und eine Woche lang in Köln Hunderte von Besucherinnen und Besuchern der Bildungsmesse didacta beraten und deren Fragen beantwortet.

Unter der organisatorischen Leitung Thüringens hatten sich die beteiligten Datenschutzbehörden unter anderem zum Ziel gesetzt, Berührungsängste und Vorurteile gegen den Datenschutz abzubauen und Möglichkeiten aufzuzeigen, wie moderne digitale Lernangebote datenschutzkonform eingesetzt werden können. Durch die Corona-Pandemie – und die sich in diesem Rahmen rasant entwickelte Digitalisierung im Bildungsbereich – war bei den meisten Standbesuchern eine erfreuliche Vorkenntnis in Sachen Datenschutz in Kita und Schule zu verzeichnen. Oft drehten sich die Gespräche um konkrete Anwendungen und spezielle Situationen vor allem im Schulbereich. Aus Sicht der Datenschützer ist besonders positiv hervorzuheben, dass in den meisten Fällen der Datenschutz bereits mit bedacht wurde, wenngleich in den Detailfragen manchmal rechtliche Unsicherheit bestand. Hier konnte viel Aufklärung und Vermittlungsarbeit geleistet werden.

In den Gesprächen mit dem überwiegenden Fachpublikum sahen sich die Vertreter der Datenschutzbehörden jedoch auch immer wieder mit dem Vorwurf konfrontiert, dass der Datenschutz gute Projekte verhindere. Doch häufig waren es schlicht falsche Informationen und Einschätzungen, auf denen diese negative Haltung beruhte. Datenschutz verhindert nicht, er schützt insbesondere auch Kinder und Jugendliche, die noch nicht selbst in eine Verarbeitung ihrer Daten einwilligen können. Außerdem ist er ein im Grundgesetz verankertes Grundrecht – und die Vermittlung von Grundrechten und dem Rechtsstaatsprinzip ist ebenfalls Bestandteil des Bildungsauftrags in Deutschland. Unter dieser Prämisse verliefen die Gespräche mit den Lehrkräften und Pädagogen offen und ergebnisorientiert. Viele Besucher konnten Hilfestellung bei der Bewertung von datenschutzrechtlichen Fragen und Vorgängen im Kita- und Schulbereich mit nach Haus nehmen, genauso wie kleine Preise, die es bei der richtigen Lösung von Quiz-Fragen zum Thema Datenschutz gab.

Interessant war für die Datenschützer selbst auch der Rundgang über die Messe. Unzählige Innovationen, technische und digitale Entwicklungen sowie insbesondere der Einsatz von künstlicher Intelligenz im

Bildungsbereich werden in den kommenden Jahren noch für herausfordernde und umfangreiche datenschutzrechtliche Problemstellungen sorgen. Hier weiter den Ausgleich zwischen der Einhaltung der Grundrechte, dem Vermitteln von Medienkompetenz und dem innovativen Einsatz neuer digitaler Möglichkeiten zu begleiten, wird Aufgabe der Datenschutzaufsichtsbehörden sein. Daher wird es auch auf der didacta 2025 in Stuttgart einen Stand der Datenschützer als Anlaufstelle für alle Belange rund um den sicheren Umgang mit personenbezogenen Daten geben.

1.10 Entwurf Prüfschema zu Art. 33 DS-GVO

Nach Art. 33 DS-GVO muss der Verantwortliche Verletzungen des Schutzes personenbezogener Daten, die voraussichtlich zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führen, der Aufsichtsbehörde unverzüglich melden. In diesem Beitrag wird beschrieben, wie das Verfahren nach Art. 33 DS-GVO beim TLfDI abläuft.

Wenn eine Meldung nach Art. 33 der Datenschutz-Grundverordnung (DS-GVO) beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) eingeht, prüft der TLfDI zunächst, ob es sich wirklich um eine Meldung nach Art. 33 DS-GVO durch den Verantwortlichen handelt oder nicht doch um eine Beschwerde nach Art. 77 DS-GVO durch die betroffene Person. Nicht selten betiteln Beschwerdeführer ihre Eingaben als Meldungen nach Art. 33 DS-GVO.
Steht fest, dass es sich um eine Meldung nach Art. 33 DS-GVO handelt, wird geprüft, ob eine Verletzung des Schutzes personenbezogener Daten vorliegt. Die Frage ist, ob personenbezogene Daten im Sinne von Art. 4 Nr. 1 DS-GVO betroffen sind oder lediglich sonstige Daten. Außerdem muss ihr Schutz verletzt sein. Das heißt, es ist unbeabsichtigt oder auch beabsichtigt zur Vernichtung, zum Verlust oder zur Veränderung beziehungsweise unbewussten Offenlegung oder einem unbefugten Zugang zu diesen personenbezogenen Daten gekommen, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden. Sollte eine dieser beiden Voraussetzungen nicht gegeben sein, wird ein entsprechender Hinweis an den Verantwortlichen gegeben und der Vorgang wird geschlossen.

Im nächsten Schritt wird geprüft, ob der Vorfall unverzüglich, mindestens jedoch innerhalb von 72 Stunden nach dem Bekanntwerden, gemeldet wurde. Sollte dies nicht der Fall sein, wird geprüft, ob eine Begründung für die Verzögerung vorliegt, falls nicht, wird diese erfragt. Sollte es sich um eine erhebliche Verzögerung ohne nachvollziehbarer Begründung handeln, wird die Angelegenheit an die Bußgeldstelle zur Prüfung der Einleitung eines Ordnungswidrigkeitenverfahrens abgegeben. Nach Art. 33. Abs. 1 Satz 1 DS-GVO ist der Verantwortliche verpflichtet, die Meldung unverzüglich und möglichst binnen 72 Stunden, nachdem die Verletzung bekannt wurde, der Aufsichtsbehörde zu melden. Dabei handelt es sich um eine gesetzliche Verpflichtung. Der Verstoß gegen sie ist nach Art. 83 Abs. 4 Buchstabe a) DS-GVO ein Bußgeldtatbestand. Bei geringfügigen Abweichungen mit triftigem Grund kann der TLfDI von der Einleitung eines Bußgeldverfahrens absehen.
Eingereicht werden muss die Meldung nach Art. 33 DS-GVO durch den Verantwortlichen. Sollte eine andere Stelle, beispielsweise der Auftragsverarbeiter, die Meldung abgegeben haben, wird dieser darauf hingewiesen, dass eine Meldung durch den Verantwortlichen erforderlich ist. Gegebenenfalls wird in diesem Fall auf die für ihn zuständige Aufsichtsbehörde verwiesen, sollte es sich dabei nicht um den TLfDI handeln.
Erst dann wird die Meldung auf Vollständigkeit geprüft. Eine Meldung muss die Art der Verletzung des Schutzes personenbezogener Daten beschreiben, Kategorien der betroffenen Personen und ihre ungefähre Zahl angeben. Der Name und die Kontaktdaten des Datenschutzbeauftragten müssen aufgeführt sein und wahrscheinliche Folgen ebenso beschrieben werden wie die ergriffenen Maßnahmen. Auch muss die Meldung dazu Angaben enthalten, ob die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die betroffenen Personen mit sich bringt. Sollte dies nach Ansicht des Verantwortlichen nicht der Fall sein, muss begründet werden, warum kein hohes Risiko erwartet wird. Wenn diese Angaben nicht gemacht wurden, werden sie durch den TLfDI mit kurzer Frist nachgefordert.
Der TLfDI prüft dann, wenn die Unterlagen vollständig sind, ob die ergriffenen Maßnahmen ausreichend und nachvollziehbar sind und ob gegebenenfalls weitere Maßnahmen erforderlich sind, um dem Risiko für die betroffenen Personen angemessen zu begegnen. Falls dies nicht

der Fall ist, wird der Verantwortliche angeschrieben und ihm wird mitgeteilt, welche weiteren Maßnahmen der TLfDI für erforderlich hält.
Schließlich wird geprüft, ob die betroffenen Personen nach Art. 34 DS-GVO benachrichtigt worden sind. Dies muss erfolgen, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für diese Personen mit sich bringt. Dies ist in der Regel der Fall, wenn eine Verarbeitung besonderer Kategorien personenbezogener Daten nach Art. 9 Abs. 1 DS-GVO stattgefunden hat, wie beispielsweise Gesundheitsdaten. Darüber hinaus kann auch bei der Verletzung des Schutzes anderer personenbezogener Daten – wie beispielsweise Bankverbindungen und Kreditkartendaten – ein hohes Risiko bestehen. Dies liegt in der Regel dann vor, wenn aufgrund des Verlustes der Kontrolle über die Daten physische, materielle oder immaterielle Schäden drohen, wie beispielsweise Diskriminierung, Identitätsdiebstahl oder finanzielle Verluste, Rufschädigung oder Verlust der Vertraulichkeit von Berufsgeheimnissen.
Eine Benachrichtigung der betroffenen Personen ist ausnahmsweise dann nicht erforderlich, wenn der Verantwortliche geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen und diese Vorkehrungen auf die Verletzung der betroffenen Personen angewandt hat, insbesondere durch die die personenbezogenen Daten für alle Personen, die nicht zum Zugang befugt sind, unzugänglich gemacht wurden, etwa durch Verschlüsselung. Sollte die Benachrichtigung der betroffenen Personen unterblieben sein, obwohl voraussichtlich ein hohes Risiko besteht, wird der TLfDI den Verantwortlichen darauf hinweisen.
Der gesamte Schriftverkehr mit dem Verantwortlichen oder dem Meldenden erfolgt im Rahmen des Verfahrens nach Art. 33 DS-GVO in einem informellen Verfahren. Das bedeutet, dass es sich (noch) nicht um ein Verwaltungsverfahren handelt, dass den Erlass einer Maßnahme zum Ziel hat. Die Schreiben des TLfDI haben in dieser Phase des Verfahrens lediglich Empfehlungscharakter und sind (noch) nicht verbindlich. Kommt der Verantwortliche den Anforderungen, die der TLfDI aufstellt, allerdings aus nicht nachvollziehbaren Gründen nicht nach, wird dieser ein Verwaltungsverfahren eröffnen, um möglicherweise Maßnahmen nach Art. 58 Abs. 2 DS-GVO zu ergreifen um das jeweils gebotene Verhalten gegenüber dem Verantwortlichen durchzusetzen.
Der TLfDI hat mit dieser Art der Verfahrensgestaltung in der Vergangenheit positive Erfahrungen gemacht, da die Verantwortlichen sich

in aller Regel datenschutzkonform verhalten möchten und den „Forderungen“ des TLfDI nachkommen. Ein informelles Verfahren hat den Vorteil, dass es schneller durchgeführt werden kann, sodass auf effektive Weise wieder datenschutzgerechte Zustände hergestellt werden können. Außerdem ist das Verfahren für den Verantwortlichen nicht mit erheblichen Kosten verbunden.
Der Ablaufplan für die Bearbeitung einer Meldung nach Art. 33 DS-GVO ist auch im Webauftritt des TLfDI unter https://www.tlfdi.de/fileadmin/tlfdi/info/Veroeffentlichungen_nach_dem_ThuerTG/interne_Dokumente__OV_S_/Pruefschema_Meldung_Verletzung_des_Schutzes_persbezog._Daten_nach_Art._33_DS-GVO.pdf veröffentlicht.

1.11 Erleichterungen für die Einreichung von Beschwerden rund um den EU-U.S. Data Privacy Framework – dank FAQ und Beschwerdeformularen auf der TLfDI-Homepage

Seit dem Sommer 2023 finden sich auf der Internet-Seite des TLfDI zwei neue Formulare: Zum einen ein Formular zum Beschwerdeverfahren für Personen in der EU/dem EWR im Zusammenhang mit möglichen Verstößen gegen das US-Recht bei der Erhebung personenbezogener Daten durch die US-Nachrichtendienste und zum anderen ein Formular auf der Grundlage des EU-US-Data Privacy Framework im Zusammenhang mit gewerblichen Angelegenheiten bei EU-Datenschutzbehörden.

Die Verarbeitung personenbezogener Daten macht in der globalisierten und digitalisierten Welt an keiner Landesgrenze und auch nicht an der Außengrenze der Europäischen Union (EU) halt. Jeden Tag werden Kundendaten, Beschäftigtendaten oder personenbezogene Daten von Social-Media-Nutzenden an Unternehmen außerhalb Europas übermittelt. Das hat auch die Europäische Datenschutz-Grundverordnung (DS-GVO) frühzeitig erkannt und deshalb in einem eigenen Kapitel V die Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen geregelt (Art. 44 bis Art. 50 DS-GVO).
Insbesondere eine Datenübermittlung in die Vereinigten Staaten von Amerika (USA) ist dabei nicht frei von rechtlichen Problemen: Bereits zweimal musste der Europäische Gerichtshof (EuGH) dazu Recht

sprechen. Im Jahr 2015 (EuGH, Urteil vom 06.10.2015 – Aktenzeichen: C-362/14) erklärte er das Safe-Harbor-Abkommen, das seinerzeit die Datenübermittlung zwischen der Europäischen Union und den USA regelte, für unwirksam. Grund dafür war, dass die EU-Kommission in dem damaligen Abkommen die Sicherheit der übermittelten personenbezogenen Daten im Hinblick auf den Zugriff durch US-amerikanische öffentliche Stellen nicht ausreichend in den Fokus genommen hatte. Aber auch das Nachfolge-Abkommen, das EU/US Privacy Shield und den darauf gegründeten Beschluss 2016/1250 erklärte der EuGH 2012 für ungültig (EuGH, Urteil vom 16.07.2020, Aktenzeichen: C 311/18), weil die US-amerikanischen Überwachungsprogramme und ihre rechtlichen Grundlagen nicht auf das zwingend erforderliche Maß beschränkt waren und daher gegen den unionsrechtlichen Grundsatz der Verhältnismäßigkeit verstießen.
Seit dem Jahr 2022 verhandelten die US-Administration und die EU-Kommission erneut ein Abkommen zur datenschutzgerechten Übermittlung personenbezogener Daten in die USA. Den Entwurf für einen solchen Angemessenheitsbeschluss veröffentlichte die EU-Kommission am 13. Dezember 2022. Trotz deutlich geäußerter Kritik ist der Angemessenheitsbeschluss am 10. Juli 2023 unter dem Namen EU-U.S Data Privacy Framework (EU-U.S. DPF) in Kraft getreten.
Wenn nun ein EU-U.S. DPF-zertifiziertes Unternehmen, an das personenbezogene Daten eines EU-Bürgers/ einer EU-Bürgerin übermittelt worden sind, mit seiner Datenverarbeitung gegen die Pflichten aus dem EU-U.-S. DPF verstößt, kann sich der betreffende Bürger/die betreffende Bürgerin mit seiner/ihrer Beschwerde an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) wenden. Dazu haben die Datenschutzbehörden der EU-Mitgliedstaten ein Beschwerdeformular entwickelt, das auf der Seite des TLfDI abrufbar ist: https://tlfdi.de/fileadmin/tlfdi/Europa/Internationaler_Datenverkehr/Beschwerdeformular_DPF-Nachrichtendienste.pdf. Mit der Verwendung dieses Formulars wird sichergestellt, dass alle Informationen, die für eine Bearbeitung des Anliegens erforderlich sind, auch zur Verfügung stehen. Das Beschwerdeformular ist auch verwendbar, wenn es noch um Übermittlungen personenbezogener Daten auf der Grundlage des Vorgängerabkommen, des EU-U.S. Privacy Shield, geht.
Ferner ist auf der Seite des TLfDI ein weiteres Beschwerdeformular zu finden, nämlich für ungelöste EU-U.S. DPF-Beschwerden von Pri-

vatpersonen über den Umgang mit personenbezogenen Daten im Zusammenhang mit gewerblichen Angelegenheiten, die gemäß der DS-GVO aus der EU übermittelt wurden und für die das informelle Gremium der EU-Datenschutzbehörden zur Beratung der involvierten US-Unternehmen zuständig ist, (siehe dazu das Formular auf der Seite des TLfDI: https://tlfdi.de/fileadmin/tlfdi/Europa/Internationaler_Datenverkehr/DPF_Template_Complaint_Form_Commercial_complaints.pdf). Für diese Beschwerden hat sich das informelle Gremium der EU eine Geschäftsordnung gegeben, die ebenfalls auf der Seite des TLfDI abrufbar ist, und zwar unter: https://tlfdi.de/fileadmin/tlfdi/Europa/Internationaler_Datenverkehr/DPF_Rules_of_Procedure_Informal_Panel_DPAs_DE_UEbersetzung_f.pdf.
Abgerundet wird dieses Serviceangebot durch zwei sogenannte Häufig-gestellte-Fragen-Übersichten (auf Englisch: frequently asked questions-lists [FAQ-lists]), in denen die wichtigsten Probleme und Antworten darauf zum einen für Privatpersonen (abrufbar unter: https://tlfdi.de/fileadmin/tlfdi/Europa/Internationaler_Datenverkehr/DPF_F.A.Q.-Privatpersonen.pdf) und zum anderen für Unternehmen (abrufbar unter: https://tlfdi.de/fileadmin/tlfdi/Europa/Internationaler_Datenverkehr/DPF_F.A.Q.-Unternehmen.pdf) thematisiert werden.

1.12 Aufsichtsbehörden geben Hilfestellung bei Unternehmensveräußerungen

Am 11. September 2024 hat die Datenschutzkonferenz, die aus Vertretern aller Aufsichtsbehörden des Bundes und der Länder besteht, einen neuen Beschluss in Bezug auf die Übermittlung personenbezogener Daten an Erwerber eines Unternehmens im Rahmen eines sog. „Asset Deals“ getroffen. Der alte Beschluss vom 24 Mai 2019 wurde damit abgelöst und die Vorgaben für datenschutzrechtliche Fragestellungen in Bezug auf Unternehmensveräußerungen durch den neuen Beschluss konkretisiert.

Werden Unternehmen durch Übertragung von Vermögenswerten und/oder Wirtschaftsgütern (wie zum Beispiel Grundstücken, Gebäuden, Maschinen, dem Kundenstamm oder Rechten) veräußert, handelt es sich um einen sogenannten Asset Deal. Ein solcher liegt zum Beispiel vor, wenn eine Einzelunternehmerin oder ein Einzelunternehmer

ihren oder seinen Betrieb an eine Nachfolgerin oder Nachfolger übergibt und hier beispielsweise die Maschinen, der Kundenstamm et cetera übernommen werden und der Betrieb fortgeführt wird. Hier ergeben sich in Bezug auf die Weitergabe der Kundendaten datenschutzrechtliche Fragestellungen.
Insbesondere bei Daten der Kundinnen und Kunden muss in Bezug auf eine zulässige Übermittlung der Daten nach verschiedenen Stadien der Vertragsabwicklung unterschieden werden. Sofern nur Vertragsverhandlungen zwischen dem Veräußerer und dem Erwerber geführt werden, ist die Übermittlung der personenbezogenen Daten grundsätzlich unzulässig. Etwaige Ausnahmen oder zulässige Fallkonstellationen werden in dem Beschluss umfassend beschrieben. Im Fall der Vertragsanbahnung, also, wenn zwischen Veräußerer und Erwerber bereits konkrete Vertragsverhandlungen geführt werden, hat der Veräußerer vor der Vornahme einer Übermittlung der personenbezogenen Daten der Kunden zu prüfen, ob keine überwiegenden Interessen der Kundinnen und Kunden den eigenen berechtigten Interessen an der Übermittlung entgegenstehen (Art. 6 Abs. 1 Satz 1 Buchstabe f) Datenschutz-Grundverordnung [DS-GVO]). In aller Regel können die Interessen der Kunden durch eine Widerspruchslösung gewahrt werden. Hierbei wird den Kundinnen und Kunden die Datenübermittlung an den Erwerber angekündigt und eine angemessene Frist für einen Widerspruch eingeräumt. Ein solcher Widerspruch ist dann durch den Veräußerer zu beachten und die Daten dürfen nicht an den Erwerber übermittelt werden.
In Bezug auf laufende Vertragsbeziehungen zwischen Veräußerer und Kundinnen oder Kunden ist ebenfalls wiederum eine Unterscheidung notwendig, um die Rechtsgrundlage für eine Datenübermittlung ermitteln zu können. Übernimmt der Erwerber die Verträge und wird selbst Schuldner oder Gläubiger der jeweiligen Kunden, erfüllt der Erwerber den Vertrag mit den Kunden. Dann kann die Verarbeitung der Daten die für die vorzunehmende Vertragserfüllung auf Art. 6 Abs. 1 Satz 1 Buchstabe b) DS-GVO gestützt werden. Sofern der Erwerber den Veräußerer lediglich von seiner Schuld gegenüber den Kundinnen und Kunden freistellen soll, handelt es sich um eine reine Erfüllungsübernahme. Hierbei ist zu prüfen, ob eine Übertragung der Daten der Kundinnen und Kunden vom Veräußerer auf den Erwerber die Interessen der Kundinnen und Kunden entgegenstehen (Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO).

Bei bereits beendeten vertraglichen Beziehungen (Altdaten) kommt allenfalls eine Übermittlung zur Erfüllung der gesetzlichen Aufbewahrungsfristen in Betracht. Hierfür ist der Abschluss eines Auftragsverarbeitungsvertrages nach Art. 28 Abs. 3 DS-GVO zwischen Veräußerer und Erwerber notwendig. Der Erwerber muss diese Daten zwingend von den Daten der Kundinnen und Kunden mit laufenden vertraglichen Beziehungen trennen. Alternativ kann der Veräußerer die Daten selbst bis zum Ablauf der gesetzlichen Aufbewahrungsfristen speichern oder ein anderes Dienstleistungsunternehmen mittels Auftragsverarbeitungsvertrag damit beauftragen. Der Erwerber darf diese Daten zu anderen Zwecken nur mit einer wirksamen Einwilligung der Kundinnen und Kunden nutzen.
Ist die Übermittlung im Rahmen eines Verkaufs der Daten der Kundinnen und Kunden das einzige „Asset“ (Verkauf der Datenbanken), so ergeben sich andere Erwägungen. Regelmäßig ist dies nur mit vorheriger Einwilligung der betroffenen Kundinnen und Kunden möglich, insbesondere dann, wenn die Datenbanken zur Nutzung von Werbung für Geschäftstätigkeiten eingesetzt werden sollen, die keinen Bezug zu dem ursprünglichen Unternehmen aufweist.
In dem jetzigen Beschluss wurde diese Auffassung zugunsten von Kleinstunternehmen (weniger als zehn Beschäftigte) und Kleinunternehmen (weniger als 50 Beschäftigte und Jahresumsatz von max. 10 Millionen Euro) aufgeweicht und hier die anfänglich aufgeführte Widerspruchslösung für möglich erklärt.
Tiefergehende ausführliche Ausführungen, auch zur Übermittlung von Bankdaten, besonderen Kategorien personenbezogener Daten, Beschäftigtendaten und die werbliche Nutzung finden sich in dem Beschluss. Der vollständige Beschluss ist auf der Webseite der Datenschutzkonferenz unter https://www.datenschutzkonferenz-online.de/media/dskb/2024-09-11_Beschluss%20DSK_%20Asset_Deals.pdf abrufbar.

1.13 Mieterselbstauskunft

Mieterselbstauskünfte sind ein immerwährender Anlass für Beschwerden beim TLfDI. Der potenzielle neue Vermieter kann nicht zu jedem Zeitpunkt alles abfragen. Zu diesem Thema gibt es eine neue Orientierungshilfe der DSK.

Mieterselbstauskünfte stellen einen wichtigen Baustein im Rahmen eines Vermietungsprozesses dar. Aufgrund des vielerorts sehr angespannten Wohnungsmarktes sind die Mieter oftmals darauf angewiesen, dass Vermieter ihre Vormachtstellung nicht nutzen und datenschutzrechtliche faire Auskünfte verlangen. Dennoch gehen beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) viele Beschwerden zu dieser Thematik ein.
Hauptkritikpunkt ist die Frage, zu welchem Zeitpunkt welche Fragen gestellt werden dürfen. Die Konferenz der deutschen Datenschutzaufsichtsbehörden der Länder und des Bundes (DSK) hat eine Orientierungshilfe zur Einholung von Selbstauskünften bei Mietinteressentinnen (Abrufbar unter: https://www.datenschutzkonferenz-online.de/media/oh/20180207_oh_mietauskuenfte.pdf) herausgegeben, bei der drei Zeitpunkte der zulässigen Datenverarbeitung definiert werden. So gelten zum Zeitpunkt der Besichtigung (Zeitpunkt A), zum Zeitpunkt der Erklärung des Mietinteressenten die Wohnung anmieten zu wollen (Zeitpunkt B), sowie zum Zeitpunkt, zu dem sich ein Vermieter für einen Mietinteressenten entschieden hat (Zeitpunkt C), unterschiedliche Voraussetzungen für die Datenverarbeitung.
Quelle zahlreicher Beschwerden ist die Bitte einiger Vermieter, die Mieterselbstauskunft vor dem Besichtigungstermin zu übermitteln. Hier ist ganz klar festzuhalten, dies ist datenschutzrechtlich unzulässig. Die Zulässigkeit der Erhebung personenbezogener Daten der Mietinteressenten richtet sich vor/während des Besichtigungstermins regelmäßig nach Art. 6 Abs. 1 Buchstabe f) der Datenschutz-Grundverordnung (DS-GVO). Streben Mietinteressenten zunächst nur eine Besichtigung der Räumlichkeiten an, so ist es in aller Regel nicht erforderlich, Angaben zu den wirtschaftlichen Verhältnissen des Mietinteressenten zu erfragen. Erfragt werden dürfen Angaben zur Identifikation wie Name, Vorname und Anschrift, sowie Angaben aus dem Wohnungsberechtigungsschein, soweit die künftige Wohnung im Rahmen eines Programms zur sozialen Wohnraumförderung errichtet wurde (nach § 27 Abs. 1 Wohnraumförderungsgesetz). Wichtig: Das Anfertigen einer Personalausweiskopie ist nicht erforderlich und damit unzulässig.
Erklärt der Mietinteressent nun, die Wohnung anmieten zu wollen, ist der Vermieter berechtigt, weitere Angaben im Rahmen einer Mieterselbstauskunft zu erfragen. Auch hier werden oftmals unzulässige Fragen gestellt und zu viele Daten erfasst.

Zunächst gibt es bereits Probleme bei der Beantwortung der Frage, auf welcher datenschutzrechtlichen Rechtsgrundlage die Mieterselbstauskunft fußt. Viele Vermieter legen den Mietinteressenten eine Einwilligung zur Datenverarbeitung entsprechend Art. 6 Abs. 1 Buchstabe a) DS-GVO vor. Voraussetzung für eine Einwilligung ist, dass sie freiwillig abgegeben wird. Damit eine Einwilligung freiwillig ist, muss der Betroffene eine echte Wahl haben. Es gilt das sogenannte „Kopplungsverbot". So darf ein Vertragsabschluss nicht von der Einwilligung zur Verarbeitung weiterer personenbezogener Daten abhängig gemacht werden, die für die Durchführung des Geschäftes nicht nötig sind.
Spätestens nach der Erklärung der Mietinteressenten, eine konkrete Wohnung anmieten zu wollen, entsteht ein vorvertragliches Schuldverhältnis zu den künftigen Vermietern, sodass dann Art. 6 Abs. 1 Buchstabe b) DS-GVO maßgebend ist. Im Rahmen der Mieterselbstauskünfte werden auch zu diesem Zeitpunkt immer wieder unzulässige Daten erfragt.
So sind Angaben zur Religion, Rasse, Staatsangehörigkeit, Zugehörigkeit zu Vereinen oder gar die Frage nach dem Kinderwunsch grundsätzlich unzulässig, da sie gegen das Allgemeine Diskriminierungsverbot nach § 19 Abs. 1 des Allgemeinen Gleichbehandlungsgesetzes (AGG) verstoßen und zudem die Bonität des Mietinteressenten nicht betreffen. Nach § 19 Abs. 3 AGG ist die Frage bezüglich der Rasse, der ethnischen Herkunft und der Religion bei der Vermietung von Wohnraum ausnahmsweise zulässig, wenn dies im Hinblick auf die Schaffung und Erhaltung sozial stabiler Bewohnerstrukturen und ausgewogener Siedlungsstrukturen sowie ausgeglichener wirtschaftlicher, sozialer und kultureller Verhältnisse notwendig ist. Zwingende Voraussetzung hierfür ist, dass zunächst ein schlüssiges wohnungspolitisches Konzept vorliegt.
Fragen zum Familienstand, Geburtsdatum und sogar Beruf von miteinziehenden Personen sind nicht erlaubt. Aus Bonitätsgründen dürfen solche Angaben zu Beruf und Einkommen nur erfragt werden, wenn die miteinziehende Person ebenfalls Vertragspartner wird. Dies ist üblicherweise bei Kindern nicht der Fall. Auch Ehepartner werden nicht zwangsläufig Mitmieter. Um einer Überbelegung des Wohnraumes vorzubeugen reicht es, die Namen und Geburtsjahrgänge der miteinziehenden Personen zu erfragen.

Auch die Frage, ob der Mietinteressent Raucher ist, ist unzulässig, da es sich um eine Frage handelt, die in die Privatsphäre der Interessenten eingreift.
Angaben zum aktuellen Arbeitgeber dürfen erfragt werden, jedoch darf dieser nicht durch den Vermieter kontaktiert werden. Da die heutige Gesellschaft eine mobile Gesellschaft mit häufigeren Berufswechseln ist, besteht für den Vermieter kein größeres Bonitätsrisiko, wenn der Mietinteressent nur ein befristetes Arbeitsverhältnis hat oder sich noch in der Probezeit befindet. Daher dürfen diese Daten nicht erfragt werden.
Ob in begründeten Fällen ein Fragerecht nach abgegebenen Vermögensauskünften (eidesstattliche Versicherung) besteht, hängt davon ab, nach welchem Zeitraum (in der Regel zwei Jahre) gefragt wird. Bei der Abgabe einer Versicherung an Eides statt im Rahmen einer Vermögensauskunft (§ 802c Abs. 3 der Zivilprozessordnung) sind Mietzinsansprüche der Vermieter nicht in gleicher Weise gefährdet wie bei Insolvenzerfahren, die den Mietinteressenten betreffen. Fragen darüber, ob über das Vermögen des Mietinteressenten eine Verbraucherinsolvenz eröffnet und noch nicht abgeschlossen ist, sind zulässig.
Überraschend für alle Vermieter: Nachweise zu den Einkommensverhältnissen, die der Mietinteressent angibt, dürfen erst erfragt werden, wenn sich der Vermieter für einen Mietinteressenten entschieden hat (Zeitpunkt C). Zuvor durfte zwar nach den Einkommensverhältnissen gefragt, jedoch keine Nachweise angefordert werden.
Häufige Missverständnisse gibt es auch rund um Bonitätsauskünfte. Auch diese dürfen erst jetzt (Zeitpunkt C) abgefragt werden. Zudem gilt es zu berücksichtigen: Liegen bereits ausreichende Informationen über die Bonität der Mietinteressenten vor, zum Beispiel durch Nachweise über die Einkommensverhältnisse wie Gehaltszettel, ist eine Abfrage bei Auskunfteien durch Vermieter nicht zulässig. Das Interesse des Vermieters, einen finanziell stabilen Mieter zu finden, wird ausreichend gewahrt, wenn der Mietinteressent Gehaltsnachweise oder Bonitätsauskünfte vorlegt.
Auch ist wichtig zu beachten, dass der Mietinteressent nicht in eine Datenverarbeitung durch die Schufa (zur Abfrage von Bonitätsauskünften) nach Art. 6 Abs. 1 Buchstabe a) DS-GVO einwilligen kann, denn auch diese Einwilligung ist nicht freiwillig, da sie vom Abschluss des Mietvertrages abhängig gemacht wird (Kopplungsverbot).
Nicht von Vermietern angefordert werden dürfen „Selbstauskünfte“

im Sinne des Art. 15 DS-GVO, die betroffene Personen bei Auskunfteien über sich selbst einholen können. Denn diese enthalten häufig wesentlich mehr Angaben über die wirtschaftlichen Verhältnisse des Mietinteressenten, als für eine Beurteilung der Bonität im Rahmen des Mietverhältnisses erforderlich sind.
Hat sich der Vermieter für einen Erstplatzierten entschieden (Zeitpunkt C) sind Fragen nach erheblichen Pflichtverletzungen aus dem vorherigen Mietverhältnis, die eine Kündigung rechtfertigen, begrenzt zulässig, wenn die Pflichtverletzung erheblich ist. Diese Pflichtverletzungen sind im Rahmen des angestrebten Mietverhältnisses jedenfalls dann erheblich, wenn sie auch noch in Zukunft zu erwarten sind. Die Kündigung muss entweder rechtskräftig oder die Pflichtverletzung in tatsächlicher Hinsicht unbestritten sein und auch aus Sicht der Mietinteressenten eine Kündigung in rechtlicher Hinsicht rechtfertigen. Fragen nach den Kontaktinformationen aktueller oder früherer Vermieter der Mietinteressenten (zum Beispiel Name, Anschrift, Telefonnummer, E-Mail-Adresse) sind unzulässig, denn solche Angaben sind für die Entscheidung über die Begründung eines Mietverhältnisses nicht erforderlich. Eine Kontaktaufnahme zu vorherigen Vermietern in Vorbereitung des Abschlusses eines Mietverhältnisses ist regelmäßig nicht erforderlich und daher unzulässig. Die Frage, warum ein Mietinteressent umziehen möchte, ist ebenfalls nicht relevant für die Eingehung eines neuen Mietverhältnisses.
Auch stellt der TLfDI fest, dass die Löschung von Daten der Mietinteressenten allzu oft nicht korrekt (entsprechend Art. 17 DS-GVO) ausgeführt wird. Daten der Mietinteressenten, mit denen kein Vertrag abgeschlossen wird, sind zu löschen, wenn der Zweck, zu dem sie erhoben wurden, weggefallen ist. In den Fällen, in denen Mietinteressenten Ansprüche auf Beseitigung einer Benachteiligung nach § 21 AGG verlangen können, müssen die Daten regelmäßig spätestens nach sechs Monaten gelöscht werden, soweit keine weitere Geltendmachung von Ansprüchen infrage kommt. Alle anderen Daten sind unverzüglich nach Mietvertragsschluss mit einem Mietinteressenten zu löschen.
Auch die Daten aus dem Vermietungsprozess, die für die Mietvertragsdurchführung nicht zwingend erforderlich sind, sind unverzüglich zu löschen (beispielsweise Einkommensnachweise).
Abschließend ist auf die Orientierungshilfe der DSK (Link siehe oben) zu verweisen, der am Ende ein Musterformular angefügt ist.

1.14 Zwei Datenschutzbeauftragte sind einer zu viel

Das Datenschutzrecht räumt zwar einige Flexibilität bei der Bestellung von Datenschutzbeauftragten ein. Aus der Rechtsstellung und den Aufgaben ergibt sich aber, dass grundsätzlich nur eine Person zum Datenschutzbeauftragten berufen werden kann. Das Amt lässt sich nur aufteilen, wenn innerhalb der Behörde oder des Unternehmens eine eindeutige Abgrenzung der Zuständigkeiten möglich ist. In diesem Fall sind die Kontaktdaten der jeweiligen Datenschutzbeauftragten zu veröffentlichen und dem TLfDI mitzuteilen.

In der Beratungspraxis des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) stellte sich die Frage, ob ein Verantwortlicher mehrere Datenschutzbeauftragte benennen kann, die sich das Amt teilen und sich bei der Aufgabenwahrnehmung wechselseitig vertreten.
Das Datenschutzrecht enthält verbindliche Regelungen zur Bestellung behördlicher und betrieblicher Datenschutzbeauftragter (Art. 37 Datenschutz-Grundverordnung in Verbindung mit § 5 Bundesdatenschutzgesetz). Dabei wird den Verantwortlichen und Auftragsverarbeitern zwar einige Flexibilität bei der Bestellung eingeräumt. So ist die Bestellung eines Konzerndatenschutzbeauftragten oder eines gemeinsamen Datenschutzbeauftragten für mehrere öffentliche Stellen ebenso möglich wie die Beauftragung externer Personen. Auch kann der interne Datenschutzbeauftragte seinen Aufgaben in Voll- oder Teilzeit nachgehen oder in großen Organisationseinheiten mit Hilfe eines Teams tätig werden. Von mehreren Datenschutzbeauftragten ist dabei aber nicht die Rede. Aus der Rechtsstellung des Datenschutzbeauftragten als Ansprechpartner der Behörden- oder Geschäftsleitung, der in Wahrnehmung der ihm übertragenen Überwachungs- und Beratungsaufgaben weisungsfrei ist, ergibt sich vielmehr, dass pro Verantwortungsbereich nur eine Person mit dem Amt des Datenschutzbeauftragten betraut werden kann. Weder die Datenschutz-Grundverordnung (DS-GVO) noch das Bundesdatenschutzgesetz kennen die Funktion eines Stellvertreters mit gleichen Rechten und Pflichten. Wenn ein Stellvertreter benannt wird, tritt dieser nur bei längerfristiger, zum Beispiel krankheits-, urlaubs- oder elternzeitbedingter Abwesenheit des eigentlichen Datenschutzbeauftragten an dessen Stelle. Im Einzelfall kann er bei einem auftretenden Interessenkonflikt auch einen Vor-

gang anstelle des Datenschutzbeauftragten übernehmen (VG Stuttgart, Beschluss vom 29.3.2021 – 11 K 484/21 RN 54). Bei der Benennung mehrerer Datenschutzbeauftragter bestünde hingegen die Gefahr, dass die Stellenleitung auswählt, wen sie wann in auftauchende Fragen des Datenschutzes einbindet, was dem umfassend zu verstehenden Benachteiligungsverbot widerspricht (Art. 38 Abs. 3 Satz 2 DS-GVO). Außerdem hätten mehr Personen als erforderlich einen uneingeschränkten Zugang zu Daten und Datenverarbeitungen.
Das Amt des Datenschutzbeauftragten lässt sich nur aufteilen, wenn innerhalb einer Behörde oder eines Unternehmens eindeutige Abgrenzungen der Zuständigkeiten möglich und sinnvoll sind. Daher wird die Berufung eines ausschließlich für den Mitarbeiterdatenschutz zuständigen Datenschutzbeauftragten regelmäßig an dem Umstand scheitern, dass die Aufgabe nur mit einem Gesamtüberblick über die Tätigkeit des Verantwortlichen effektiv wahrgenommen werden kann. Werden für abgegrenzte Bereiche unterschiedliche Datenschutzbeauftragte bestellt, darf im Interesse der Vertraulichkeit der Kommunikation auch keine gemeinsame Postanschrift beziehungsweise E-Mail-Adresse genutzt oder ein einheitliches Kontaktformular bereitgestellt werden. Die jeweiligen Kontaktdaten sind mit Benennung der Aufgabenbereiche in die Datenschutzinformationen aufzunehmen (Art. 13, 14 DS-GVO), in allgemein zugänglicher Form (zum Beispiel im Intra- und Internet) zu veröffentlichen und dem TLfDI vorzugsweise über das DSB-Meldeportal (https://tld.dsb-meldung.de) mitzuteilen (Art. 37 Abs. 7 DS-GVO).

1.15 Anspruch auf eine unentgeltliche Kopie schriftlicher Prüfungsarbeiten

Das Auskunftsrecht nach Art. 15 DS-GVO verleiht Prüflingen einen Anspruch auf Überlassung einer unentgeltlichen Kopie der von ihnen angefertigten Prüfungsarbeiten samt Korrekturbemerkungen und Prüfgutachten. Die Kopie ist unabhängig von der Möglichkeit zur Klausureinsicht bereitzustellen und bei einem elektronisch gestellten Antrag in einem gängigen Dateiformat (PDF, Word et cetera) zu übermitteln.

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichten wiederholt Anfragen und Be-

schwerden von Absolventen, Studierenden und Schülern, die von Prüfungsämtern und Bildungseinrichtungen mit Verweis auf den Auskunftsanspruch nach Art. 15 Datenschutz-Grundverordnung (DS-GVO) die Zurverfügungstellung der von ihnen angefertigten Prüfungsarbeiten verlangten. Diese bezogen sich sowohl auf Abiturprüfungen als auch auf die „Besondere Leistungsfeststellung“ (BLF) oder aber auch auf Studienabschlussprüfungen.

Als eine Form der Auskunftserteilung legt Art. 15 Abs. 3 DS-GVO fest, dass Verantwortliche die personenbezogenen Daten, die Gegenstand der Verarbeitung sind, den betroffenen Personen in Form einer Kopie zur Verfügung stellen müssen (vergleiche EuGH, Urteil vom 4. Mai 2023 – C-487/21). Der Begriff „Kopie“ bezieht sich zwar nicht auf ein Dokument als solches, sondern auf die personenbezogenen Daten, die es enthält und die vollständig sein müssen. Die „personenbezogenen Daten“ umfassen aber Informationen sowohl objektiver als auch subjektiver Natur, das heißt nicht nur überprüfbare Merkmale oder Aussagen der betroffenen Person, sondern auch Einschätzungen und Urteile über die in Rede stehende Person, so dass auch ein Dokument vollständig zu übermitteln ist, wenn es ausschließlich aus personenbezogen Daten besteht.

Die von einem Prüfling angefertigte Prüfungsarbeit erfüllt diese Voraussetzungen, da sie insgesamt – das heißt letztlich Wort für Wort – Informationen über die Leistung des Prüflings enthält. Neben ihrem Inhalt sind die Informationen auch aufgrund ihres Zwecks und ihrer Auswirkungen mit der in Rede stehenden Person verknüpft (EuGH, Urteil vom 20. Juli 2017 – C-434/16). Sie dienen der Beurteilung derselben durch den Prüfer oder das Prüfungsamt und haben, jedenfalls in Form von Abschluss- und Examensklausuren, Einfluss auf die Versetzung oder die beruflichen Möglichkeiten des Kandidaten. Macht der Prüfling sein Recht auf Datenkopie geltend, muss der Prüfer oder das Prüfungsamt daher eine vollständige Kopie der Prüfungsarbeit zur Verfügung stellen (BVerwG, Urteil vom 30. November 2022 – 6 C 10.21). Unabhängig von der Option der prüfungsrechtlichen Einsichtnahme ist die Kopie unentgeltlich bereitzustellen und, sofern sie elektronisch beantragt wurde, in einem gängigen Dateiformat (PDF, Word et cetera) zu übermitteln, auch wenn die Prüfungsunterlagen in Papierform aufbewahrt werden (OVG NRW, Urteil vom 8. Juni 2021 – 16 A 1582/20).

Die vom Prüfer in den Arbeiten angebrachten Korrekturbemerkungen stehen dem Anspruch des Prüflings auf Erhalt einer Kopie der von ihm

angefertigten Prüfungsarbeit nicht entgegen. Sie stellen zwar zugleich Informationen über den Prüfer dar. Mit der Überlassung einer Kopie der korrigierten Prüfungsarbeit ist aber keine Beeinträchtigung der Rechte des Prüfers nach Art. 15 Abs. 4 DS-GVO verbunden. Denn der Prüfer erstellt seine Bewertung generell mit der Maßgabe, dass diese dem Prüfling auf dessen Antrag hin zugänglich gemacht werden kann. Im Gegensatz zu den Prüfungsarbeiten, die mitsamt der dazugehörigen Prüfergutachten vollumfänglich Informationen über den Prüfling enthalten, erstreckt sich der Anspruch auf Auskunft und Kopie grundsätzlich nicht auf die Zurverfügungstellung der Aufgabentexte und Prüfungsfragen. Etwas anderes gilt für die bei elektronischen Prüfungen generierten Protokolldateien, wenn diese unerlässlich sind, um die Verständlichkeit der verarbeiteten Daten zu gewährleisten und dem Prüfling die wirksame Ausübung der ihm durch die Datenschutz-Grundverordnung verliehenen Rechte (Art. 16 bis 19 DS-GVO) zu ermöglichen.
Der TLfDI möchte an dieser Stelle klarstellen, dass, auch wenn die Entscheidung des BVerwG 6 C 10.21 sich mit einer berufsbezogenen Prüfung auseinandergesetzt hat, die Voraussetzungen des Auskunftsanspruches nach Art. 15 DS-GVO selbstverständlich auch für Abiturprüfungen, die „Besondere Leistungsfeststellung (BLF)“ an Gymnasien in Thüringen oder für andere Schulabschlussprüfungen gelten und Anträgen auf Auskunft und auf eine Kopie der Daten daher stattzugeben ist.

1.16 Aufbewahrung von Patientenakten nach Tod des Arztes

Die Erben eines Arztes sind für die Patientenunterlagen und die darin enthaltenen personenbezogenen Daten i. S. d. Art. 4 Nr. 7 DS-GVO verantwortlich und daher auch grundsätzlich verpflichtet, ehemaligen Patienten die Möglichkeit zur Einsichtnahme und Kopie der Patientenakte zu ermöglichen. Um allerdings auch für die Dauer der Aufbewahrungsfrist einen datenschutzkonformen Umgang mit den sensiblen Patientenunterlagen zu gewährlisten, sollte der Gesetzgeber eine datenschutzgerechte Lösung finden.

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichte die Anfrage eines Mannes, der sich als Alleinerbe seiner verstorbenen Ehefrau, die als niedergelassene

Ärztin tätig war, mit dem Auskunftsanspruch eines ehemaligen Patienten nach Art. 15 Datenschutz-Grundverordnung (DS-GVO) konfrontiert sah. Er wollte wissen, ob er verpflichtet sei, diesen zu erfüllen.

Der TLfDI teilte dem Fragesteller mit, dass er für die Patientenunterlagen und die darin enthaltenen personenbezogenen Daten im Sinne des Art. 4 Nr. 7 DS-GVO verantwortlich ist, wenn er die Patientenakten lagert. Die Verantwortlichkeit hängt nicht davon ab, ob der Betreffende die Daten selbst erhoben oder verarbeitet hat, sondern ob er die rechtliche oder tatsächliche Einflussmöglichkeit auf die Datenverarbeitung besitzt. Die Verfügungsbefugnis folgt dabei aus dem Umstand, dass die Arztpraxis mit allen Rechten und Pflichten auf den Erben übergeht (§ 1922 BGB). Folglich ist dieser auch grundsätzlich verpflichtet, auf Antrag eines ehemaligen Patienten die Möglichkeit zur Einsichtnahme und Kopie der Patientenakte zu ermöglichen (vergleiche EuGH, Urteil vom 26. Oktober 2023, C-307/22).

Bei den Patientendaten handelt es sich allerdings um besondere Kategorien von personenbezogenen Daten, die nur unter den strengen Voraussetzungen des Art. 9 Abs. 2 Buchstabe h) DS-GVO verarbeitet werden dürfen. Danach bedarf es zum einen einer Rechtsgrundlage oder eines Vertrags mit einem Angehörigen eines Gesundheitsberufs. Zum anderen dürfen die Daten nach Art. 9 Abs. 3 DS-GVO auch nur von Fachpersonal oder unter seiner Verantwortung von Personen verarbeitet werden, die der ärztlichen Schweigepflicht unterliegen. Dies ist bei einem Erben, der nicht selbst in einem derartigen Beruf arbeitet, fraglich.

Nach § 630g BGB hat der Patient ein Recht auf Einsicht in die ihn betreffende Akte. Der Anspruch folgt aus dem zwischen Arzt und Patienten geschlossenen Behandlungsvertrag und wird durch das verfassungsrechtlich garantierte Persönlichkeitsinteresse des Patienten und den unionsrechtlichen Auskunftsanspruch nach Art. 15 DS-GVO überlagert. Wegen des fortbestehenden Patientengeheimnisses dürfen die Patientenunterlagen aber nur mit Einwilligung weitergegeben werden. Man kann zwar annehmen, dass die Einwilligung in dem Antrag nach Art. 15 DS-GVO enthalten ist, so dass eine Kopie der Patientenakte herausgeben werden kann, sofern keine Zweifel an der Identität des Antragstellers bestehen. Es bleibt allerdings das Problem, dass Patientenunterlagen nach den Vorschriften der Schweigepflicht und des Datenschutzes nur von Berechtigten verwahrt werden dürfen. Hierfür

sieht § 10 Abs. 4 der Musterberufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte (MBO-Ä) vor, dass die Patientenakten einem Arzt im Rahmen eines Verwahrungsvertrags in Obhut gegeben werden. Kann der Arzt seiner gesetzlichen Verpflichtung nicht nachkommen, etwa, weil er in Konkurs, dauerhaft erkrankt oder wie im vorliegenden Fall verstorben ist, stellt sich die Frage, wer für die Patientenunterlagen zuständig ist.
Einige Länder verpflichten die Landesärztekammer, die Patientenunterlagen zu verwahren und zu verwalten, wenn die Aufgabe nicht durch den Rechtsnachfolger gesichert werden kann (vergleiche § 4 Abs. 1 S. 3 Heilberufe-Kammergesetz Baden-Württemberg; § 22 Abs. 2 S. 2 Heilberufegesetz Rheinland-Pfalz).
Die Erben des Arztes unterliegen zwar der Schweigepflicht (§ 203 Abs. 4 Satz 2 Nr. 3 Strafgesetzbuch) und treten in die dem Arzt obliegende Pflicht zur Aufbewahrung der Patientenakten ein (§ 630f Abs. 3 BGB). Es ist aber fraglich, ob sie die Aufbewahrung, Einsichtnahme und Löschung der Patientenunterlagen datenschutzkonform gewährleisten können. Dies gilt auch für eine angemessene Sicherheit elektronischer Patientenakten. Für den Fall, dass sich kein Praxisnachfolger findet und der Arzt seiner Aufbewahrungspflicht nicht nachkommen kann, bedarf es daher einer Regelung, die bisher im Landesrecht leider fehlt. Der TLfDI hat sich mit diesem Anliegen bereits an das zuständige Ressort gewandt.

2. Fälle öffentlicher Bereich

Rathaus Architektur Gebäude - Pixabay

2.1 Zu viele personenbezogene Daten in einem Einstellungsbescheid der Staatsanwaltschaft

Verarbeitet eine Staatsanwaltschaft in Thüringen im Rahmen eines Strafverfahrens personenbezogene Daten, greift gemäß § 500 Abs. 1 Strafprozessordnung (StPO) nicht das Thüringer Datenschutzgesetz, sondern das Bundesdatenschutzgesetz (BDSG). Erlässt sie einen Einstellungsbescheid, gilt der sich aus § 47 BDSG ergebene Datenminimierungsgrundsatz. Die Angabe aller Geschädigten mit ihren Vor- und Nachnamen, ihrem jeweiligen Geburtsdatum, ihrer Adresse, der Höhe ihres Schadens sowie der Tatzeit in einem Einstellungsbescheid, der an alle Geschädigten versandt wurde, entsprach diesem Grundsatz nicht und führte zu einer Beanstandung seitens des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit.

Eine Beschwerdeführerin wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und trug vor, dass sie von der Staatsanwaltschaft einen Einstellungsbescheid zu einer Strafsache erhielt, in der sie als Geschädigte betroffen war. Diese Tatsache an sich stellt noch keinen datenschutzrechtlichen

Verstoß dar. Da aber der Einstellungsbescheid neben den mitzuteilenden Gründen für die Einstellung eine Tabelle enthielt, in der alle Geschädigten mit ihren Vor- und Nachnamen, ihrem jeweiligen Geburtsdatum, ihrer Adresse, der Höhe ihres Schadens sowie der Tatzeit aufgeführt waren, brachte dies den TLfDI ins Spiel. Der Einstellungsbescheid ging an die Beschwerdeführerin und an alle weiteren Geschädigten. Folglich konnte jeder wissen, welche Person – inklusive des Geburtsdatums und der kompletten Wohnanschrift – welchen Schaden erlitten hatte. Da der materielle Schaden bei der Beschwerdeführerin sehr groß war, hatte dies unter anderem zu Folge, dass sich diese Tatsache schnell in ihrem Wohngebiet herumsprach und sie diesbezüglich auch angesprochen wurde.
Der TLfDI nahm sich der Sache an, forderte die betreffende Staatsanwaltschaft zu einer Stellungnahme auf und würdigte den Sachverhalt danach aus datenschutzrechtlicher Sicht.
Gemäß § 171 Strafprozessordnung (StPO) hat die Staatsanwaltschaft den Antragsteller (hier die Beschwerdeführerin) unter Angabe der Gründe zu bescheiden, wenn sie die Einstellung des Verfahrens verfügt. Dabei dürfen personenbezogene Daten verarbeitet werden. Gemäß § 47 Nr. 3 Bundesdatenschutzgesetz (BDSG) müssen jedoch personenbezogene Daten dem Verarbeitungszweck entsprechen, für das Erreichen des Verarbeitungszwecks erforderlich sein und ihre Verarbeitung nicht außer Verhältnis zu diesem Zweck stehen. Aus der gebotenen Erforderlichkeit der Datenverarbeitung („kein milderes, gleich wirksames Mittel“) ergibt sich der Grundsatz der Datenminimierung (Gola/Heckmann/Braun, 3. Auflage 2022, BDSG § 47 Randnummer 17). Der in § 47 Nr. 3 BDSG festgelegte Grundsatz bezieht sich auf jede Form der Verarbeitung im Anwendungsbereich des § 45 BDSG. Das BDSG war – obwohl es sich um eine Thüringer Staatsanwaltschaft handelte – in diesem Fall aufgrund von § 500 Abs. 1 StPO anwendbar.
Die verantwortliche Stelle muss sich bei der Verarbeitung personenbezogener Daten auf den Umfang beschränken, den sie für ihre Zwecke tatsächlich benötigt. Dabei hat sie auch zu prüfen, ob nicht eine Reduzierung des Personenbezugs durch eine (teilweise) Anonymisierung möglich ist oder ob gegebenenfalls eine Pseudonymisierung in Betracht kommen kann (Kühling/Buchner/Schwichtenberg, 4. Auflage 2024, BDSG § 47 Randnummer 2c).

Der Grundsatz der Datenminimierung obliegt der verantwortlichen öffentlichen Stelle, in diesem Fall der Staatsanwaltschaft, da sie die Einstellungsverfügung verfasst und übermittelt hat. Daher musste seitens der Geschädigten kein besonderes Schutzinteresse betreffend ihrer personenbezogenen Daten vorab bekundet werden.
Gemäß § 171 StPO hat die Staatsanwaltschaft den Antragsteller unter Angabe der Gründe zu bescheiden, wenn sie die Einstellung des Verfahrens verfügt. Gemäß Nummer 89 Abs. 2 der Richtlinien für das Strafverfahren und das Bußgeldverfahren (RiStBV) dürfen die Einstellungsgründe vereinfacht und gekürzt wiedergegeben werden. Eine lediglich formelhafte Angabe nichtssagender Redewendungen oder eine Wiederholung des Gesetzestextes ist nicht ausreichend. Inhaltlich muss in der Einstellungsmitteilung deutlich werden, ob es sich um eine völlige oder teilweise Einstellung handelt, ob sie auf tatsächlichen oder rechtlichen Gründen beruht und ob die Staatsanwaltschaft die Ermittlungen eingestellt oder keine Ermittlungen aufgenommen hat. (HK-GS/Kai Ambos, 5. Auflage 2022, StPO § 171 Randnummer 3). Die Erläuterung soll dabei knapp gefasst sein, die wahren Einstellungsgründe sollen aber präzise und für juristische Laien verständlich angeben werden (siehe Nummer 89 Abs. 2 und 4 RiStBV). Berücksichtigt werden muss jedoch, dass keine unnötigen Einblicke in die Privatsphäre des Beschuldigten oder etwaiger Zeugen stattfinden (KK-StPO/Moldenhauer, 9. Auflage 2023, StPO § 171 Randnummer 9).
Grenzen ergeben sich aus der Verhältnismäßigkeit des in der Mitteilung liegenden informationellen Eingriffs (MüKoStPO/Kölbel/Neßeler, 2. Auflage 2024, StPO § 171 Randnummer 8-8a). Der Mitteilungsinhalt muss zur Erreichung des mit ihm verfolgten Zwecks – die Einordnung und das Verständnis der Einstellungsgründe für den Antragsteller – geeignet, erforderlich und angemessen sein. Er muss aber in der Breite der Auskunft hinter dem Ausmaß einer Akteneinsicht (§§ 406e, 475 StPO) zurückbleiben (MüKoSt-PO/Kölbel/Neßeler, am angeführten Ort). Auch berechtigte Geheimhaltungsinteressen dritter Personen können unter Verhältnismäßigkeitsgesichtspunkten eine Kürzung etwaiger Passagen erforderlich machen. (MüKoStPO/Kölbel/Neßeler, am angeführten Ort).
Unter Berücksichtigung des Datenminimierungsgrundsatzes gemäß § 47 Nr. 3 BDSG wäre in dem vorliegenden Fall der Einstellungsbe-

scheid auch ohne die Angaben der gesamten personenbezogenen Daten (Vor- und Nachname, Geburtsdatum, Adresse und der Höhe des Schadens) in der Tabelle auf Seite 2 verständlich gewesen.
Die Beanstandung stellt das einzige Sanktionsinstrument des TLfDI in Umsetzung der JI-Richtlinie dar, um den Verstoß gegen die datenschutzrechtlichen Bestimmungen zu ahnden. Von dieser kann abgesehen werden gemäß § 7 Abs. 6 Satz 3 Thüringer Datenschutzgesetz (ThürDSG) insbesondere, wenn es sich um unerhebliche oder inzwischen beseitigte Mängel handelt.
Eine Beseitigung des Mangels war aufgrund der Versendung der Einstellungsbescheide nicht mehr möglich. Der Verstoß war aus Sicht des TLfDI auch nicht unerheblich. Aufgrund der Nennung sämtlicher Klardaten konnten mindestens die anderen Geschädigten, und möglicherweise auch weitere dritte Personen aus deren Umfeld, genaue Kenntnis des doch beträchtlichen Schadens der Beschwerdeführerin erhalten. Die Streubreite einer solchen Information konnte nicht mehr eingefangen werden und stellte eine erhebliche Beeinträchtigung des informationellen Selbstbestimmungsrechts dar. Das zeigte sich unter anderem darin, dass sie bereits auf der Straße in ihrem Wohnviertel auf ihren Fall und auf die hohe Geldsumme, die sie an die Täter verloren hatte, angesprochen wurde.
Aus diesen Gründen sprach der TLfDI gegenüber der Staatsanwaltschaft eine Beanstandung gemäß § 7 Abs. 6 Satz 1 ThürDSG in Verbindung mit § 500 Abs. 2 Nummer 2 StPO aus.
Die betreffende Staatsanwaltschaft nahm den Sachverhalt zum Anlass, ihre Staatsanwälte zu dieser Thematik zu sensibilisieren.

2.2 Mahnungen erlaubt – aber bitte an die richtige Adresse

Eine Staatsanwaltschaft in Thüringen versandte versehentlich ein Mahnschreiben aus einem gegen eine Privatperson geführten Strafvollstreckungsverfahren an die dienstliche Adresse des Arbeitgebers dieser Person. Dies stellte eine erhebliche Beeinträchtigung des Grundrechts auf informationelle Selbstbestimmung dar. Auch unter Beachtung seines Ermessenspielraumes konnte der TLfDI in diesem konkreten Fall nicht von einer Beanstandung absehen.

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichte im Berichtszeitraum die Eingabe eines Bürgers, welcher sich über eine Staatsanwaltschaft in Thüringen

beschwerte. Hintergrund dessen war die Übermittlung eines Mahnschreibens aus einem privaten Strafvollstreckungsverfahren an die dienstliche Adresse des Arbeitgebers des Beschwerdeführers, obwohl dessen private Anschrift der Staatsanwaltschaft durchaus bekannt war. Die Ermittlungen des TLfDI ergaben, dass die dienstliche Adresse des Arbeitgebers des Beschwerdeführers aus einem anderem Verfahren bei der Staatsanwaltschaft systemseitig gespeichert war. Durch die Neuregistrierung des sodann gegen den Beschwerdeführer geführten Strafvollstreckungsverfahrens wurde softwarebedingt die dienstliche Adresse des Arbeitgebers zur führenden Adresse im genannten Strafvollstreckungsverfahren gegen den Beschwerdeführer.
Nach eingehender datenschutzrechtlichen Prüfung gelangte der TLfDI in dieser Sache zu dem Entschluss, gegenüber der Staatsanwaltschaft eine Beanstandung gemäß § 7 Abs. 6 Satz 1 Thüringer Datenschutzgesetz (ThürDSG) in Verbindung mit § 500 Abs. 2 Nummer 2 Strafprozessordnung (StPO) auszusprechen. Die Übermittlung und Zugänglichmachung des Mahnschreibens der Staatsanwaltschaft an den Arbeitgeber des Beschwerdeführers stellte einen Verstoß gegen § 47 Nummer 4 Bundesdatenschutzgesetz (BDSG) dar.
Gemäß § 500 Abs. 1 StPO ist Teil 3 des BDSG entsprechend anzuwenden, soweit öffentliche Stellen der Länder im Anwendungsbereich dieses Gesetzes personenbezogene Daten verarbeiten. Bei der in Rede stehenden Staatsanwaltschaft handelte es sich um eine solche öffentliche Stelle des Landes Thüringen, die in den Anwendungsbereich der StPO fallen. Somit gilt in der hier dargestellten Fallkonstellation nicht das ThürDSG, sondern das BDSG.
Gemäß § 47 Nummer 4 BDSG müssen personenbezogene Daten unter anderem sachlich richtig sein. Der Grundsatz der Richtigkeit verlangt bei der Verarbeitung personenbezogener Daten auch eine zutreffende Unterscheidung nach der Kategorie der betroffenen Person („Verdächtige, Verurteilte, Straftäter, Opfer, Zeugen, Personen, die über einschlägige Informationen verfügen, oder Personen, die mit Verdächtigen oder verurteilten Straftätern in Kontakt oder in Verbindung stehen“), wie in § 72 BDSG präzisiert (so Gola/Heckmann, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Auflage 2022, § 47 Nummer 4 BDSG, Randnummer 22-24).
Die dienstliche Adresse des Arbeitgebers des Beschwerdeführers stammte hier aus einem anderen, früheren Ermittlungsverfahren. Die beanstandete Staatsanwaltschaft räumte auch ein, dass sie offensichtlich nicht bemerkt hatte, dass der Beschwerdeführer bereits mit seiner

Wohnanschrift bei der Staatsanwaltschaft erfasst war. Der TLfDI ging in diesem Falle von einem Büroversehen aus. Im Nachgang wurden sodann die dienstlichen Adressdaten aus dem sachfremden Ermittlungsverfahren in dem Strafvollstreckungsverfahren bei der Staatsanwaltschaft versehentlich genutzt. Damit war die Verarbeitung der dienstlichen Adresse für das Strafvollstreckungsverfahren, das gerade nicht im Rahmen einer dienstlichen Tätigkeit des Beschwerdeführers initiiert war, sachlich unrichtig und verstieß gegen § 47 Nr. 4 BDSG. Auch unter Beachtung und Ausübung des in § 7 Abs. 6 Satz 3 ThürDSG eingeräumten Ermessens konnte der TLfDI im vorliegenden Falle nicht von einer Beanstandung gegenüber der Staatsanwaltschaft absehen. Dies ist nur dann möglich, wenn es sich um unerhebliche oder inzwischen beseitigte Mängel handelt. Eine Beseitigung des Mangels war im vorliegenden Falle aufgrund der Versendung des Mahnschreibens an den Arbeitgeber nicht mehr möglich. Der Verstoß war auch nicht unerheblich. Dabei war insbesondere zu berücksichtigen, dass personenbezogene Daten aus einem Strafvollstreckungsverfahren an Dritte – hier dem Arbeitgeber – und dort mindestens der Poststelle beziehungsweise einer weiteren Person – preisgegeben wurden. Zudem erfolgte der Versand des in Rede stehenden Briefes an den Arbeitgeber des Beschwerdeführers weder mittels Postzustellungsurkunde noch mit etwaigen Zusätzen wie „persönlich/vertraulich“, was gegebenenfalls eine Offenlegung personenbezogener Daten an Dritte hätte verhindern können. Dadurch ist mindestens eine weitere Person im dienstlichen Umfeld des Beschwerdeführers in Kenntnis des gegen ihn privat geführten Strafvollstreckungsverfahrens gelangt. Zudem konnte eine weitere Streubreite dieser Informationen nicht mehr eingefangen werden, was eine erhebliche Beeinträchtigung des Grundrechts auf informationelle Selbstbestimmung nach sich zog. Die ausgesprochene Beanstandung im konkreten Fall stellte die einzige Sanktionsmaßnahme dar, die dem TLfDI gemäß § 7 Abs. 6 Satz 1 ThürDSG eingeräumt worden ist – obwohl Art. 47 der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 (kurz: Justiz/Inneres-Richtlinie – JI-Richtlinie – genannt) weitere und vor allem konkretere Sanktionsinstrumente für die Datenschutzaufsichtsbehörden vorsieht. Diese hat der Thüringer Gesetzgeber aber im Jahr 2018 und auch danach nicht in das ThürDSG übernommen.

2.3 Verfügung eines vorsitzenden Richters an den falschen Strafverteidiger

Die verfahrensleitende Verfügung eines Richters im Rahmen eines Strafverfahrens unterfällt der richterlichen Unabhängigkeit und ist nicht durch den TLfDI zu überprüfen, auch wenn sie einen Verstoß gegen datenschutzrechtliche Vorschriften beinhaltet. Die Entscheidungen des TLfDI haben keine Auswirkungen auf ein Strafverfahren oder eine Haftaussetzung. Noch immer sind in der Bundesrepublik Deutschland keine besonderen Stellen für die datenschutzrechtliche Aufsicht im Justizsystem geschaffen worden.

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichte eine Beschwerde über ein Thüringer Gericht. Dieses hatte in einem Strafverfahren einen Schriftsatz zur Stellungnahme an den vormaligen Pflichtverteidiger zugestellt. Der Beschwerdeführer hatte jedoch bereits zuvor einen Wahlverteidiger beauftragt, so dass der Schriftsatz letztendlich an den falschen Verteidiger zugestellt wurde. Im Rahmen der Anhörung teilte das Gericht dem TLfDI mit, der vorsitzende Richter habe unter Bezugnahme auf die Angaben im Rubrum eines Beschlusses des Gerichts der vorherigen Instanz die Übersendung von Unterlagen an den dort namentlich benannten (Pflicht-)Verteidiger des Beschwerdeführers angeordnet. Hierzu teilte das Gericht dem TLfDI den genauen Wortlaut der Verfügung mit. Die Unterlagen seien von der Geschäftsstelle an diese Kanzlei versandt worden. Zu diesem Zeitpunkt sei die Pflichtverteidigung bereits aufgehoben und der Wahlverteidiger bestellt gewesen. Dies habe sich wohl aus der Akte ergeben, sei dem vorsitzenden Richter aber nicht bewusst gewesen.
Der Beschwerdeführer monierte gegenüber dem TLfDI nicht nur den Datenschutzverstoß, sondern auch, dass durch die Fehlzustellung und den damit einhergehenden datenschutzrechtlichen Verstoß freiheitsentziehende Maßnahmen rechtswidrig vorgenommen worden seien, sodass das Gericht bis zu einer Klärung die Vollziehung auszusetzen habe. Zudem käme es nicht darauf an, was ein Richter verfüge. Vielmehr habe die Urkundsbeamtin der Geschäftsstelle den Fehler begangen. Diesem Vorbringen konnte der TLfDI nicht zustimmen.
Der TLfDI ist gemäß § 4 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) Aufsichtsbehörde nach Art. 41 der Richtlinie (EU) 2016/680 für die für die Verhütung, Ermittlung, Aufdeckung,

Verfolgung oder Ahndung von Straftaten zuständigen öffentlichen Stellen. Für die Gerichte ist der TLfDI nur datenschutzrechtliche Aufsichtsbehörde, soweit diese in Verwaltungsangelegenheiten tätig werden. Dies ergibt sich aus § 2 Abs. 9 Satz 2 ThürDSG.
Im vorliegenden Fall wurde das Gericht nicht in einer Verwaltungsangelegenheit tätig. Vielmehr war die Anordnung durch den vorsitzenden Richter getroffen worden. Sie war ganz konkret auf einen bestimmten Verteidiger in einem bestimmten Beschluss gerichtet. Es handelt sich dabei um eine verfahrensleitende Anordnung. Sie unterfällt der richterlichen Unabhängigkeit und ist seitens der Urkundsbeamtin lediglich auszuführen. Diese justizielle Tätigkeit unterliegt nicht der datenschutzrechtlichen Kontrolle des TLfDI.
Ferner war hier auf Folgendes hinzuweisen: Ermittlungen des TLfDI im Rahmen der Bearbeitung einer Beschwerde hemmen keine gerichtlichen Fristen und führen auch nicht zu Haftaussetzungen bis zur Sachverhaltsaufklärung.
Die Beschwerde war daher als unzulässig abzulehnen. Der Beschwerdeführer erhob daraufhin Klage gegen die Entscheidung des TLfDI. Das verwaltungsgerichtliche Verfahren dauerte bei Redaktionsschluss zu diesem Tätigkeitsbericht noch an.
Anzumerken ist noch, dass in der Bundesrepublik Deutschland bisher keine besonderen Stellen für die datenschutzrechtliche Aufsicht im Justizsystem geschaffen wurden (siehe Erwägungsgrund 20 zur Datenschutz-Grundverordnung). Es besteht daher keine anderweitige datenschutzrechtliche Aufsicht für die justizielle Tätigkeit. Die Schaffung dieser besonderen Stellen mahnten die Datenschutzbeauftragten der Länder und des Bundes bereits mehrfach an – bisher ohne Erfolg. Vollständiger effektiver Rechtschutz bleibt den Beschwerdeführern in diesen Fällen weiterhin verwehrt.

2.4 Beschwerde über einen Zweckverband wegen der Weitergabe von personenbezogenen Daten ohne Einwilligung

Zweckverbände für Trinkwasserversorgung und Abwasserbeseitigung dürfen keine offene Rechnung von Kunden an den Notar des zukünftigen Käufers des Eigenheims übermitteln. Dies stellt einen Verstoß gegen datenschutzrechtliche Bestimmungen dar, da es an einer Rechtsgrundlage für eine solche Datenübermittlung fehlt.

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichte im Berichtszeitraum eine Beschwerde, die Folgendes zum Gegenstand hatte: Die Beschwerdeführerin, Kundin eines Zweckverbandes für Trinkwasserversorgung und Abwasserbeseitigung, hatte eine Benachrichtigung von ihrem Immobilienverwalter erhalten, dass der Käufer und neue Eigentümer ihrer Immobilie den Zweckverband über eine Wieder-Öffnung des Wasseranschlusses auf dem besagten Grundstück kontaktiert habe. Grund dafür sei gewesen, dass der Zweckverband dem neuen Eigentümer über dessen Notar inklusive der Benennung der Gesamtforderung mitgeteilt habe, dass eine offene Rechnung der Beschwerdeführerin und Kundin als frühere Eigentümerin des Grundstücks vorliege.
Der TLfDI hörte daraufhin den Zweckverband für Trinkwasserversorgung und Abwasserbeseitigung an und stellte im Ergebnis fest, dass ein Verstoß gegen datenschutzrechtliche Bestimmungen vorlag, da es für die Übermittlung der offenen Rechnung der Beschwerdeführerin an den neuen Eigentümer keine Rechtsgrundlage gab.
Nach Art. 4 Nummer 2 Datenschutz-Grundverordnung (DS-GVO) wird der Ausdruck der Verarbeitung wie folgt definiert: Verarbeitung ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.
Art. 5 DS-GVO regelt die Grundsätze für die Verarbeitung personenbezogener Daten. Nach Art. 5 Abs. 1 Buchstabe a) DS-GVO müssen personenbezogene Daten auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“). Die Rechtmäßigkeit der Verarbeitung ergibt sich aus Art. 6 DS-GVO. Die Verarbeitung, worunter auch die Übermittlung von personenbezogenen Daten fällt, durch öffentliche Stellen ist rechtmäßig, wenn die betroffene Person ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben hat (Art. 6 Abs. 1 Satz 1 Buchstabe a) DS-GVO); die Verarbeitung zur Erfüllung einer

rechtlichen Verpflichtung erforderlich ist, der der Verantwortliche unterliegt (Art. 6 Abs. 1 Satz 1 Buchstabe c) DS-GVO) oder die Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde (Art. 6 Abs. 1 Satz 1 Buchstabe e) DS-GVO).
Die Übermittlung der offenen Rechnung der Beschwerdeführerin und Kundin des Zweckverbandes durch diesen an den Notar des Käufers stellte eine Verarbeitung im Sinne des Art. 4 Nr. 2 DS-GVO dar. Der TLfDI vermochte keine der oben genannten Voraussetzungen des Art. 6 Abs. 1 Buchstaben a), c) oder e) DS-GVO für die Übermittlung der offenen Rechnung an den Notar als erfüllt ansehen. Es lag keine Einwilligung seitens der Beschwerdeführerin und Kundin vor, ebenso gab es keine rechtliche Verpflichtung für die Übermittlung der offenen Rechnung an den Notar des Käufers. Auch war die Verarbeitung für die Wahrnehmung einer Aufgabe nicht erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Es war nicht erforderlich, dass der Zweckverband die offene Rechnung an den Notar übermittelt, da dieser die offene Rechnung nicht für die Erfüllung seiner Aufgaben – hier die Eigentumsübertagung des Grundstücks – benötigte.
Der TLfDI hatte aufgrund dessen zu entscheiden, welche Befugnisse er für den festgestellten Datenschutzverstoß ausübt. Nach Art. 58 Abs. 2 DS-GVO verfügt jede Aufsichtsbehörde über Abhilfebefugnisse, die es ihr gestatten einen Verantwortlichen oder einen Auftragsverarbeiter zu verwarnen, wenn er mit Verarbeitungsvorgängen gegen diese Verordnung verstoßen hat. Aus den oben genannten Gründen stellte der TLfDI fest, dass gegen die Vorschriften der DS-GVO verstoßen wurde, und er verwarnte den Zweckverband nach Art. 58 Abs. 2 Buchstabe b) DS-GVO für diesen Datenschutzverstoß. Im Rahmen seiner Ermessensausübung nach § 7 Abs. 1 Satz 5 Thüringer Datenschutzgesetz konnte der TLfDI im vorliegenden Fall nicht von einer Verwarnung absehen, da ein schwerwiegender Datenschutzverstoß vorlag, denn der Notar beziehungsweise der Käufer hätten aus dem oben genannten Grund nichts von der offenen Rechnung wissen müssen. Die Verwarnung war auch verhältnismäßig, denn sie war geeignet, um zukünftig einen solchen Verstoß zu vermeiden. Ein milderes Mittel, das die gleiche Wirkung erzielt hätte, sieht die DS-GVO nicht vor. Auch war die Verwarnung angemessen, da die Abwägung

der informationellen Selbstbestimmung höher zu gewichten war als das Handeln des Zweckverbandes. Zugleich forderte der TLfDI einen schriftlichen Nachweis vom Zweckverband dafür, dass der Notar des Käufers die offene Rechnung der Kundin gelöscht hat. Dieser Aufforderung des TLfDI kam der Zweckverband nach.

2.5 Verwarnung wegen der Veröffentlichung einer Schöffenwahlliste mit zu vielen personenbezogenen Daten im Amtsblatt

Auch im Rahmen der Veröffentlichung von Interessenten zur Wahl als Schöffen im Amtsblatt sind durch die öffentlichen Stellen die Vorgaben der DS-GVO zu beachten. Die Angabe und damit Veröffentlichung von Familienname, Vorname, Geburtsjahr, Wohnort einschließlich Postleitzahl sowie Beruf im Amtsblatt können aufgrund einer rechtlichen Verpflichtung nach Art. 6 Abs. 1 Satz 1 Buchstabe c) und Abs. 3 in Verbindung mit § 36 Abs. 3 Satz 1 Gerichtsverfassungsgesetz (GVG) datenschutzrechtlich zulässig sein. Die Veröffentlichung von personenbezogenen Daten, die über diese rechtliche Verpflichtung hinausgeht, bedarf datenschutzrechtlich ebenfalls einer Rechtsgrundlage.

Im Berichtszeitraum erreichte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) eine Beschwerde, in der es um die Offenlegung der vollständigen Anschrift und des Geburtsdatums einer Beschwerdeführerin als Interessentin zur Wahl als Schöffin im Amtsblatt einer Stadt in Thüringen ging. Die Beschwerdeführerin hatte sich im Rahmen der Schöffenwahl 2023 als Interessentin bei der Stadt angemeldet und das Interessenbekundungsformular ausgefüllt übermittelt. Daraufhin veröffentlichte die Stadt im Amtsblatt alle für die Vorschlagsliste gemeldeten Interessenten mit den vollständigen Angaben des Interessenbekundungsformulars und damit neben Namen und Vornamen, Geburtsdatum, Geburtsort und dem Beruf auch die vollständige Anschrift.
Der TLfDI gelangte nach Prüfung des zugrundeliegenden Sachverhalts zu dem Ergebnis, dass die Stadt durch die Veröffentlichung der vollständigen Anschrift und des Geburtsdatums der Beschwerdeführerin einen Verstoß gegen Art. 5 Abs. 1 Buchstabens a) und f) Datenschutz-Grundverordnung (DS-GVO) beging. Nach Art. 5 Abs. 1

Buchstabe a) DS-GVO müssen personenbezogene Daten auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden. Weiterhin müssen nach Art. 5 Abs. 1 Buchstabe f) DS-GVO personenbezogene Daten in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung. Mangels zusätzlicher Informationen für die Beschwerdeführerin nach Art. 13 DS-GVO über die Aufnahme ihrer genannten personenbezogenen Daten in die Vorschlagsliste für die Wahl als Schöffin lag auch ein Verstoß gegen das Transparenzgebot vor.
Gemäß § 36 Abs. 3 Satz 1 Gerichtsverfassungsgesetz (GVG) ist die Vorschlagsliste für Schöffen in der Gemeinde eine Woche lang zu jedermanns Einsicht aufzulegen. Die Vorschlagsliste muss gemäß § 36 Abs. 2 Satz 2 GVG Familienname, Vornamen, gegebenenfalls einen vom Familiennamen abweichenden Geburtsnamen, Geburtsjahr, Wohnort einschließlich Postleitzahl sowie Beruf der vorgeschlagenen Person enthalten; bei häufig vorkommenden Namen ist auch der Stadt- oder Ortsteil des Wohnortes aufzunehmen.
Die Angabe und damit Veröffentlichung im Amtsblatt von Familienname, Vorname, Geburtsjahr, Wohnort einschließlich Postleitzahl sowie Beruf sind damit aufgrund einer rechtlichen Verpflichtung nach Art. 6 Abs. 1 Satz 1 Buchstabe c) und Abs. 3 in Verbindung mit § 36 Abs. 3 Satz 1 GVG datenschutzrechtlich zulässig.
Die Art der Auflegung und Bekanntmachung der Schöffenliste richtete sich mangels Regelung im GVG nach den kommunalrechtlichen Vorschriften.
Die Veröffentlichung dieser vorgenannten personenbezogenen Daten im Amtsblatt war auch nach der Hauptsatzung der Stadt zulässig. Jedoch ergab sich eine Rechtsgrundlage für die Veröffentlichung der vollständigen Anschrift und des Geburtsdatums gerade nicht aus dem Wortlaut des § 36 Abs. 2 Satz 2 GVG.
Im Fall der Beschwerdeführerin war damit lediglich die Veröffentlichung ihres Wohnorts und ihrer Postleitzahl sowie ihres Geburtsjahres auf Grundlage der genannten Vorschriften zulässig. Für die Veröffentlichung ihrer vollständigen Anschrift und des Geburtsdatums der Beschwerdeführerin fehlte es hingegen an einer Rechtsgrundlage.
Auch stellte die Einwilligung in dem Interessenbekundungsformular keine wirksame Rechtsgrundlage im Sinne des Art. 6 Abs. 1 Satz 1

Buchstabe a) DS-GVO zur Veröffentlichung der vollständigen Anschrift und des Geburtsdatums der Beschwerdeführerin im Amtsblatt dar. Denn aufgrund des Über- und Unterordnungsverhältnisses zwischen einem Bürger und einer Behörde fehlte es hier bereits an der Freiwilligkeit der Einwilligung.
Nach Art. 5 Abs. 1 Buchstabe a) DS-GVO ist die Verarbeitung von personenbezogenen Daten nur dann zulässig, soweit diese transparent erfolgt. Nach Erwägungsgrund 39 der DS-GVO sollte für natürliche Personen Transparenz dahingehend bestehen, dass sie betreffende personenbezogene Daten erhoben, verwendet, eingesehen oder anderweitig verarbeitet werden und in welchem Umfang die personenbezogenen Daten verarbeitet werden und künftig noch verarbeitet werden. Der Grundsatz der Transparenz setzt ferner voraus, dass alle Informationen und Mitteilungen zur Verarbeitung dieser personenbezogenen Daten leicht zugänglich und verständlich und in klarer und einfacher Sprache abgefasst sind. Danach muss der Verantwortliche die betroffenen Personen über die in Art. 13 Abs. 1 und 2 DS-GVO aufgelisteten Punkte, wie beispielsweise Name und Kontaktdaten des Verantwortlichen, Erhebungszwecke und -umfang, sowie über Auskunftsrechte hinsichtlich der gespeicherten Daten informieren.
Im konkreten Fall wurden die Schöffeninteressenten zwar mit beigefügter datenschutzrechtlicher Einwilligung darauf hingewiesen, dass die Erhebung, Speicherung und Verarbeitung zum Zweck der ordnungsgemäßen Auswahl der Berufung der ehrenamtlichen Richter in der Strafgerichtsbarkeit erfolgte und dass die Daten an die Gemeindevertretung und den Schöffenauswahlausschuss zum Zweck der Schöffenwahl weitergeben werden. Dem Interessenbekundungsformular der Beschwerdeführerin wurden jedoch keine weiteren Datenschutzhinweise beigefügt. Insbesondere entsprachen die Informationen auf dem Musterformular nicht den gesetzlichen Vorgaben des Art. 13 DS-GVO.
Aufgrund dieses festgestellten Verstoßes gegen Art. 5 Abs. 1 Buchstaben a) und f) DS-GVO sprach der TLfDI gegen die Stadt eine Verwarnung gemäß Art. 58 Abs. 2 Buchstabe b) DS-GVO aus. Der TLfDI informierte die Beschwerdeführerin über die Verwarnung der Stadt und schloss das Verwaltungsverfahren damit ab.

2.6 Verwarnung einer Bank wegen der Übermittlung personenbezogener Daten an die Schufa

Nach Art. 6 Abs. 1 Satz 1 Buchstabe b) DS-GVO ist die Datenverarbeitung rechtmäßig, wenn die Verarbeitung für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich ist, die auf Anfrage der betroffenen Person erfolgen. Datenübermittlungen von personenbezogenen Daten an die Schufa können danach zur Vertragserfüllung eines Bankkontovertrages zulässig sein. Nach einer Kontolöschung ist eine Datenverarbeitung jedoch nicht mehr zur Vertragserfüllung erforderlich.

Aufgrund einer Beschwerde erhielt der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) Kenntnis von einer mutmaßlich unbefugten Datenverarbeitung und -übermittlung einer Bank in Thüringen an die Schutzgemeinschaft für allgemeine Kreditsicherung (Schufa). Die Beschwerdeführerin trug dem TLfDI vor, dass in ihrer Schufa-Aufstellung der letzten zwölf Monate eine Bank aufgetaucht sei, obwohl sie mehr als fünf Jahre keine Geschäftsbeziehung mehr mit dieser Bank pflegte. Die Bank führte gegenüber der Beschwerdeführerin aus, dass an dem streitgegenständlichen Tag generell eine Datenabfrage aller ihrer Kunden zum Zweck der Datenaktualität bei der Schufa vorgenommen worden sei. Die Bank konnte sich nicht erklären, warum die Schufa für die Beschwerdeführerin diese automatische Datenabfrage vorgenommen hatte, obwohl sie keine Bankkundin mehr war.
Daraufhin wandte sich der TLfDI zur Aufklärung des Sachverhalts mit einem Auskunftsersuchen zu der (unberechtigten) Schufa-Abfrage an die Bank. Die Bank teilte dem TLfDI mit, dass die Beschwerdeführerin mit der Bank im Jahr 2009 einen Kundenstammvertrag vereinbart hatte. In diesem Zusammenhang hatte die Beschwerdeführerin eine Einverständniserklärung zur Schufa-Abfrage abgegeben. Diese Einverständniserklärung meldete dann die Bank automatisiert elektronisch an die Schufa weiter sowie an die Beschwerdeführerin. Ferner übermittelte die Bank die Kontoschließung in einer Nachverarbeitung elektronisch an die Schufa. Dies erfolgte im Fall der Beschwerdeführerin im Jahr 2015 offenbar aufgrund technischer Probleme nicht korrekt. Es habe sich nach Aussage der Bank dabei jedoch um einen Einzelfall gehandelt. Aufgrund dieser fehlerhaften Meldung über die

Kontenlöschung der Beschwerdeführerin hatte die Schufa weiterhin die Datenaktualisierung im Namen der Bank vorgenommen. Nachdem der TLfDI die Bank angeschrieben hatte, veranlasste die Bank umgehend die Korrektur, was die Schufa gegenüber der Bank bestätigte.
Nach datenschutzrechtlicher Prüfung ergab sich für den TLfDI folgendes Bild: Da die Beschwerdeführerin vor mehr als fünf Jahren ihr Konto bei der Bank gekündigt hatte, lag keine Rechtsgrundlage für eine zulässige Übermittlung der personenbezogenen Daten an die Schufa vor. Nach Art. 5 Abs. 1 Buchstabe a) Datenschutz-Grundverordnung (DS-GVO) gilt der Grundsatz der Rechtsmäßigkeit, das heißt, eine der Bedingungen nach Art. 6 Abs. 1 Satz 1 DS-GVO muss für eine rechtmäßige Datenverarbeitung erfüllt sein. Die Übermittlung der personenbezogenen Daten der Beschwerdeführerin war in dem geschilderten Fall nicht rechtmäßig, weil keine der in Art. 6 Abs. 1 Satz 1 DS-GVO genannten Bedingungen für diese Rechtmäßigkeit vorgelegen hatte. Die DS-GVO hat die Verarbeitung personenbezogener Daten unter ein Verbot mit Erlaubnisvorbehalt gestellt. Danach ist die Datenverarbeitung grundsätzlich verboten, es sei denn, dass ein gesetzlicher Ermächtigungstatbestand für die Datenverarbeitung vorliegt (Art. 6 Abs. 1 Satz 1 DS-GVO).
Nach Art. 6 Abs. 1 Satz 1 Buchstabe b) DS-GVO ist die Datenverarbeitung unter anderem dann rechtmäßig, wenn die Verarbeitung für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich ist, die auf Anfrage der betroffenen Person erfolgen. Die Verarbeitung erfolgte im Fall der Beschwerdeführerin zunächst zur Durchführung vorvertraglicher Maßnahmen oder zur Vertragserfüllung. Die Übermittlung der personenbezogenen Daten an die Schufa war im Rahmen dieser Vertragserfüllung daher in diesem Stadium zulässig. Rechtsgrundlagen dieser Übermittlung waren Art. 6 Abs. 1 Satz 1 Buchstabe b) und Buchstabe f) DS-GVO. Solange die Beschwerdeführerin ein Konto bei der Bank besessen hatte, war die Verarbeitung der personenbezogenen im Rahmen dieser Geschäftsbeziehung mithin zulässig und damit auch erforderlich.
Ab dem Zeitpunkt der Kontolöschung vor mehr als fünf Jahren war die Verarbeitung jedoch nicht mehr zur Vertragserfüllung erforderlich. Auch konnte die Übermittlung der personenbezogenen Daten der Beschwerdeführerin durch die Bank an die Schufa nicht auf die Rechtsgrundlage der Einwilligung nach Art. 6 Abs. 1 Satz 1 Buch-

stabe a) DS-GVO gestützt werden. Eine solche Einwilligung der Beschwerdeführerin lag zum Zeitpunkt der Meldung an die Schufa nicht mehr vor. Durch die Löschung des Kundenstammvertrages bei der Bank war nämlich auch die Einwilligung der Beschwerdeführerin für die Meldung der Bank an die Schufa entfallen.
Weiterhin darf nach Art. 5 Abs. 1 Buchstabe e) DS-GVO bei der Speicherung der personenbezogenen Daten die Identifizierung der betroffenen Personen nur solange möglich sein, wie es für die Verarbeitungszwecke erforderlich ist. Mit diesem Grundsatz der Speicherbegrenzung wird eine zeitliche Grenze der Verarbeitung personenbezogener Daten normiert: Die Speicherung personenbezogener Daten muss beendet werden, sobald sie für die Zwecke der Verarbeitung nicht mehr erforderlich ist. Auch hier war die Übermittlung der personenbezogenen Daten an die Schufa nicht mehr erforderlich für die nicht mehr bestehende Geschäftsbeziehung zwischen der Bank und der Beschwerdeführerin.
Damit stellte der TLfDI fest, dass die Übermittlung der personenbezogenen Daten der Beschwerdeführerin an die Schufa ohne Bestehen einer Geschäftsbeziehung gegen die Regelungen des Datenschutzrechts verstoßen hatte. Der TLfDI hat das Verfahren gegen die Bank mit einer Verwarnung nach Art. 58 Abs. 2 Buchstabe b) DS-GVO abgeschlossen.

2.7 Schulsozialarbeit: Auch Schülernamen unterliegen der Schweigepflicht

Wenn es um das Wohl der Schülerinnen und Schüler geht, arbeiten an den Schulen Lehrkräfte und Schulsozialarbeiter grundsätzlich Hand in Hand. Doch dem sind datenschutzrechtliche Grenzen gesetzt – und das aus gutem Grund. Schülerinnen und Schüler müssen darauf vertrauen können, dass Lehrkräfte nicht darüber informiert werden, wenn sie Hilfe und Unterstützung durch die Schulsozialarbeit in Anspruch nehmen. Die Schweigepflicht bezieht sich auch auf die bloße Weitergabe des Namens, hier muss zuvor dann eine Einwilligung von den Schülerinnen und Schülern beziehungsweise deren Sorgeberechtigten eingeholt werden.

Aus organisatorische Gründen benötige sie die Namen der Schülerinnen und Schüler, mit denen die Schulsozialarbeiterin wöchentliche Gespräche führe, gab eine Schulleiterin an und beklagte sich beim

Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) darüber, dass die an ihrer Schule tätige Schulsozialarbeiterin ihr diese mit Verweis auf den Datenschutz verweigern würde. Für eine bessere Koordinierung der Arbeitszeit sei diese Information für die Schulleitung jedoch wichtig; schließlich würden mit der bloßen Weitergabe der Schülernamen keine schutzwürdigen Interessen der Jugendlichen berührt.
Doch der TLfDI gab der Schulsozialarbeiterin recht. Berufspsychologen, Familien-, Erziehungs- oder Jugendberater, staatlich anerkannte Sozialarbeiter oder staatlich anerkannte Sozialpädagogen und andere in § 203 Strafgesetzbuch (StGB) aufgeführte Berufsgruppen unterliegen der Schweigepflicht. Ohne eine ausdrückliche Einwilligung der Betroffenen, also der Schülerinnen und Schüler beziehungsweise deren Sorgeberechtigten, dürfen sie keine Daten weitergeben. Es ist dabei unerheblich, ob die Schulsozialarbeiterinnen und Schulsozialarbeiter von Lehrkräften oder der Schulleitung zur Übermittlung von Informationen angefragt werden oder ob sie diese von sich aus übermitteln möchten.
Sofern die Schulsozialarbeiterinnen und Schulsozialarbeiter nicht zu den in § 203 StGB aufgeführten Berufsgruppen gehören und auch nicht den Regelungen des Sozialdatenschutzes unterliegen, gilt das allgemeine Datenschutzrecht. Wenn Schülerinnen und Schüler die Schulsozialarbeiterinnen oder Schulsozialarbeiter aufsuchen, offenbaren sie ihre Daten freiwillig, also mit ihrer Einwilligung. Die von den Schülerinnen und Schülern offenbarten Daten unterliegen dann einer engen Zweckbindung, eine Offenlegung an die Schulleitung, Lehrkräfte oder andere Stellen ist daher auch in diesem Fall nur mit einer zuvor erteilten Einwilligung zulässig. Dies umfasst nicht nur die Inhalte der Gespräche und die vereinbarten Maßnahmen zur Hilfe, sondern auch die Namen der Betroffenen, da bereits durch die Offenlegung des Namens Rückschlüsse darüber möglich sind, dass die Betroffenen möglicherweise eine persönliche oder soziale Unterstützung benötigen.
Um dennoch dem Wunsch der Schulleitung für eine vereinfachte Planung und Koordination der Arbeitszeiten der Schulsozialarbeit entgegenzukommen, schlug der TLfDI vor, lediglich die belegten Zeiträume und nicht die Namen der Schülerinnen und Schüler, mit denen die Gespräche stattfinden, an die Schulleitung zu übermitteln.

2.8 Nachweis zum Masernschutz kann auf unterschiedliche Arten erbracht werden

Für den Schulbesuch muss ein Nachweis erbracht werden, dass eine Impfung oder Immunität gegen Masern oder eine Kontraindikation gegen eine Masern-Schutzimpfung besteht. Der Nachweis gegenüber der Schulleitung muss nicht zwingend durch Vorlage des Impfausweises oder einer ärztlichen Bescheinigung erfolgen, es genügt auch eine Bestätigung der zuvor besuchten Einrichtung wie der Kita, dass ein entsprechender Nachweis dort bereits vorgezeigt wurde. Diese Bestätigung darf dann auch für die Schülerakte kopiert werden.

Ranzen auf den Rücken, Zuckertüte unter den Arm und los geht's in die Schule? Bevor es so weit ist, heißt es für die Eltern erst einmal: jede Menge Formulare ausfüllen, Dokumente vorlegen und sich zum Thema Datenschutz Gedanken machen. Eine aufmerksame Mutter hatte sich beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) gemeldet und beklagt, dass eine Grundschule in einem Informationsblatt für den Anmeldetermin ihres Kindes unter anderem die Vorlage des Impfausweises verlangte. Den hätte sie jedoch schon beim Eintritt ihres Kindes in der Kita vorgelegt, sie verfüge über eine entsprechende Bescheinigung der Kita, dass ein Nachweis zur Masernimmunität vorgelegen habe. Nach Auffassung der Mutter müsse diese Bescheinigung für die Aufnahme in der Grundschule ausreichend sein, mit der Vorlage des Impfausweises würde die Schule ansonsten Einblicke in weitere Gesundheitsdaten ihres Kindes erhalten.
Der TLfDI, dem das Informationsschreiben der Grundschule vorlag, konnte der Mutter Recht geben. Für den Besuch einer Gemeinschaftseinrichtung wie zum Beispiel einer Kita oder der Schule bedarf es entweder eines Impfschutzes oder einer Immunität gegen Masern (§ 20 Abs. 8 Infektionsschutzgesetz IfSG). Der Nachweis darüber kann gemäß § 20 Abs. 9 IfSG auf unterschiedliche Weise erbracht werden. Zum einen kann ein Impfausweis vorgelegt werden, hier ist jedoch zu beachten, dass außer der Masernimpfung alle weiteren Schutzimpfungen bei der Vorlage abgedeckt werden, da für die Offenlegung der weiteren Gesundheitsdaten keine Rechtsgrundlage besteht. Zum anderen kann eine Bescheinigung eines Arztes vorgelegt werden, die entweder eine Immunität gegen Masern oder eine bestehende Kontra-

indikation gegen eine entsprechende Schutzimpfung belegt. Als weitere Möglichkeit ist zulässig, die Bestätigung einer zuvor besuchten Einrichtung vorzulegen, die bescheinigt, dass ein entsprechender Nachweis über eine Impfung, Immunität oder Kontraindikation gegen die Impfung vorgelegt wurde.
Der TLfDI informierte die Mutter darüber, dass die Bescheinigung der Kita für den Nachweis gemäß § 20 Abs. 8 IfSG ausreichend sei und bot ihr an, sich erneut an den TLfDI zu wenden, sollte die Schule dieses Dokument nicht akzeptieren und auf die Vorlage des Impfausweises bestehen.
Im Nachgang zur Schulanmeldung wandte sich die Mutter erneut an den TLfDI und beschwerte sich gemäß Art. 77 Datenschutz-Grundverordnung (DS-GVO) darüber, dass die Schule die Bestätigung der Kita über den bereits dort vorgelegten Impfnachweis zwar auch ohne Vorlage des im Info-Blatt geforderten Impfausweises akzeptiert hatte, von dieser Bescheinigung jedoch eine Kopie für die Schülerakte angefertigt hatte.
Nach § 20 Abs. 9 Satz 1 IfSG ist der Nachweis über die Masernschutzimpfung gegenüber der Leitung der jeweiligen Einrichtung zu erbringen, hier also der Schulleitung. Die Kontrolle des Masernschutzes muss vom Schulleiter gegebenenfalls gegenüber dem Gesundheitsamt nachgewiesen werden. Dazu wird in der Schülerakte ein Formular hinterlegt, auf dem dokumentiert ist, dass ein entsprechender Nachweis gemäß § 20 Abs. 9 IfSG vorgelegt wurde. Die Schulen dürfen den Immunitätsnachweis (Impfpass und/oder ärztliches Attest) jedoch nur einsehen und sich einen entsprechenden Vermerk über die Vorlage machen. Für das Anfertigen einer Kopie besteht hingegen keine Rechtsgrundlage.
Die Bestätigung einer vorher besuchten Einrichtung, dass ein Impfpass beziehungsweise ein ärztliches Attest vorgelegt wurde, entspricht vom Umfang der verarbeiteten personenbezogenen Daten also genau dem, was in der Schülerakte dokumentiert werden muss, nämlich lediglich, dass ein Immunitätsnachweis vorgelegt wurde. Dabei kann die Schule dies auf einem eigenen, von ihr verwendeten Formular dokumentieren oder ein vom Thüringer Ministerium für Arbeit, Soziales, Gesundheit, Frauen und Familie in Zusammenarbeit mit dem TLfDI entwickeltes Formular verwenden. Sie kann jedoch ebenso die Bestätigung der vorherigen Einrichtung als Dokumentation des erbrachten Immunitätsnachweises kopieren und in die Schülerakte aufnehmen. Aus datenschutzrechtlicher Sicht kommt es lediglich darauf an, dass

in der Schülerakte keine besonderen Kategorien personenbezogener Daten (hier: Gesundheitsdaten) gemäß Art. 9 DS-GVO geführt werden, für die es keine Rechtsgrundlage gibt. Die Kopie der Bestätigung der Kita enthielt keine solchen Daten. Ein Verstoß gegen datenschutzrechtliche Regelungen lag damit nicht vor und die Beschwerde der Mutter musste abgewiesen werden.
Unabhängig davon hatte sich der TLfDI zwischenzeitlich an die Grundschule gewandt und darauf hingewiesen, dass die Vorlage eines Nachweises gegen die Masernschutzimpfung ausreichend ist und ein Impfausweis nicht zwingend vorgelegt werden muss.

2.9 Verstoß gegen DS-GVO durch Bekanntmachung im Amtsblatt?

Den TLfDI erreichen regelmäßig Anfragen oder Beschwerden von Bürgern, wenn ihre personenbezogenen Daten von öffentliche Stellen in Veröffentlichungen preisgegeben werden. Selbstverständlich dürfen Städte, Gemeinden oder Landkreise sowie andere Thüringer Behörden solche Informationen nicht einfach so veröffentlichen, wie auch der folgende Fall zeigt. Hier hatte ein Landkreis einen Bescheid mit vielen personenbezogenen Daten der Beschwerdeführerin im Amtsblatt veröffentlicht – was im Ergebnis aber rechtmäßig war.

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichte eine Beschwerde einer Bürgerin zu einer sie selbst betreffenden Veröffentlichung eines Bescheides über die Androhung von Zwangsmaßnahmen in einer bauordnungsrechtlichen Angelegenheit. Für die Mitarbeiter des TLfDI war der Inhalt der Beschwerde anfangs nur schwer ermittelbar. Die Bürgerin teilte mit, dass der handelnde Landkreis trotz ihrer gestellten Strafanzeige, Stellung von Strafanträgen und ohne Zustimmung eine Duldungsanordnung bezüglich des zwangsweisen Zutritts zu einem im Miteigentum der Beschwerdeführerin stehenden Grundstück im Amtsblatt veröffentlicht habe.
Auf Nachfrage des TLfDI wurde die Situation durch die Beschwerdeführerin nicht klarer erläutert: Sie erhob Vorwürfe der Amtsanmaßung und des Amtsmissbrauchs gegen Mitarbeiter der Baubehörde des Landkreises. Sie habe ein Schreiben des Landkreises aus dem Dezember 2022 ausdrücklich wegen fehlendem Vertrauensverhältnis auf-

grund von Lügen zurückgewiesen. Und dann plötzlich sei sie im Frühjahr 2023 informiert worden, dass im Amtsblatt des Landkreises ein Bescheid mit sämtlichen relevanten personenbezogenen Daten von der Beschwerdeführerin veröffentlicht worden sei. Dabei habe sie selbst doch eine Adresse, an die dieser Bescheid hätte geschickt werden können, und außerdem hätte der Landkreis die Post ja auch an das von ihr mitgeteilte Postfach übersenden können.
Das vom TLfDI angehörte Landratsamt nahm zu dem Vorhalt ausführlich Stellung. Es bestätigte, dass die personenbezogenen Daten der Beschwerdeführerin veröffentlicht wurden. Dies sei jedoch berechtigterweise erfolgt, da dem Landkreis für die Beschwerdeführerin keine zustellfähige Adresse vorgelegen habe.
Der Landkreis hatte Erkenntnisse, dass auf dem Grundstück möglicherweise unzulässige Baumaßnahmen stattgefunden hätten. Zur Prüfung wurde der Beschwerdeführerin das oben erwähnte zurückgewiesene Schreiben mit einer Terminmitteilung für eine Grundstücksbegehung durch die zuständigen Mitarbeiter des Bauamtes übersandt. Die Rücksendung durch die Beschwerdeführerin erfolgte mit den Vermerken „Treuhandbruch-Betretungsverbot“ und „Entwertet mangels Prokura“. Auch teilte die Beschwerdeführerin im beiliegenden Anschreiben Folgendes mit: „Nach ausführlicher Prüfung der Aktenlage muss festgestellt werden, dass kein Auftrag an Sie oder Ihr Haus ergangen ist. Es konnte kein Vorgang gefunden werden. Das Schreiben ist somit unzurechnungsfähig.“
Dem Schreiben der Beschwerdeführerin waren noch umfangreiche weitere Unterlagen beigefügt, unter anderem Strafanträge an den „Militärstaatsanwalt für das US-Protektorat BRD“ und ein „Vorläufiger Staatsangehörigkeitsausweis Königreich Sachsen“. Kurze Zeit später versuchte der Landkreis eine Duldungsanordnung nebst Androhung von Zwangsmitteln bei der Beschwerdeführerin zuzustellen. Dieser Bescheid kam mit dem Vermerk der Post „Empfänger unbekannt verzogen“ zurück. Vor Ort wurden vom Landkreis noch Ermittlungen angestellt. An der Adresse fand sich jedoch ein Schild „Keine Post für ... einwerfen“ und eine Nachfrage ergab, dass der Vermieter die Beschwerdeführerin beim Einwohnermeldeamt abgemeldet hatte. Daher, so der Landkreis gegenüber dem TLfDI, sei die „öffentliche Zustellung“ der Duldungsanordnung über das Amtsblatt erfolgt.
Für den TLfDI ergab sich aus dem schlussendlich festgestellten Sachverhalt kein Verstoß gegen datenschutzrechtlich Vorschriften.

Grundsätzlich ist die Verarbeitung personenbezogener Daten nur bei Einhaltung der Vorschriften der Europäischen Datenschutz-Grundverordnung (DS-GVO) zulässig. Im vorliegenden Fall war die Behörde, der Landkreis, nach Art. 6 Abs. 1 Buchstabe e) DS-GVO in Verbindung mit Art. 6 Abs. 2 und 3 DS-GVO befugt, die personenbezogenen Daten der Beschwerdeführerin im Rahmen der öffentlichen Bekanntmachung der Duldungsanordnung im Amtsblatt zu verarbeiten. Nach Art. 6 Abs. 1 Buchstabe e) DS-GVO dürfen Behörden personenbezogene Daten verarbeiten, wenn diese zur Erfüllung einer öffentlich-rechtlichen Aufgabe notwendig sind. Die entsprechenden anwendbaren und im Berichtszeitraum geltenden gesetzlichen Regelungen der Thüringer Bauordnung (ThürBO) und des Thüringer Verwaltungszustellungs- und Vollstreckungsgesetzes (ThürVwVZG) sind unter Berücksichtigung des Art. 6 Abs. 2 und 3 DS-GVO erlassen worden und regeln die Art und Weise der Verarbeitung.
Ein Landkreis beziehungsweise dessen Baubehörde ist nach § 58 ThürBO berechtigt, nach vorheriger Ankündigung Grundstücke zur Prüfung der Einhaltung baulicher Vorschriften zu betreten. Da die Beschwerdeführerin im konkreten Fall ihre Zustimmung verweigerte, musste eine Duldungsanordnung mit der Androhung von Zwangsmitteln erlassen werden. Diese ist wegen der angedrohten Zwangsmittel nach § 46 Abs. 6 ThürVwVZG immer zuzustellen.
Selbstverständlich musste die Behörde vor der öffentlichen Zustellung alle rechtlich möglichen Schritte unternehmen, um eine zustellfähige Adresse zu ermitteln. Das Landratsamt hatte dazu das Anhörungsschreiben mit Vorschlag für einen Begehungstermin an die Beschwerdeführerin übersandt. Dieses Schreiben aber hat diese mit rechtlich unzulässigen Vermerken an das Landratsamt zurückgesandt. Da somit ein Begehungstermin nicht zustande kam, wurde an die Beschwerdeführerin eine Duldungsverfügung nebst Androhung von Zwangsmitteln mittels Postzustellungsurkunde an ihre letzte bekannte Meldeanschrift versandt. Diese kam mit dem Vermerk der Unzustellbarkeit (Empfänger unbekannt verzogen) zurück. Eine andere zustellungsfähige Adresse war dem Landkreis nicht bekannt, eine Wegzuganschrift war nicht zu ermitteln.
Da der entsprechende Bescheid zur Ankündigung eines Begehungstermins nicht nachweisbar zugestellt werden konnte, erfolgte die Ankündigung einschließlich der zulässigerweise mitgeteilten Androhung von Zwangsmitteln dann entsprechend der bestätigten Hauptsatzung des Landkreises über das Amtsblatt der Behörde. Dabei wurden die

gesetzlichen Voraussetzungen des § 15 Abs. 2 ThürVwZVG eingehalten. Eine Einwilligung der oder gar eine Beauftragung durch die Beschwerdeführerin ist bei Vorliegen einer gesetzlichen Berechtigung nicht erforderlich.
Infolgedessen kam der TLfDI zu dem Ergebnis, dass die Datenschutzbeschwerde der Beschwerdeführerin hier unbegründet war, und er erließ einen Bescheid, in dem er die Gründe dafür der Beschwerdeführerin ausführlich mitteilte.

2.10 Fünf Gesundheitsämter und ein Problem – *MikroproHealth*

Im November/Dezember 2023 und im Frühjahr 2024 berichteten verschiedene Medien (unter anderem *Die Zeit* und der MDR) wiederholt über mögliche datenschutzrechtliche Lücken in der Software *MikroproHealth*. Die Software wird in mehreren Bundesländern von verschiedenen Gesundheitsämtern genutzt, nach Kenntnis des TLfDI auch von fünf Gesundheitsämtern in Thüringen. Bei einer Vor-Ort-Kontrolle in einem Thüringer Gesundheitsamt, das die Software nutzt, konnte der TLfDI feststellen, dass die Nutzer selbst mögliche sicherheitsrelevante Schwachpunkte der Software abstellen und die Software im Sinne von Art. 5 Abs. 1 Buchstabe f) DS-GVO datenschutzkonform einsetzen können.

Durch einen Zeitungsartikel hatte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) im November 2023 Kenntnis davon erhalten, dass in der Software *MikroproHealth*, die auch in einigen Thüringer Gesundheitsämtern genutzt wird, „massive Sicherheitsprobleme“ festgestellt worden seien (vergleiche https://www.computerbase.de/2023-11/software-mikroprohealth-massive-sicherheitsprobleme-in-gesundheitsaemtern-aufgedeckt/).
Der Einsatz einer Software stellt nicht per se einen Verstoß gegen die Datenschutz-Grundverordnung (DS-GVO) dar, wenn die Nutzer der Software als Verantwortliche diese selbst datenschutzkonform konfigurieren können und beispielsweise ein dem erhöhten Schutzniveau von sensiblen Gesundheitsdaten angemessenes Rechte- und Rollenkonzept sowie rechtskonforme Löschfristen implementieren können. Gemäß entsprechender Angaben im oben genannten Presseartikel konnten durch technische und organisatorische Maßnahmen hierdurch

die in der Presse bemängelten datenschutzrechtlichen Sicherheitsprobleme durch die Administratoren in den Gesundheitsämtern behoben werden. Der TLfDI teilte dem Thüringer Landesverwaltungsamt und dem Thüringer Ministerium für Arbeit, Soziales, Gesundheit, Frauen und Familie mit, dass die Gesundheitsämter als Nutzer der Software technische und organisatorische Maßnahmen wie angemessene Rollen- und Rechte-Konzepte selbst implementieren müssen. Der TLfDI wies beide Behörden auf die Einhaltung datenschutzrechtlicher Vorgaben für besondere Datenkategorien hin, vorliegend Gesundheitsdaten gemäß Art. 9 Abs. 1 DS-GVO und dass dem erhöhten Schutzniveau angemessene technische und organisatorische Maßnahmen nach Art. 32 Abs. 1 DS-GVO von den Gesundheitsämtern selbst umzusetzen sind.

Im Februar 2024 teilten zwei nicht betroffene Personen dem TLfDI mit, dass es in Thüringer Gesundheitsämtern zu Verstößen gegen den Schutz von personenbezogenen Daten durch den Einsatz der Software *MikroproHealth* komme. So könnten scheinbar alle Mitarbeiter Einsicht in die Stammdatenbank aller hinterlegten Personen nehmen, da hier „Sicherheitsmaßnahmen“ – wie beispielsweise angemessene Rechte- und Rollenkonzepte – und damit verbundene Zugriffsbeschränkungen fehlten. Außerdem seien mit der Software beliebige Datenbank-Abfragen möglich, sodass die Datenbank beliebig manipuliert und auch gelöscht werden könne. Zudem protokolliere die Software nichts, sodass eine Person Daten manipulieren, verändern und löschen könne, ohne dass dies auf die Person zurückgeführt werden könne. Weiterhin sei die Software mangelhaft bei der Umsetzung von Löschfristen, sodass viele Datenbanken Vorgänge enthielten, die längst gelöscht sein müssten.

Geeignete Nachweise oder Belege für ihre Angaben legten die Eingebenden dem TLfDI nicht vor. Obgleich dem TLfDI keine Beschwerden von betroffenen Personen gemäß Art. 4 Nummer 1 DS-GVO in Verbindung mit Art. 77 Abs. 1 DS-GVO aus Thüringen vorlagen, die die Verletzung des Schutzes personenbezogener Daten durch den Einsatz dieser Software zum Gegenstand hatten, nahm der TLfDI die Beschwerde zum Anlass und führte Anfang Mai 2024 eine Vor-Ort-Kontrolle in einem Thüringer Gesundheitsamt durch, das die Software nutzte, um die konkreten Konfigurationsmöglichkeiten der Software aus datenschutzrechtlicher Sicht zu prüfen.

Die Mitarbeiter des Gesundheitsamtes zeigten sich sehr interessiert und kooperativ und beantworteten sämtliche datenschutzrechtliche

Fragen zu den genutzten Softwarekomponenten der Firma Mikropro detailliert und nachvollziehbar, wobei auch das Modul „Health“ thematisiert wurde. Ebenso führten sie dem TLfDI den praktischen Einsatz der Software in den verschiedenen Fachbereichen des Gesundheitsamtes technisch vor. Hierbei stellte der TLfDI fest, Adresse (Einzelfelder)(Briefanrede)dass die Software grundsätzlich technische Einstellungsoptionen bietet, die eine datenschutzkonforme Nutzung durch die jeweiligen Gesundheitsämter ermöglichen oder technische Maßnahmen durch das Gesundheitsamt gefunden wurden, bestehende Schwachstellen zu umgehen. Jedoch hatte die Firma Mikropro selbst nach Information der Administratoren des Gesundheitsamtes ein zentrales Zugangspasswort festgelegt (Administrator-Passwort im Quellcode) und vom Nutzer, vorliegend dem zuständigen Landratsamt, gefordert, dieses Passwort nicht zu ändern, obwohl eine Änderung möglich war. Die System-administratoren des Landratsamtes hatten jedoch das Passwort gegen die Vorgabe von Mikropro selbst geändert, um den Datenschutz zu wahren und eine Verarbeitung durch unbefugte Dritte von personenbezogenen Daten zu verhindern, die über die Software gespeichert werden.
Weiterhin hatte die Firma Mikropro die Nutzer der Software, vorliegend das zuständige Landratsamt, über mehrere datenschutzrechtlich mögliche technische Optionen der Software – wie Passwortänderung, Nutzerbeschränkungen und Festlegung von Rollen- und Rechtekonzepten – nicht informiert. Die Systemadministratoren im Landratsamt hatten die entsprechenden Optionen jedoch selbst herausgefunden und die erforderlichen technischen Änderungen vorgenommen, um die Software grundsätzlich datenschutzkonform nutzen zu können. Auch wurden zusätzliche Einschränkungen zu Datenbankzugriffen implementiert und die organisatorische Struktur des Gesundheitsamtes so gewählt, dass der durchaus sehr weite Zugriffsrahmen auf Daten innerhalb einer Modul-Instanz nur auf wenige Mitarbeiter beschränkt werden konnte. Der Firmensitz des Softwareunternehmens, der Mikroprojekt GmbH, befindet sich in Kaiserlautern, Rheinland-Pfalz. Somit ist der TLfDI für die Prüfung der Software auf Datenschutzkonformität nicht zuständig. Dennoch behält sich der TLfDI eine weitere Prüfung der Software vor, sofern sich konkrete Anhaltspunkte für Verstöße gegen den Datenschutz durch den Einsatz der Software durch Gesundheitsämter in seinem Zuständigkeitsbereich ergeben.

2.11 Datenverarbeitung durch das Gesundheitsamt: Ermitteln erlaubt

Nach Art. 5 Abs. 1 Buchstabe a) DS-GVO in Verbindung mit Art. 6 Abs. Satz 1 Buchstabe c) DS-GVO und Art. 9 Abs. 2 Buchstabe g) DS-GVO ist die Verarbeitung personenbezogener Daten rechtmäßig, wenn hierfür eine Rechtsgrundlage besteht. Für die Verarbeitung von Gesundheitsdaten finden sich verschiedene einschlägige Rechtsnormen im IfSG, unter anderem in § 20 Abs. 9 Satz IfSG und § 20 Abs. 12 Satz 2 IfSG.

Im November 2023 beschwerte sich der Vater eines Kindergartenkindes beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) über ein Gesundheitsamt in Thüringen. Das Gesundheitsamt hatte von den Eltern gefordert, für die Gestattung des Kindergartenbesuchs einen schriftlichen Nachweis über die bestehende Kontraindikation zur Masernschutzimpfung des Kindes als betroffene Person zu erbringen. Der Vater trug vor, dass das Kind über ein entsprechendes ärztliches Attest verfüge, das dem Kindergarten bereits bekannt sei. Dieses Attest über die Kontraindikation hatte jedoch nicht der behandelnde Kinderarzt des Kindes ausgestellt, sondern ein anderer Arzt. Diesbezüglich forderte das Gesundheitsamt von der Familie eine Schweigepflichtentbindungserklärung für den das Attest ausstellenden Arzt.
Gegenstand der Beschwerde war die Verarbeitung der personenbezogenen Daten des betroffenen Kindes und dessen Eltern durch das Gesundheitsamt, da den Eltern unklar war, woher das Gesundheitsamt wusste, dass das Attest zur Kontraindikation von einem anderen Arzt als dem behandelnden Kinderarzt ausgestellt worden war. Diese Information habe sich nicht in der Kindergartenakte befunden und sei dem Gesundheitsamt von der betroffenen Person auch nicht mitgeteilt worden. Die Eltern hatten das Attest nur bei Kindergarteneintritt ihres Kindes im Kindergarten ohne weitere Informationen vorgelegt. Das Gesundheitsamt hatte im Schreiben an die betroffene Person zur geforderten Schweigepflichtentbindung mitgeteilt, dass Zweifel an der inhaltlichen Richtigkeit des ausgestellten Attests zur Kontraindikation bestünden, da der ausstellende Arzt eine Vielzahl solcher formal gleichlautender, zeitlich unbefristeter, jede Art von Impfstoff betreffenden pauschalen Atteste ohne Diagnose und Begründung ausgestellt

habe, ohne der behandelnde Kinderarzt der betreffenden Kinder zu sein.
Der TLfDI erläuterte dem Vater des betroffenen Kindes die Rechtslage zur Forderung des Gesundheitsamtes anhand der Datenschutz-Grundverordnung (DS-GVO) und des Infektionsschutzgesetzes (IfSG). Gemäß Art. 5 Abs. 1 Buchstabe a) DS-GVO in Verbindung mit Art. 6 Abs. 1 Satz 1 Buchstabe a) DS-GVO und Art. 9 Abs. 1 DS-GVO ist die Verarbeitung personenbezogener Gesundheitsdaten zulässig, wenn die betroffene Person in die Verarbeitung ihrer Daten eingewilligt hat. Ohne Einwilligung der betroffenen Person ist eine Verarbeitung ihrer personenbezogenen Daten nur unter den Voraussetzungen von Art. 6 Abs. 1 Satz 1 Buchstabe b) bis e) sowie Art. 9 Abs. 2 Buchstabe b) bis j) zulässig. Nach Art. 5 Abs. 1 Buchstabe a) DS-GVO in Verbindung mit Art. 6 Abs. 1 Satz 1 Buchstabe c) DS-GVO und Art. 9 Abs. 2 Buchstabe g) DS-GVO ist die Verarbeitung personenbezogener Daten rechtmäßig, wenn hierfür eine Rechtsgrundlage besteht, wie im Falle der Beschwerde die Rechtsnormen des Infektionsschutzgesetzes (IfSG). Zudem ist die Verarbeitung von personenbezogenen Daten im Sinne von Art. 6 Abs. 1 Satz 1 Buchstabe e) DS-GVO durch öffentliche Behörden im Rahmen der Erfüllung ihrer staatlichen Verwaltungsaufgaben zulässig.
Nach § 20 Abs. 9 Satz 1 IfSG ist der Nachweis über die Masernschutzimpfung gegenüber der Leitung der jeweiligen Einrichtung zu erbringen. Der/die Leiter/in ist die Person, die mit den Leitungsaufgaben in der jeweiligen Einrichtung beauftragt ist, vergleiche § 2 Nr. 15 IfSG. Die Kindergartenleitung darf den Immunitätsnachweis (Impfpass und/oder ärztliches Attest) nur einsehen und sich einen entsprechenden Vermerk über die Vorlage machen, jedoch keine Kopie anfertigen. Eine Ausnahme von der Impfpflicht besteht unter anderem für Personen, die mit einem ärztlichen Attest nachweisen, dass eine Impfung aus gesundheitlichen Gründen kontraindiziert ist, oder wenn sie bereits immun sind. Diese Kontraindikation muss – ebenso wie der Nachweis der Impfung – ärztlich bestätigt sein.
Zu den Aufgaben des Gesundheitsamtes gehört es auch, den öffentlichen Gesundheitsschutz im Sinne des IfSG umfassend sicherzustellen und zu gewährleisten, vergleiche § 1 Abs. 1 der Verordnung über den öffentlichen Gesundheitsdienst und die Aufgaben der Gesundheitsämter in den Landkreisen und kreisfreien Städten (GesDV Thüringen). Sofern das Gesundheitsamt im Zusammenhang mit der Information

nach § 20 Abs. 9 Satz 1 IfSG selbst begründete Zweifel an der Echtheit oder Richtigkeit eines ärztlichen Attestes zur Kontraindikation hat, ist das Gesundheitsamt gemäß § 20 Abs. 12 Satz 2 ff. IfSG befugt, zum betreffenden Attest auch bei dem ausstellenden Arzt weitere Informationen zur Kontraindikation einzuholen und die zugehörigen personenbezogenen Daten zu verarbeiten. Für die Beurteilung, ob Zweifel an der Echtheit des Attestes medizinisch oder sachlich berechtigt sind, ist der TLfDI nicht zuständig, diese Bewertung obliegt ausschließlich den öffentlichen Gesundheitsbehörden.
Der TLfDI empfahl dem Vater, sich selbst direkt an das Gesundheitsamt zu wenden und auf Grundlage von Art. 15 Abs. 1 DS-GVO um Auskunft über die Verarbeitung der personenbezogenen Daten der betroffenen Person zu bitten und zu erklären, woher dem Gesundheitsamt die Information bekannt sei, welcher Arzt das Attest zur Kontraindikation ausgestellt hatte. Gemäß Art. 15 Abs. 1 DS-GVO hat jede betroffene Person das Recht, vom Verantwortlichen umfassende Auskunft über die Verarbeitung ihrer personenbezogenen Daten zu verlangen. Das Auskunftsrecht der betroffenen Person schließt sämtliche Auskünfte über die Verarbeitungszwecke und Empfänger der personenbezogenen Daten sowie Dauer der Speicherung dieser Daten ein. Zudem ist der Verantwortliche gemäß Art. 15 Abs. 1 Buchstabe g) DS-GVO verpflichtet, alle verfügbaren Informationen über die Herkunft der Daten zu erteilen, sofern die Daten nicht bei der betroffenen Person selbst erhoben wurden. Somit konnte der Beschwerdeführer vom Gesundheitsamt auch die Auskunft verlangen, wodurch dem Gesundheitsamt bekannt war, welcher Arzt das Attest zur Kontraindikation ausgestellt hatte.
Im Februar 2024 wandte sich der Vater des betroffenen Kindes erneut an den TLfDI und wiederholte seine Beschwerde über das Gesundheitsamt. Zwischenzeitlich hatte der Vater im Gesundheitsamt Akteneinsicht genommen und auf einem Aktendeckel eine handschriftliche Notiz gefunden, welcher Arzt das Attest zu Kontraindikation der Masernschutzimpfung ausgestellt hatte. Der TLfDI verwies den Vater auf die Antwort des TLfDI zur Beschwerde des Vaters vom November 2023 und die darin aufgeführte Rechtslage der DS-GVO und des IfSG. Aus datenschutzrechtlicher Sicht hatte das Gesundheitsamt die personenbezogenen Daten der betroffenen Person gemäß Art. 6 Abs. 1 Satz 1 Buchstabe c) und Buchstabe e) DS-GVO sowie Art. 9 Abs. 2 Buchstabe g) DS-GVO in Verbindung mit § 20 Abs. 9 Satz 2 IfSG und § 20 Abs. 12 Satz 2 ff. IfSG rechtmäßig verarbeitet und dem

Beschwerdeführer gemäß Art. 15 Abs. 1 DS-GVO auch fristgemäß eine nachvollziehbare Aufstellung der personenbezogenen Daten übersandt hatte, die es von der betroffenen Person verarbeitet hatte. Somit konnte der TLfDI keinen Verstoß des Gesundheitsamtes gegen den Schutz von personenbezogenen Daten der betroffenen Person feststellen und beendete das Verwaltungsverfahren. Daraufhin legte der Beschwerdeführer Klage gegen den Bescheid des TLfDI beim zuständigen Verwaltungsgericht ein. Eine Entscheidung lag zum Ende des Berichtszeitraums noch nicht vor.

2.12 Gemeinsame Verantwortlichkeit der Unfallkasse Thüringen mit Stellen der öffentlichen Verwaltung wegen Betreibens einer Datenbank

Ein Cyberangriff auf die Unfallkasse Thüringen führte zu einem Datendiebstahl bei Verantwortlichen aus den nicht-öffentlichen und öffentlichen Bereichen. Zu prüfen war, ob eine gemeinsame Verantwortlichkeit nach Art. 26 DS-GVO vorlag und damit auch die betroffenen Verantwortlichen eine Meldung nach Art. 33 DS-GVO an den TLfDI machen mussten. Der TLfDI kam zu dem Ergebnis, dass dies nicht der Fall war und nur die Unfallkasse eine Meldung abzugeben hatte.

Die Unfallkasse Thüringen ist der Unfallversicherungsträger unter anderem für Kindergarten- und Schulkinder sowie Studierende, Arbeiter, Angestellte und Auszubildende in Einrichtungen der Kommunen oder des Landes. Die Unfallkasse Thüringen hat zur Aufgabe, Betroffene von Arbeits-, Schul- und Wegeunfällen sowie Berufskrankheiten medizinisch, beruflich und sozial mit allen geeigneten Mitteln zu rehabilitieren beziehungsweise durch Geldleistungen zu entschädigen. Im Falle eines Unfalls haben Unternehmen gemäß § 193 Sozialgesetzbuch (SGB) VII die Pflicht zur Meldung eines Unfalls beim Unfallversicherungsträger.
Am 19. Dezember 2023 meldete die Unfallkasse Thüringen dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) eine Verletzung des Schutzes personenbezogener Daten nach Art. 33 Datenschutz-Grundverordnung (DS-GVO). Durch einen Cyberangriff auf die Unfallkasse Thüringen wurden rund 750.000 Datensätze von Versicherten gestohlen.

Aus der Meldung ging hervor, dass die Angreifer mit Hilfe einer Ransomware Teile der IT-Infrastruktur verschlüsselt und Daten gestohlen haben, die im Darknet veröffentlicht wurden. Bei den gestohlenen Daten handelte es sich um Informationen über die Versicherten, Hinterbliebene und deren Bevollmächtigte sowie Informationen über die Mitgliedseinrichtungen. Betroffen waren persönliche Daten der Versicherten sowie betriebliche Daten der mit der Unfallkasse Thüringen in Verbindung stehenden Leistungserbringer, Unternehmen und sonstigen Einrichtungen.
Durch die Unfallkasse Thüringen wurden umfangreiche Sicherheitsmaßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten vorgenommen. Nach Prüfung der vorgenommenen technischen und organisatorischen Maßnahmen durch die Unfallkasse Thüringen konnte der TLfDI die Meldung nach Art. 33 DS-GVO abschließen.
Im Nachgang des IT-Sicherheitsvorfalls und der damit verbundenen Verletzung des Schutzes personenbezogener Daten nach Art. 33 DS-GVO hat der TLfDI von einer Kommune die Anfrage erhalten, ob gemäß Art. 26 DS-GVO eine gemeinsame Verantwortlichkeit für das Betreiben einer gemeinsamen Datenbank vorliegt und ob alle Beteiligten gemäß Art. 33 DS-GVO eine Meldung des Schutzes personenbezogener Daten abgeben müssen.
Hintergrund ist, dass die Kommune annahm, es handele sich um ein arbeitsteiliges Zusammenwirken zwischen der öffentlichen Verwaltung und der Unfallkasse Thüringen, wobei beide Einfluss auf die personenbezogenen Daten sowie auf die Zwecke und Mittel nehmen und somit dieselben Interessen verfolgen.
Man ging davon aus, dass die Übertragung der Aufgabenerledigung auf die Unfallkasse Thüringen zur Folge hat, dass diese Stelle gemäß Art. 4 Nr. 7 DS-GVO verantwortlich ist. Wenn mehrere Verantwortliche an der Erledigung von Aufgaben mitwirken, wie etwa bei der Pflege personenbezogener Daten in einer Datenbank, wurde vom zuständigen Verantwortlichen im öffentlichen Sektor die Annahme getroffen, dass eine gemeinsame Verantwortung gemäß Art. 26 DS-GVO vorliegt. Wenn mehrere Verantwortliche gemäß Art. 26 DS-GVO gemeinsam handeln, so sind im Außenverhältnis alle von ihnen meldepflichtig.
Die Beantwortung der Frage war wichtig, weil es nur vereinzelt Meldungen von verantwortlichen Arbeitgebern gegeben hatte. Wären sie

gemeinsam mit der Unfallkasse verantwortlich gewesen, hätten sie unter Umständen auch melden müssen.
Bei einem Verantwortlichen handelt es sich gemäß Art. 4 Nr. 7 DS-GVO um jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Der Verantwortliche definiert sich somit insbesondere dadurch, dass dieser stets die Zwecke und Mittel der Datenverarbeitung festlegt, also über das *Ob* und das *Wie* der Datenverarbeitung entscheidet. Nach dem Gesetzeswortlaut des Art. 26 DS-GVO besteht eine gemeinsame Verantwortlichkeit, wenn zwei oder mehrere Verantwortliche die Zwecke und wesentlichen Mittel der Verarbeitung gemeinsam festlegen.
Die Unfallkasse Thüringen wurde zu der Frage angehört. Sie ging nicht von einer gemeinsamen Verantwortlichkeit aus. Sie begründete dies damit, dass ihrer Auffassung nach nicht mehrere Verantwortliche die Zwecke und Mittel der Datenverarbeitung gemeinsam festlegen. Der Zweck der Datenverarbeitung und damit auch die jeweiligen Pflichten des Unfallversicherungsträgers und der Unternehmer sind im SGB VII gesetzlich festgelegt. Eine Festlegung durch sie gemeinsam erfolgt daher nicht. Auch die Entscheidung über die eingesetzten Mittel, also wie der Unfallversicherungsträger seinen Verpflichtungen zur Leistungserbringung nach dem SGB VII nachkommt und welche technischen Infrastrukturen für die Datenverarbeitung genutzt werden, obliegt allein der Unfallkasse Thüringen.
Der Datenschutzvorfall ereignete sich in den nachgelagerten Systemen der Unfallkasse Thüringen, für die diese allein verantwortlich ist. Ein „gemeinsames Ziel“ zwischen der Unfallkasse Thüringen und den Verantwortlichen im Hinblick auf die Fallbearbeitung konnte durch den TLfDI nicht festgestellt werden, da die meldende Stelle einzig ihrer gesetzlichen Meldepflicht gegenüber der Unfallkasse nachkommt. Das „gemeinsame Ziel“ zwischen der Unfallkasse Thüringen und den Verantwortlichen ist einzig die Einhaltung der Anforderungen des SGB VII. Für die „Fallbearbeitung“ der Behandlung und Geltendmachung von Ansprüchen aus Versicherungsleistungen ist die Unfallkasse Thüringen Verantwortlicher, da diese die Zwecke per Gesetz übertragen bekommen und die einzusetzenden Mittel selbstständig festgelegt hat.
Somit konnten aus Sicht des TLfDI zwei voneinander getrennte Verantwortlichkeiten festgestellt werden. Die entsprechende Meldung

nach Art. 33 DS-GVO musste, wie geschehen, allein von der Unfallkasse Thüringen erfolgen. Die verantwortlichen Arbeitgeber mussten keine Meldung nach Art. 33 DS-GVO gegenüber dem TLfDI abgeben.

2.13 Zustellung von Abmahnungen durch den Hausmeister

Bei der Verarbeitung von personenbezogenen Beschäftigtendaten, wie einer Abmahnung, muss der Arbeitgeber darauf achten, dass die unbeabsichtigte Kenntnisnahme durch einen anderen, nicht berechtigten Mitarbeiter verhindert wird.

Im Berichtszeitraum 2024 beschwerte sich eine Bürgerin beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) darüber, dass der Hausmeister ihres Arbeitgebers, eine Stadtverwaltung in Thüringen, als Zeuge/Bote und dadurch als nichtberechtigte Person für Personalangelegenheiten eine Abmahnung per Einwurf in ihren Briekasten zugestellt hatte. Der Hausmeister ist bei der verantwortlichen Stelle im Bereich Hausmeistertätigkeiten angestellt und nicht für Personalsachen zuständig. Der Hausmeister sollte als Zeuge für die Übergabe der Abmahnung fungieren. Da die Beschwerdeführerin nicht persönlich angetroffen wurde, stellte die Stadtverwaltung die Abmahnung per Einwurf in den Briefkasten zu. Die Zustellung der Abmahnung bestätigten der Hausmeister und der Beschäftigte der Personalabteilung direkt auf Seite 2 der Abmahnung mit „Abmahnungsschreiben persönlich in den Briefkasten hinterlegt durch“.
Dem Hausmeister als unberechtigte Person war es dadurch möglich gewesen, den Zweck des Schreibens sowie den Inhalt der Abmahnung zur Kenntnis zu nehmen. Die Stadtverwaltung berief sich darauf, dass das Hinzuziehen des Hausmeisters als Zeuge notwendig gewesen sei, um die Zustellung rechtssicher zu dokumentieren. Dafür sei es erforderlich, dass dem Boten/Zeugen der Inhalt des Schreibens bekannt sei, damit dieser nicht bestritten werden kann.
Nach 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. Bei der Verarbeitung der personenbezogenen Daten, konkret hier der Abmahnung der Beschwerdeführerin, muss

der Arbeitgeber darauf achten, dass die unbeabsichtigte Kenntnisnahme durch einen anderen, nicht berechtigten Mitarbeiter – in diesem Fall den Hausmeister – verhindert wird. Insbesondere ergibt sich hier die Zustellung mittels Bote auch nicht aus einer rechtlichen Verpflichtung, vergleiche Art. 6 Abs. 1 Buchstabe c) DS-GVO. Die Zustellung ist die Bekanntgabe eines Schriftstückes an eine Person in der gesetzlich vorgeschriebenen Form zur Sicherung des Nachweises von Zeit und Art der Übergabe (§§ 166–195 Zivilprozessordnung [ZPO]). Zugestellt werden kann nach §§ 3 fortfolgende Thüringer Verwaltungsverfahrensgesetz (ThürVwVfG) durch die Post mit Zustellungsurkunde, durch die Post mittels Einschreiben, durch die Behörde gegen Empfangsbekenntnis oder durch De-Mail-Dienste als zusätzliche Zustellungsform bei elektronischen Dokumenten. Wenn die Behörde selbst zustellt und den Empfänger nicht antrifft, sind nach § 5 Abs. 2 S. 2 Nr. 3 Thüringer Verwaltungszustellungs- und Vollstreckungsgesetz (ThürVwZVG) der Grund der Ersatzzustellung sowie Informationen darüber, wann und wo das Schriftstück in einen Briefkasten eingelegt oder sonst niedergelegt und in welcher Weise die Niederlegung schriftlich mitgeteilt wurde, zum Nachweis der Zustellung in den Akten zu vermerken (vergleiche §§ 180 bis 181 ZPO). Nach § 180 ZPO kann das Schriftstück in einen zu der Wohnung oder dem Geschäftsraum gehörenden Briefkasten oder in eine ähnliche Vorrichtung eingelegt werden, die der Adressat für den Postempfang eingerichtet hat und die in der allgemein üblichen Art für eine sichere Aufbewahrung geeignet ist. Mit der Einlegung gilt das Schriftstück als zugestellt. Zum Nachweis der Zustellung nach den §§ 171, 177 bis 181 ZPO ist eine Urkunde anzufertigen, vergleiche § 182 Abs. 1 S. 1 ZPO. Nach § 182 Abs. 2 Nr. 1, Nr. 4, Nr. 6 bis 8 ZPO muss die Zustellurkunde die Bezeichnung der Person, der zugestellt werden soll, im Fall des § 180 die Angabe des Grundes, der diese Zustellung rechtfertigt, die Bemerkung, dass der Tag der Zustellung auf dem Umschlag, der das zuzustellende Schriftstück enthält, vermerkt ist, den Ort, das Datum und auf Anordnung der Geschäftsstelle auch die Uhrzeit der Zustellung und den Namen, Vornamen und die Unterschrift des Zustellers sowie die Angabe des beauftragten Unternehmens oder der ersuchten Behörde enthalten. Die Angabe vom Inhalt des Briefes – hier die Abmahnung – sowie der Name von Zeugen und deren Unterschrift zum Nachweis ist nach den gesetzlichen Bestimmungen nicht zu benennen, vielmehr lediglich der Grund der Ersatzzustellung, also beispielsweise „Empfänger wurde nicht angetroffen“.

Bei dem Hausmeister handelte es sich nicht um einen berechtigten Personalsachbearbeiter. Aus Sicht des TLfDI wäre es ausreichend gewesen und dadurch ein milderes Mittel, lediglich das Aktenzeichen zu vermerken und den Hausmeister als Zeugen zum Einwurf des Briefes in den Briefkasten der Beschwerdeführerin hinzuzuziehen, ohne dass er dabei Kenntnis über die Abmahnung und den Inhalt erhalten konnte. Dies ergibt sich auch aus § 5 Abs. 1 S. 1 ThürVwZVG. Danach händigt der zustellende Bedienstete bei der Zustellung durch die Behörde das Schriftstück in einem verschlossenen Umschlag dem Empfänger aus. Nach § 5 Abs. 1 S. 2 ThürVwZVG sind dabei der Empfänger, die zustellende Behörde und das Geschäftszeichen auf der Sendung anzugeben, weitere Angaben sind nicht benannt. Damit lag ein Verstoß gegen Art. 5 Abs. 1 Buchstabe f) DS-GVO vor. Der TLfDI sprach gegen die Stadtverwaltung eine Verwarnung nach Art. 58 Abs. 2 Buchstabe b) DS-GVO aus.

2.14 Videokonferenzlösung *Meet/OpenTalk* für die Thüringer Landesverwaltung

Seit dem 1. März 2024 befindet sich die Videokonferenzlösung *Meet/OpenTalk* der Thüringer Landesverwaltung im Produktivbetrieb. Das TFM hat mit dem TLfDI zusammen einen Muster-Auftragsverarbeitungsvertrag erarbeitet, der allen Verantwortlichen und behördeninternen Datenschutzbeauftragten der Thüringer Landesverwaltung zur Verfügung steht.

Die zurückliegende Corona-Pandemie offenbarte, dass zur Digitalisierung der Thüringer Landesverwaltung auch eine sichere sowie datenschutzgerechte Videokonferenzlösung benötigt wird. So stellte das Thüringer Finanzministerium (TFM) am 7. März 2023 in der 28. Sitzung des Arbeitskreises E-Government und IT (AK eGovIT) einen Sachstandsbericht zur neuen Videokonferenzlösung OpenTalk vor. Auch würde ein Auftragsverarbeitungsvertrag (AVV) gemäß Art. 28 Datenschutz-Grundverordnung (DS-GVO) in Vorbereitung sein.
Vorausgegangen waren umfangreiche Tests dieser Videokonferenzlösung in circa 18 Behörden mit etwa 200 Teilnehmern, an denen auch der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) teilnahm. Dabei fungierte der TLfDI zu diesem Zeitpunkt nicht als Datenschutzaufsichtsbehörde, sondern als zu-

künftiger End-Nutzer. Mit dem vorgestellten Sachstandsbericht während der Sitzung wurde mitgeteilt, dass die geplante Videokonferenzlösung als zukünftiges System favorisiert und weiterverfolgt werde. Der erweiterte Probebetrieb für interessierte Dienststellen wurde in Aussicht gestellt, sobald der finale AVV vorliegt. Der TLfDI bot an, den AVV vorab datenschutzrechtlich zu prüfen sowie gemeinsam mit dem Thüringer Landesrechenzentrum (TLRZ) als erste Behörde den AVV-Mustervertrag abzuschließen. Ziel des TLfDI war ein datenschutzkonformes Muster zur Verfügung stellen zu können, da alle Behörden einen AVV abschließen müssen. Außerdem würde ein Muster, das zuvor der TLfDI datenschutzrechtlich geprüft hat und selbst anwendet, alle Verantwortlichen, Personalräte und internen Datenschutzbeauftragte der Behörden bei der eigenen Prüfung entlasten.
Der AVV zwischen dem TLfDI und TLRZ wurde am 16. November 2023 unterzeichnet. Am 29. November 2023 teilte dann das TFM den Ressorts unter anderem mit: „Im Ergebnis wurde ein Muster-AVV mit dem TLfDI erarbeitet und unterzeichnet, der als Mustervereinbarung zwischen den Behörden und dem TLRZ zur Verfügung steht. Insofern wird mit *Meet/OpenTalk* eine datenschutzkonforme Videokonferenzlösung zentral zur Verfügung (DS-GVO-Konformität) bereitgestellt.“ Am 4. März 2024 teilte das TFM mit: „Da nunmehr mit der überwiegenden Zahl der Landesbehörden die Auftragsverarbeitungsverträge (AVV) abgeschlossen sowie die im letzten Jahr veranlassten Stabilitäts- und Performanceverbesserungen erfolgreich getestet wurden, ist der Produktivbetrieb zum 1. März 2024 aufgenommen worden.“
Auch der TLfDI nutzt das System, sofern zur Wahrnehmung seiner gesetzlichen Aufgaben die Durchführung einer Videokonferenz erforderlich ist.

3. Fälle nicht-öffentlicher Bereich

Erfolg Kurve Hand – Pixabay

3.1 Der Konzernbetriebsrat muss nicht alles wissen

Auch bei der Kommunikation zwischen dem Betriebsrat vor Ort und dem Konzernbetriebsrat sind die datenschutzrechtlichen Grundsätze zu beachten. Dem Konzernbetriebsrat sind personenbezogene Daten nur insoweit zu übermitteln, als dies für die Erfüllung seiner Aufgaben erforderlich ist.

Nach seiner Kündigung wandte sich der Mitarbeiter eines Krankenhauses an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Er beschwerte sich darüber, dass der Betriebsratsvorsitzende vor Ort sich mit einer E-Mail an den Konzernbetriebsrat gewandt habe,über die Hintergründe der Kündigung informiert und dabei auch Gesundheitsdaten übermittelt hätte. Den Beschwerdeführer störte vor allem, dass durch die Übermittlung an den Konzernbetriebsrat, dem alle Betriebsräte des gesamten Konzerns angehören, ein sehr großer Kreis von Personen diese Angaben über ihn erhielt.

Im vorliegenden Fall war zunächst zu klären, wer überhaupt Verantwortlicher für die in Rede stehende Datenverarbeitung ist. Es handelte sich hier um eine nicht-öffentliche Stelle, sodass grundsätzlich die Bestimmung des § 79a Satz 2 Betriebsverfassungsgesetz gilt, nach dem der Arbeitgeber Verantwortlicher für die Datenverarbeitung durch den Betriebsrat ist. Zum Zeitpunkt der Versendung der E-Mail galt diese Bestimmung allerdings noch nicht. Bis zum Inkrafttreten der gesetzlichen Regelung hat der TLfDI die Auffassung vertreten, dass der Betriebsrat selbst Verantwortlicher im Sinne von Art. 4 Nr. 7 Datenschutz-Grundverordnung (DS-GVO) ist. Deswegen wandte er sich auch im vorliegenden Fall an den Betriebsrat als Verantwortlichen.
Ein Verstoß gegen den Grundsatz der Integrität und Vertraulichkeit stand nicht im Raum, weil die E-Mail im geschützten konzerninternen Netz versandt worden war. Eine Rechtsgrundlage konnte der Betriebsrat des Klinikums im Anhörungsverfahrens für die Übermittlung der Gesundheitsdaten des Beschwerdeführers nicht nennen.
Nach der DS-GVO ist eine Übermittlung von personenbezogenen Daten nur zulässig, wenn es hierfür eine Rechtsgrundlage gibt, Art. 5 Abs. 1 Buchstabe a) in Verbindung mit Art. 6 DS-GVO. Es war im vorliegenden Fall nicht ersichtlich, welche der in Art. 6 Abs. 1 DS-GVO abschließend genannten Rechtsgrundlagen für die Datenübermittlung an den Konzernbetriebsrat vorgelegen haben könnte. Eine Einwilligung des Betroffenen lag nicht vor, auch war die Übermittlung zur Beendigung des Arbeitsverhältnisses nicht erforderlich. Zwar erlaubt Art. 79a des Betriebsverfassungsgesetzes grundsätzlich die Verarbeitung personenbezogener Daten durch den Betriebsrat. Dies steht jedoch immer unter dem Vorbehalt der Erforderlichkeit der Datenverarbeitung. Nach Art. 58 Abs. 1 Betriebsverfassungsgesetz ist der Konzernbetriebsrat zuständig für die Behandlung von Angelegenheiten, die den Konzern oder mehrere Konzernunternehmen betreffen und nicht durch die einzelnen Gesamtbetriebsräte innerhalb ihrer Unternehmen geregelt werden können. Bei personellen Angelegenheiten, wie im vorliegenden Fall, ist der Konzernbetriebsrat regelmäßig nicht zuständig, da es sich um personelle Einzelmaßnahmen handelt. Zuständig für diese Angelegenheiten sind die einzelnen Betriebsräte vor Ort. Dies gilt selbst im Fall einer Versetzung innerhalb des Konzerns oder aber bei einem Konzernversetzungsvorbehalt im Arbeitsvertrag. Hierüber ist sich auch die Kommentarliteratur einig (vergleiche beispielsweise Boecken/Düwell/Diller/Hanau, Gesamtes Arbeitsrecht, 2. Auflage 2022, Betriebsverfassungsgesetz, § 58, Rn. 7, und Beck

online Arbeitsrecht, 71. Edition, Betriebsverfassungsgesetz, § 58, Rn. 4). Es war nicht erforderlich, den Umstand der Kündigung und die Gründe dafür dem Konzernbetriebsrat mitzuteilen. Dies galt umso mehr, als es sich im vorliegenden Fall um besondere Kategorien von personenbezogenen Daten nach Art. 9 Abs. 1 DS-GVO gehandelt hat. In diesem Fall besteht ein grundsätzliches Verarbeitungsverbot, es sei denn, die Verarbeitung wird nach Art. 9 Abs. 2 DS-GVO erlaubt. Eine derartige Erlaubnis nach den gesetzlichen Vorgaben war ebenfalls nicht erkennbar. Damit hat der TLfDI einen Verstoß gegen Art. 5 Abs. 1 Buchstabe a) DS-GVO festgestellt.
Der TLfDI hat gegenüber dem Betriebsrat des Krankenhauses eine Verwarnung ausgesprochen. Weitere Maßnahmen hielt er nicht für erforderlich, da der Verstoß zum einen nicht mehr andauerte und sowohl der Betriebsrat als auch der Konzernbetriebsrat die Angelegenheit als Anlass dafür genommen haben, weitere Maßnahmen für die Zukunft zu ergreifen. Es wurde festgelegt, dass personenbezogene Daten möglichst anonymisiert werden sollten, sodass ein Rückschluss auf die betroffene Person nicht möglich ist, wenn der Betriebsrat mit dem Konzernbetriebsrat kommuniziert.

3.2 Personaldaten gehören nicht in Chatgruppen

Personaldaten dürfen nur durch Personen verarbeitet werden, die dafür zuständig sind. Der Arbeitsvertrag eines Mitarbeiters hat in einem Gruppenchat nichts zu suchen, selbst dann nicht, wenn er sofort wieder gelöscht wird.

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichte die Beschwerde eines Beschäftigten eines Pflegezentrums. Er gab an, dass sein Arbeitsvertrag über einen Messengerdienst innerhalb eines Gruppenchats in dem Unternehmen veröffentlicht worden war. Der TLfDI wandte sich daraufhin an das Pflegeunternehmen. Der Verantwortliche räumte die Veröffentlichung der ersten Seite des Arbeitsvertrages des Beschwerdeführers im Gruppenchat ein, teilte aber mit, dass dieses Bild sofort wieder gelöscht worden sei.
Hierin sah der TLfDI einen datenschutzrechtlichen Verstoß. Personenbezogene Daten von Beschäftigten dürfen nach Art. 6 Abs. 1 Satz 1 Buchstabe b) Datenschutz-Grundverordnung (DS-GVO) nur für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn

dies für die Entscheidung oder Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung ergebenen Rechte und Pflichten erforderlich ist. Eine solche Erforderlichkeit der Veröffentlichung der ersten Seite des Arbeitsvertrages gegenüber anderen Beschäftigten des Unternehmens wurde nicht gesehen. Es wurde davon ausgegangen, dass auch, wenn der Verantwortliche das Bild sofort wieder gelöscht hatte, die Einsicht durch Dritte stattgefunden hat, da der Beschwerdeführer von seinen Kollegen mittels Screenshot über die Veröffentlichung in der Chatgruppe informiert worden ist. Da der Verstoß bereits geschehen war, jedoch nicht mehr andauerte, sprach der TLfDI gegenüber dem Verantwortlichen eine Verwarnung aus.
Hiergegen legte der Verantwortliche Klage beim Verwaltungsgericht Weimar ein. Dieses wies die Klage ab, weil es die Entscheidung des TLfDI für rechtmäßig hielt. Das Verwaltungsgericht stellte einen Verstoß gegen Art. 5 Abs. 1 Satz 1 Buchstabe a) DS-GVO fest, weil es für die Übersendung des Fotos keine Rechtsgrundlage gegeben hatte. Das Foto sei Dritten zugänglich gemacht worden, ohne dass es hierzu eine gesetzliche Rechtfertigung gegeben hätte. Die Mitglieder der Gruppe waren gegenüber dem Beschwerdeführer Dritte im Sinne von Art. 4 Nr. 10 DS-GVO. Alle Personen oder Stellen, die nicht Verantwortlicher oder Auftragsverarbeiter sind und auch nicht zu den betroffenen Personen gehören, gelten als Dritte. Keine Dritten sind interne Personen, das heißt solche Bedienstete oder Organisationen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder eines Auftragsverarbeiters befugt sind, personenbezogene Daten des Betroffenen zu verarbeiten. Dies war aber im vorliegenden Fall gerade nicht gegeben.
Der Verantwortliche hatte zudem im Laufe des Gerichtsverfahrens angegeben, dass er nicht in seiner Funktion als Geschäftsführer Mitglied der Gruppe sei, sondern dort als Privatperson gehandelt habe. Diesen Vortrag fand das Gericht nicht überzeugend. Ein willentliches Handeln als Privatperson vermag die Verantwortlichkeit des Verantwortlichen nicht aushebeln. Außerdem hatte die Chatgruppe einen rein dienstlichen Charakter und diente ausschließlich dem Zweck, Arbeitsprozesse zu optimieren und intern zu organisieren. Daher war eindeutig klar, dass der Geschäftsführer der Verantwortlichen dort für den Pflegedienst handelte.

Das Gericht bestätigte außerdem die Auffassung, dass eine Verarbeitung in Form einer Offenlegung im Sinne des Art. 4 Nr. 2 siebte Variante DS-GVO vorgelegen hatte, da der Verantwortliche personenbezogene Daten anderen Stellen in der Weise zugänglich gemacht hat, dass diese Kenntnis vom Informationsgehalt der betreffenden Daten erlangen konnten. Auf die tatsächliche Kenntnisnahme der Gruppenmitglieder kam es deswegen nicht an.
Auch § 26 Abs. 1 Satz 1 des Bundesdatenschutzgesetzes (BDSG) rechtfertigte nach Auffassung des Gerichtes die Datenverarbeitung nicht. Die Offenlegung in der Gruppe war nicht erforderlich, was sich bereits aus dem Umstand ergeben habe, dass die Verantwortliche selbst mitgeteilt habe, dass es sich um ein schlichtes Versehen gehandelt hatte.
Das Gericht stellte auch fest, dass der TLfDI sein Ermessen fehlerfrei ausgeübt hat. Er habe lediglich eine Verwarnung ausgesprochen und keine Geldbuße verhängt, sodass sich die Maßnahme bereits aus objektiver Betrachtung heraus als mildestes Mittel gestaltet. Einen Anspruch auf Absehen vom behördlichen Einschreiten habe der Verantwortliche nicht gehabt.
Das Verwaltungsgericht ließ die Berufung gegen seine Entscheidung nicht zu, weswegen sich die Verantwortliche/Klägerin mit einer Zulassungsbeschwerde an das Thüringer Oberverwaltungsgericht (OVG) wandte.
Nach § 124 der Verwaltungsgerichtsordnung ist eine Berufung dann zuzulassen, wenn ernstliche Zweifel an der Richtigkeit des Urteils bestehen, wenn die Rechtssache besondere tatsächliche oder rechtliche Schwierigkeiten aufweist oder wenn die Rechtssache grundsätzliche Bedeutung hat. Hiervon ging der Kläger aus. Das OVG hatte keine ernstlichen Zweifel an der Richtigkeit des Urteils des Verwaltungsgerichts Weimar und lehnte den Antrag auf Zulassung der Berufung ab. Der Verantwortliche hatte in der Begründung des Antrags nunmehr geleugnet, das Foto in den Gruppenchat gestellt zu haben und war der Auffassung, der Sachverhalt sei nicht richtig übermittelt worden. Hierzu legte das OVG dar, dass der Vortrag des Verantwortlichen, die Aufklärung der Umstände insbesondere im Hinblick auf die Herkunft des streitgegenständlichen Fotos durch den TLfDI sei nicht ordentlich erfolgt und der TLfDI habe damit den Mindeststandard für eine Ermittlungstätigkeit nicht genügt, die Richtigkeit des Urteils nicht berühre. Eine Aufklärungsrüge nach § 86 Abs. 1 Satz 1 Verwaltungsgerichtsordnung setze eine substantiierte Darlegung voraus, hinsichtlich

welcher entscheidungserheblicher Umstände Aufklärungsbedarf bestanden hat, welche Aufklärungsmaßnahmen hierfür in Betracht gekommen wären und welche tatsächlichen Feststellungen, die zu einem für den Verantwortlichen günstigeren Ergebnis geführt hätten, voraussichtlich getroffen worden wären. Außerdem hatte der Verantwortliche im Verfahren vor dem Verwaltungsgericht – insbesondere auch in der mündlichen Verhandlung – diese Anhaltspunkte nicht dargelegt. Es wurde kein entsprechender Beweisantrag gestellt. Es reiche nicht, wenn der Verantwortliche pauschal fordere, dass entlastenden Hinweisen hätte nachgegangen werden müssen.
Nach der Entscheidung des Thüringer Oberverwaltungsgerichts ist die Verwarnung des TLfDI nunmehr rechtskräftig.

3.3 Artikel 15 DS-GVO – die Crux mit der Auskunft

Gemäß Art. 12 Abs. 3 DS-GVO ist die/der Verantwortliche verpflichtet, personenbezogene Daten des Betroffenen, die diese/er gemäß Art. 15 DS-GVO anfordert, „… unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags zur Verfügung [zu stellen].“ Der Verantwortliche muss der betroffenen Person die Auskünfte über die Verarbeitung ihrer personenbezogenen Daten nach Art. 15 DS-GVO grundsätzlich innerhalb dieser Frist erteilen, anderenfalls begeht er einen Verstoß gegen Art. 5 Abs. 1 Buchstabe a) DS-GVO, wenn er der betroffenen Person gemäß Art. 12 Abs. 3 Satz 3 DS-GVO auch keine Gründe für eine verspätete Antwort mitteilt.

Im Juni 2024 beschwerte sich eine betroffene Person nach Art. 4 Nummer 1 Datenschutz-Grundverordnung (DS-GVO) in Verbindung mit Art. 77 DS-GVO beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) darüber, dass sie von der Standortniederlassung eines Klinikums, in der sie behandelt wurde, keine Antwort auf ihr im April 2024 gestelltes Auskunftsersuchen nach Art. 15 Abs. 1 DS-GVO zur Verarbeitung ihrer personenbezogenen Daten erhalten habe. Neben ihrem Auskunftsersuchen hatte die betroffene Person vom Verantwortlichen auch die Übersendung ihres ärztlichen Befundberichts an ihre Hausärztin gefordert.
Der TLfDI wandte sich daraufhin auf Grundlage von Art. 58 Abs. 1 Buchstabe a) DS-GVO an das verantwortliche Klinikum und forderte dieses zur Stellungnahme zum Sachverhalt auf. Der TLfDI wies das Klinikum darauf hin, dass der Verantwortliche gemäß Art. 12 Abs. 3

DS-GVO verpflichtet ist, personenbezogene Daten des Betroffenen, die dieser gemäß Art. 15 DS-GVO anfordert, unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags zur Verfügung zu stellen. Sofern dies nicht möglich sein sollte, ist der Verantwortliche gemäß Art. 12 Abs. 3 Satz 3 DS-GVO verpflichtet, dem Betroffenen die Gründe für eine spätere Übermittlung seiner Daten innerhalb der Monatsfrist darzulegen.
Das verantwortliche Klinikum teilte dem TLfDI zum Beschwerdesachverhalt mit, dass es das Auskunftsersuchen gemäß Art. 15 Abs. 1 DS-GVO erhalten und die von der betroffenen Person geforderten ärztlichen Befundberichte bereits Ende April 2024 postalisch an deren Hausärztin übermittelt habe. Das Klinikum legte jedoch nicht dar, ob und wann es das Auskunftsersuchen der betroffenen Person vom April 2024 zur Verarbeitung sämtlicher personenbezogenen Daten an der Standortniederlassung beantwortet hatte.
Auf entsprechende Nachfrage des TLfDI zum nichtbeantworteten Auskunftsersuchen der betroffenen Person teilte das Klinikum mit, dass die betroffene Person bereits im Oktober 2022 schriftlich in die Verarbeitung ihrer personenbezogenen Daten eingewilligt habe. Daher sei das verantwortliche Klinikum davon ausgegangen, dass der betroffenen Person bereits ausreichend klar gewesen sei, welche ihrer personenbezogenen Daten zur medizinischen Behandlung in der Standortniederlassung des Klinikums verarbeitet würden und sich das Auskunftsersuchen insofern nur auf die Übermittlung seines medizinischen Befundberichts an die Hausärztin beziehe. Das verantwortliche Klinikum räumte ein, das Auskunftsersuchen der betroffenen Person irrtümlicherweise nicht so verstanden zu haben, dass die betroffene Person außer den persönlichen Daten ihres ärztlichen Befundberichts auch Auskunft über weitergehende, von der Standortniederlassung verarbeitete Daten wünschte. Dieses Missverständnis sei erst Mitte Juni 2024 geklärt worden. Die geforderten Daten habe das verantwortliche Klinikum Mitte Juni an die betroffene Person übersandt.
Im Hinblick auf die verspätete Beantwortung des Auskunftsersuchens der betroffenen Person vom April 2024 räumte das verantwortliche Klinikum ein, dass dies ein Versehen gewesen sei, das in den Abläufen seiner Standortniederlassung nicht vorkommen sollte. Gemäß Art. 12 Abs. 3 DS-GVO erteilte das verantwortliche Klinikum die Antwort auf das Auskunftsersuchen der betroffenen Person aus April 2024 nicht der datenschutzrechtlich vorgegebenen vierwöchigen

Frist, sondern erst verspätet Mitte Juni 2024. Ebenso hatte das verantwortliche Klinikum der betroffenen Person gemäß Art. 12 Abs. 3 Satz 3 DS-GVO keine Gründe für die verspätete Beantwortung dargelegt. Damit verstieß das Klinikum gegen Art. 5 Abs. 1 DS-GVO. Nach Art. 5 Abs. 1 Buchstabe a) DS-GVO müssen personenbezogene Daten in einer für die betroffene Person rechtmäßigen, transparenten und für die betroffene Person nachvollziehbaren Weise verarbeitet werden (Transparenzgebot).
Das verantwortliche Klinikum teilte dem TLfDI mit, dass die organisatorischen Abläufe, die zur verspäteten Beantwortung des Auskunftsersuchens der betroffenen Person geführt hätten, bereits intern geprüft und geändert worden seien, um sicherzustellen, dass Auskunftsersuchen zur Verarbeitung personenbezogener Daten im Sinne von Art. 15 Abs. 1 DS-GVO zukünftig nicht unbearbeitet blieben.
Ende August 2024 sprach der TLfDI gegenüber dem verantwortlichen Klinikum wegen der gemäß Art. 15 Abs. 1 DS-GVO in Verbindung mit Art. 12 Abs. 3 DS-GVO verspätet erteilten Auskunft eine Verwarnung nach Art. 58 Abs. 2 Buchstabe b) DS-GVO aus, die das Klinikum auch akzeptierte.

3.4 Wenn die Patientenquittung Fragen aufwirft – wo „Notfalldatensatz“ draufsteht, ist nicht immer ein „Notfalldatensatz“ drin

Gemäß Art. 5 Abs. 1 Buchstabe a) DS-GVO müssen personenbezogene Daten transparent und auf rechtmäßige Weise verarbeitet werden. Nach Art. 6 Abs. 1 Satz 1 Buchstabe a) DS-GVO in Verbindung mit Art. 9 Abs. 2 Buchstabe a) DS-GVO ist die Verarbeitung personenbezogener Daten und besonderer Kategorien von personenbezogenen Daten auf Grundlage einer Einwilligung der betroffenen Person nach Art. 7 DS-GVO zulässig. Gemäß § 358 Abs. 3 Nummer 1 Sozialgesetzbuch V (SGB) können Ärzte notfallrelevante Gesundheitsdaten mit Einwilligung des Patienten direkt auf der elektronischen Gesundheitskarte speichern, sodass diese Daten anderen Ärzten in einem medizinischen Notfall sofort zur Verfügung stehen.

Im Berichtszeitraum beschwerte sich eine betroffene Person beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) darüber, dass die medizinische Fachabteilung ei-

ner Klinik und mehrere niedergelassene Ärzte, bei denen die Beschwerdeführerin behandelt worden war, einen sogenannten Notfalldatensatz über sie angelegt hätten, obwohl die Beschwerdeführerin hierzu keine Einwilligung erteilt hatte. Dass ein Notfalldatensatz über sie angelegt wurde, habe die Beschwerdeführerin regelmäßig aus den Abrechnungen auf den Patientenquittungen ihrer Krankenkasse entnommen und dem TLfDI eine ihr vorliegende Patientenquittung übersandt. Auf dieser Patientenquittung war unter „Gebührenordnungsnummer 01641“ der Begriff „Notfalldatensatz“ vermerkt.
Bei Gesundheitsdaten handelt es sich um besondere Kategorien von Daten im Sinne von Art. 9 Abs. 1 Datenschutz-Grundverordnung (DS-GVO), deren Verarbeitung grundsätzlich unzulässig ist. Nach Art. 6 Abs. 1 Satz 1 Buchstabe a) DS-GVO in Verbindung mit Art. 9 Abs. 2 Buchstabe a) DS-GVO und Art. 7 DS-GVO ist die Verarbeitung dieser Daten auf Grundlage einer Einwilligung zulässig. Weiterhin ist die Verarbeitung personenbezogener Gesundheitsdaten nach Art. 6 Abs. 1 Satz 1 Buchstabe c) DS-GVO in Verbindung mit Art. 9 Abs. 2 Buchstabe g) DS-GVO zulässig, wenn dies zur Erfüllung einer rechtlichen Verpflichtung, der der Verantwortliche unterliegt, erforderlich ist, das heißt, wenn die Verarbeitung dieser Daten durch eine (unionsrechtliche oder nationalstaatliche) Rechtsnorm geregelt beziehungsweise gefordert ist.
Zur Prüfung der Beschwerde wandte sich der TLfDI zunächst mit einem Auskunftsersuchen an sämtliche von der Beschwerdeführerin genannten Verantwortlichen und forderte diese auf, zum Sachverhalt Stellung zu nehmen. Alle Verantwortlichen gaben an, keinen Notfalldatensatz über die Beschwerdeführerin angelegt zu haben und konnten entsprechende Angaben auf den der Beschwerdeführerin vorliegenden Patientenunterlagen/Abrechnungen nicht erklären. Daraufhin wandte sich der TLfDI an die Kassenärztliche Vereinigung Thüringen (KVT) und erkundigte sich über die konkrete Bedeutung und Interpretation der (Abrechnungs-) Angaben auf Patientenquittungen.
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. Die Gebührenordnungsnummer 01641 mit dem Zusatz „Notfalldatensatz“ nimmt die KVT, um die technischen Voraussetzungen einzurichten, die zur Anlage eines Notfalldatensatzes erforderlich sind, also eine Art

„technische Aufwandspauschale“. Weiterhin teilte die KVT dem TLfDI mit, dass viele Ärzte gar nicht wüssten, dass diese Abrechnungsposition von der KVT den Abrechnungen hinzugefügt werde. Insofern können betroffene Personen nur aufgrund dieser Angabe auf der Patientenquittung nicht davon ausgehen, dass tatsächlich ein Notfalldatensatz von ihnen angelegt wurde.

Das Notfalldatenmanagement (NFDM) ist eine medizinische Anwendung der Telematikinfrastruktur (TI). Es wurde mit § 291a Abs. 3 Nr. 1 Sozialgesetzbuch V als Anwendungsmöglichkeit der elektronischen Gesundheitskarte (eGK) eingeführt. Der sogenannte Notfalldatensatz enthält Informationen zu (lebens-)wichtigen Diagnosen, zur Medikation oder zu Allergien und Arzneimittel-Unverträglichkeiten. Vertragsärzte der Krankenkassen sind verpflichtet, die technischen Voraussetzungen für die Nutzung des Notfalldatenmanagements in ihren Praxen zu schaffen. Ärzte müssen dann den Notfalldatensatz elektronisch anlegen, lesen und aktualisieren. Hierfür benötigen sie einen Anschluss an die Telematikinfrastruktur mit einem sogenannten E-Health-Konnektor (verfügbar seit Sommer 2020) und ein entsprechendes Modul in ihrem Praxisverwaltungssystem.

Die Anlage des Notfalldatensatzes auf der elektronischen Gesundheitskarte ist – anders als die Nutzung der elektronischen Gesundheitskarte selbst – für Patienten freiwillig. Gemäß Art. 6 Abs. 1 Satz 1 Buchstabe d) DS-GVO in Verbindung mit Art. 9 Abs. 2 Buchstabe c) DS-GVO ist die Verarbeitung dieser medizinischen Notfalldaten, sofern sie auf der elektronischen Gesundheitskarte angelegt wurden, zum Schutz lebenswichtiger Interessen der betroffenen Person zulässig. Unabhängig von der Notfallrettung können die Notfalldaten aber auch zur Unterstützung bei der Anamnese im Rahmen einer „normalen“ medizinischen Behandlung von Bedeutung sein. Jedoch müssen Patienten für diese Datenzugriffe im Rahmen einer „normalen“ Behandlung – anders als in Notfallsituationen – dem Zugriff erst zustimmen, das heißt datenschutzrechtlich einwilligen, dass der behandelnde Arzt die Daten lesen darf (Art. 6 Abs. 1 Satz 1 Buchstabe a) DS-GVO in Verbindung mit Art. 9 Abs. 2 Buchstabe a) DS-GVO und Art. 7 Abs. 1 DS-GVO).

Die Prüfung der Beschwerde durch den TLfDI ergab, dass keiner der Verantwortlichen einen Notfalldatensatz über die Beschwerdeführerin angelegt oder eine entsprechende EBM-Nummer (Einheitlicher Bewertungsmaßstab bei der vertragsärztlichen Abrechnung) abgerechnet hatte. Somit konnte der TLfDI keinen Verstoß gegen den Schutz von

personenbezogenen Daten durch die medizinischen Einrichtungen und Arztpraxen feststellen.

3.5 Keine Meldepflicht für Wildkameras

Wildkameras müssen dem TLfDI vom Verantwortlichen nicht gemeldet werden, ebenso wenig wie herkömmliche Kameras. Es obliegt dem Verantwortlichen selbst, für einen datenschutzkonformen Betrieb der Kamera nach den Regelungen der DS-GVO Sorge zu tragen.

Beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) gehen immer wieder Anfragen von Jägern und Waldbesitzern ein, ob eine Meldepflicht für das Betreiben von Wildkameras im Wald besteht. Vor der Einführung der Datenschutz-Grundverordnung (DS-GVO) am 25. Mai 2018 mussten nicht-öffentliche Stellen nach der alten Fassung des § 4d Abs. 1 Bundestatenschutzgesetz (BDSG a. F.) grundsätzlich die zuständige Datenschutzbehörde über die Durchführung einer Videoüberwachung informieren. Mit Inkrafttreten der DS-GVO und der Aufhebung des § 4d BDSG a. F. ist diese Meldepflicht entfallen. Es finden sich jedoch im Internet noch immer Meldungen und Dokumente, die auf diese veraltete Rechtslage verweisen.
Nach aktuell geltendem Recht obliegt es gemäß Art. 5 Abs. 2 DS-GVO dem verantwortlichen Betreiber einer (Wild-)Kamera, die Einhaltung der datenschutzrechtlichen Bestimmungen nachweisen zu können. Die Zulässigkeit des Betriebs einer Videokamera durch nicht-öffentliche Stellen richtet sich nach den Vorgaben der Datenschutz-Grundverordnung, da durch die Kamera eine Verarbeitung von personenbezogenen Daten nach Art. 2 Abs. 1 in Verbindung mit Art. 4 Nr. 1 und 2 DS-GVO vorgenommen wird.
Die Datenverarbeitung muss den Grundsätzen von Art. 5 Abs. 1 DS-GVO entsprechen, insbesondere dem Grundsatz der Rechtmäßigkeit der Datenverarbeitung. Rechtmäßig ist eine Datenverarbeitung unter einer der in Art. 6 Abs. 1 Satz 1 Buchstabe a) bis f) DS-GVO genannten Voraussetzungen. Werden Flächen in der freien Landschaft (Feldflur und Wald) durch Privatpersonen überwacht, ist regelmäßig Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO anzuwenden.
Nach Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO muss die Überwachung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich sein. Die Interessen oder Grundrechte

und Grundfreiheiten von betroffenen Personen, die den Schutz personenbezogener Daten erfordern, dürfen dabei nicht überwiegen. Es ist eine Interessenabwägung mit den Rechten der Betroffenen der Datenverarbeitung, also aller Personen, die in den Erfassungsbereich der Kamera geraten, vorzunehmen.
Der Verantwortliche muss für jede eingesetzte Kamera einen konkreten Zweck für die Überwachungsmaßnahme festlegen. Zudem muss die Überwachung auch erforderlich sein.
So kann etwa die Jägerschaft ein berechtigtes Interesse daran haben, Kirr- oder Futterstellen zu überwachen. Es gilt dabei zu beachten, dass Bereiche, die sich in unmittelbarer Nähe zu einem Waldweg, einer Grillstelle oder einem Spielplatz befinden, nicht überwacht werden dürfen. Vor dem Einsatz einer (Wild-)Kamera ist immer zu prüfen, ob mildere Mittel (zum Beispiel Wilduhren) eingesetzt werden können.
Im Rahmen der vorzunehmenden Interessenabwägung sind weiterhin die Schutzinteressen des Verantwortlichen, mit dem Recht auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 Grundgesetz der Betroffenen abzuwägen. Nach § 6 Abs. 1 Thüringer Waldgesetz ist das Betreten des Waldes zum Zwecke der naturverträglichen Erholung jedem gestattet. Damit handelt es sich um einen öffentlich zugänglichen Raum, sofern kein erkennbares Betretungsverbot besteht. Hier besteht die Gefahr, dass unbeteiligte Personen anlasslos von der Kamera erfasst werden.
Sofern die Überwachung durch private Personen ausschließlich im eigenen Interesse erfolgt, überwiegen regelmäßig die Interessen der Betroffenen daran, nicht überwacht zu werden. Anders verhält es sich bei Überwachungsmaßnahmen im Zusammenhang mit der Ausübung der Jagd, da hier die Interessen des Verantwortlichen überwiegen können. Die Wildkamera muss aber so ausgerichtet sein, dass die Aufnahme von Menschen äußerst unwahrscheinlich ist und mit allen verfügbaren Mitteln vom Verantwortlichen verhindert wird.
Dies kann durch Anwendung folgender Vorgaben erreicht werden:

- Die Kamera wird maximal in einer Höhe von einem Meter angebracht und ist direkt auf den Waldboden oder eine Futterstelle ausgerichtet.
- Es werden ausschließlich Einzelbilder mit einigen Sekunden Abstand aufgenommen und keine Videos.
- Die Auflösung der Kamera sollte möglichst gering gewählt sein.
- Sollen Tiere nachts überwacht werden, muss die Kamera tagsüber ausgeschaltet werden.

- Der überwachte Bereich sollte für Waldbesucher erkennbar mit einem Betretungsverbot ausgeschildert sein.
- Es muss auf die Kamera hingewiesen werden (Art. 13 DS-GVO). Ein Muster für ein Hinweisschild stellt der TLfDI auf seiner Internetseite bereit, siehe https://www.tlfdi.de/fileadmin/tlfdi/datenschutz/video/anlage1_hinweisschild_final.pdf.
- Gespeicherte Daten müssen unverzüglich gelöscht werden, wenn sie zur Erreichung des Zwecks nicht weiter erforderlich sind. In der Regel gilt eine maximale Speicherdauer von 72 Stunden.

Ein Verstoß gegen die datenschutzrechtlichen Bestimmungen kann nach Art. 83 Abs. 5 DS-GVO mit einem Bußgeld von bis zu 20.000.000 Euro geahndet werden.
Weitergehende Informationen zur Durchführung einer Videoüberwachung durch nicht-öffentliche Stellen sind in der entsprechenden Orientierungshilfe der Datenschutzkonferenz insbesondere unter Punkt 5.8. Wildkameras, abrufbar unter https://www.datenschutzkonferenz-online.de/media/oh/20200903_oh_v%C3%BC_dsk.pdf zu finden.

3.6 Veröffentlichung personenbezogener Daten auf einem Onlinebewertungsportal

Die Veröffentlichung der privaten Anschrift, Rufnummer und E-Mail-Adresse ohne Einwilligung der betroffenen Person ist im Rahmen der Reaktion auf eine Negativbewertung bei einem Onlinebewertungsportal nicht erforderlich und damit unrechtmäßig. Für eine solche Verarbeitung der personenbezogenen Daten der Person, die die Bewertung vorgenommen hat, ist keine Rechtsgrundlage gegeben.

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) erhielt im Berichtszeitraum eine Beschwerde dahingehend, dass persönliche Daten des Beschwerdeführers auf einem Onlinebewertungsportal durch einen Onlineshop veröffentlicht wurden, so dass jeder diese Daten einsehen konnte. Hintergrund war, dass der Beschwerdeführer eine negative Bewertung auf einem Bewertungsportal zu dem Onlineshop verfasst hatte. Daraufhin reagierte das Unternehmen, das den Onlineshop betrieb, auf die Negativbewertung und stellte das an den Beschwerdeführer gerichtete Antwort-

schreiben auf der Bewertungsplattform ein. Das Schreiben enthielt unter anderem den Namen, die private Anschrift, E-Mail-Adresse und Mobilfunknummer des Beschwerdeführers.
Bei der Veröffentlichung dieser Daten auf der Plattform handelt es sich um eine Verarbeitung im Sinne des Art. 4 Abs. 2 Datenschutz-Grundverordnung (DS-GVO). Nach Art. 5 Abs. 1 Buchstabe a) DS-GVO müssen personenbezogene Daten auf rechtmäßige Weise verarbeitet werden. Aus Art. 6 Abs. 1 Satz 1 DS-GVO ergibt sich, dass nur unter den dort genannten Bedingungen eine Datenverarbeitung zulässig ist.
Eine Einwilligung nach Art. 6 Abs. 1 Satz 1 Buchstabe a) DS-GVO wurde durch den Beschwerdeführer nicht erteilt. Die Verarbeitung konnte hier auch nicht auf Art. 6 Abs. 1 Satz 1 Buchstabe b) DS-GVO gestützt werden, da die hier erfolgte Verarbeitung nicht zur Erfüllung des Kaufvertrags mit dem Beschwerdeführer erforderlich war. Allenfalls kam vorliegend Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO als Rechtsgrundlage in Betracht. 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.
Das Unternehmen hatte vorliegend zwar ein berechtigtes Interesse daran, dass im Rahmen der Negativbewertung eine Gegendarstellung vorgenommen werden kann. Hierfür ist es jedoch nicht erforderlich, die Anschrift, die private Mobilfunknummer, sowie die E-Mail-Adresse des Beschwerdeführers zu veröffentlichen. Daneben überwiegen hier auch die Interessen des Beschwerdeführers, da die Daten für jeden einsehbar waren und somit Tür und Tor für etwaige Belästigungen und unberechtigte Nutzungen seiner Daten geöffnet wurde.
Die Verarbeitung erfolgte daher unrechtmäßig. Der Beschwerdeführer hatte zwischenzeitlich erneut eine negative Bewertung zu dem Unternehmen abgegeben und darin mitgeteilt, dass er sich hinsichtlich des Datenschutzverstoßes an die zuständige Behörde gewandt hatte. Das Unternehmen entfernte daher noch vor dem ersten Anschreiben des TLfDI die Daten aus der Bewertung. Dennoch erließ der TLfDI aufgrund des gravierenden Verstoßes einen kostenpflichtigen Bescheid nach Art. 58 Abs. 2 DS-GVO, der der Aufsichtsbehörde erlaubt, den Verantwortlichen zu verwarnen, wenn er mit Verarbeitungsvorgängen gegen die Datenschutz-Grundverordnung verstoßen hat.

3.7 Veröffentlichung einer geschäftlichen E-Mail auf einer Facebook-Seite

Die Datenschutz-Grundverordnung (DS-GVO) unterscheidet nicht zwischen personenbezogenen Daten privat oder geschäftlich auftretender natürlicher Personen.

Durch eine Mitteilung wurde dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) bekannt, dass ein in Thüringen ansässiges Unternehmen auf seiner öffentlichen Facebook-Seite einen Beitrag veröffentlicht hatte, auf dem mehrere Bildschirmfotos vom elektronischen Schriftverkehr mit Geschäftspartnern des Unternehmens zu sehen waren, um diese verächtlich zu machen. Hierunter befand sich auch das Bildschirmfoto einer E-Mail, in der der vollständige Name und die Mobilfunknummer des damaligen Geschäftsführers eines Partnerunternehmens erkennbar waren. Der von der Datenverarbeitung betroffene Geschäftsführer des Partnerunternehmens hatte in die Veröffentlichung seiner personenbezogenen Daten nicht eingewilligt.
Sodann wurde beim TLfDI ein Ordnungswidrigkeitenverfahren gegen das Unternehmen eingeleitet, das den Beitrag auf seiner Facebook-Seite veröffentlicht hatte.
Im Rahmen der Anhörung durch den TLfDI gemäß § 55 Ordnungswidrigkeitengesetz § 163a Abs. 1 Strafprozessordnung erklärte der Geschäftsführer des im Bußgeldverfahren betroffenen Unternehmens, dass ihm hinsichtlich der Veröffentlichung des Bildschirmfotos der E-Mail nicht bewusst gewesen sei, dass er die personenbezogenen Daten des Geschäftsführers des Partnerunternehmens hätte unkenntlich machen müssen, da es sich hierbei um dessen E-Mail-Signatur gehandelt habe und die Daten im Rahmen der geschäftlichen Tätigkeit ohnehin im Umlauf seien. Darüber hinaus entschuldigte sich der Geschäftsführer des betroffenen Unternehmens und kündigte an, den Beitrag von der Facebook-Seite zu löschen.
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 das betroffene Unternehmen mit der Veröffentlichung des Bildschirmfotos der E-Mail personenbezogene Daten im Sinne des Art. 4

Nr. 1 DS-GVO durch Übermittlung offengelegt und damit im Sinne des Art. 4 Nr. 2 DS-GVO verarbeitet. 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. Vorliegend konnte die Verarbeitung der personenbezogenen Daten nicht auf eine Einwilligung nach Art. 6 Abs. 1 Satz 1 Buchstabe a) DS-GVO gestützt werden. Hierzu wäre es erforderlich gewesen, dass der Geschäftsführer des Partnerunternehmens vorab und in Kenntnis des Zweckes der Verarbeitung in die Offenlegung seiner Daten eingewilligt hätte. Eine solche Einwilligung lag dem betroffenen Unternehmen jedoch nicht vor. Die Einlassungen des Geschäftsführers des betroffenen Unternehmens im Rahmen der Anhörung durch den TLfDI schlossen die Annahme des Vorliegens weiterer Erlaubnistatbestände gemäß Art. 6 Abs. 1 DS-GVO aus. Auch waren solche nach Aktenlage nicht erkennbar.

Aufgrund dieser Sach- und Rechtslage erging ein Bußgeldbescheid gegen das betroffene Unternehmen. Bei der Bemessung der Geldbuße gemäß Art. 83 Abs. 2 DS-GVO wurde durch den TLfDI ein vorsätzliches Handeln berücksichtigt. Mildernd wirkte sich demgegenüber aus, dass sich der Geschäftsführer des betroffenen Unternehmens für die Veröffentlichung des Bildschirmfotos der hier relevanten E-Mail entschuldigt hatte. Verschärfend musste jedoch berücksichtigt werden, dass der Beitrag auf der Facebook-Seite des betroffenen Unternehmens zum Zeitpunkt des Erlasses des Bußgeldbescheides entgegen der Ankündigung im Rahmen der Anhörung nicht gelöscht, sondern noch immer öffentlich abrufbar war.

Das betroffene Unternehmen legte gegen den Bußgeldbescheid form- und fristgerecht Einspruch ein. Der später mandatierte Verteidiger des betroffenen Unternehmens stützte den Einspruch im Wesentlichen auf die Rechtsauffassung, dass die Veröffentlichung der personenbezogenen Daten des Geschäftsführers des Partnerunternehmens rechtmäßig erfolgt sei, da dieser vorliegend nicht als natürliche Person gehandelt und zudem in einer geschäftlichen Beziehung zum betroffenen Unternehmen gestanden habe. Zudem habe der Geschäftsführer des Partnerunternehmens seine personenbezogenen Daten selbst zum Zwecke einer direkten geschäftlichen Kontaktaufnahme beispielsweise im öffentlichen Verkehrsraum öffentlich gemacht. Aus diesem allgemeinen „Veröffentlichungsverhalten“ sei daher auch auf eine konkludente

Einwilligung zur Verarbeitung seiner Daten durch das betroffene Unternehmen zu schließen. Das zuständige Amtsgericht Erfurt verwarf den Einspruch, erhöhte die Geldbuße im unteren vierstelligen Bereich um 1.000 Euro und folgte insoweit der Rechtsauffassung des TLfDI. Demnach handelt es sich bei den Angaben zum vollständigen Namen und der Mobilfunknummer des Geschäftsführers des Partnerunternehmens um personenbezogene Daten, da die DS-GVO nicht zwischen personenbezogenen Daten privat und geschäftlich auftretender natürlicher Personen unterscheidet, sodass sowohl Privatperson wie auch Angestellte, Selbständige oder sonst wie beruflich Handelnde hinsichtlich ihrer personenbezogenen Daten, zu denen auch dienstliche Telefonnummern zählen, durch die DS-GVO geschützt werden. Unschädlich ist es auch, wenn der Geschäftsführer des Partnerunternehmens seine personenbezogenen Daten selbst öffentlich gemacht hat, denn die DS-GVO schützt auch diese personenbezogenen Daten im Rahmen einer (Weiter-) Verarbeitung durch Dritte. Natürliche Personen sind auch und gerade in der Öffentlichkeit „privat“, denn die DS-GVO schützt nicht allein „Privatheit“ oder „Abgeschiedenheit“ im Sinn eines „Allein-gelassen-Werdens“, sondern in einem weiteren Verständnis die informationelle Selbstbestimmung und Individualität des Einzelnen in all ihren Facetten und ist nicht auf die der Öffentlichkeit entzogenen Sachverhalte beschränkt. Soweit der Verteidiger die vermeintliche Rechtmäßigkeit der Datenverarbeitung schließlich auf die Geschäftsbeziehungen zwischen dem betroffenen Unternehmen und dem Partnerunternehmen zu stützen versuchte, käme eine Verarbeitung in Betracht, die zur Erfüllung eines Vertrages nach Art. 6 Abs. 1 Satz 1 Buchstabe b) DS-GVO erforderlich war. Ob eine Verarbeitung personenbezogener Daten zur Erfüllung eines Vertrags erforderlich ist, hängt davon ab, ob ein unmittelbarer sachlicher Zusammenhang zwischen der beabsichtigten Datenverarbeitung und dem konkreten Zweck des rechtsgeschäftlichen Schuldverhältnisses besteht. Hier lag jedoch lediglich eine vertragliche Beziehung zwischen dem betroffenen Unternehmen und dem Partnerunternehmen vor, sodass bereits unter diesem Aspekt eine rechtmäßige Datenverarbeitung nicht in Betracht kam. Aber selbst wenn man eine vertragliche Beziehung zwischen dem betroffenen Unternehmen und dem Geschäftsführer des Partnerunternehmens selbst bejahen würde, wäre die Veröffentlichung einer geschäftlichen E-Mail auf der Facebook-Seite des betroffenen Unternehmens unter keinen Umständen zur Erfüllung des

Vertrages erforderlich, da die Veröffentlichung ausschließlich der Verächtlichmachung diente.
Die inzwischen rechtskräftige Geldbuße ist damit zugleich wirksam, verhältnismäßig wie ausreichend abschreckend für die Zukunft.

3.8 Videoaufnahme durch MA in Pflegeeinrichtung zu privaten Zwecken

Die sogenannte „Haushaltsausnahme“ gemäß Art. 2 Abs. 2 Buchstabe c) Datenschutz-Grundverordnung ist mit der Verwendung des Begriffs „ausschließlich“ eng auszulegen und erlaubt nicht die Vermischung privater und wirtschaftlicher beziehungsweise dienstlicher Tätigkeiten. Soweit Mitarbeiter einer Pflegeeinrichtung mit ihren privaten Mobiltelefonen Videoaufnahmen von Patienten anfertigen und an Dritte übermitteln, unterfallen diese Datenverarbeitungen dem sachlichen Anwendungsbereich der Datenschutz-Grundverordnung.

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) erhielt durch die Mitteilung eines Unternehmens, das im Bereich der Kranken- und Altenpflege tätig ist, Kenntnis davon, dass eine Mitarbeiterin des Unternehmens während einer Nachtschicht aus privaten Motiven mit ihrem Mobiltelefon eine Videoaufnahme einer Patientin angefertigt hatte. Auf dem Video ist zu erkennen, wie die Patientin hilflos und desorientiert durch die Räumlichkeiten der Pflegeeinrichtung irrt, während die Mitarbeiterin des Unternehmens hörbar abfällige Bemerkungen macht und über die Patientin lacht. Im Anschluss wurde die Videoaufnahme durch die Mitarbeiterin über den Instant-Messaging-Dienst *WhatsApp* an zwei weitere Personen übermittelt.
Nach Eingang der Mitteilung des Unternehmens wurde beim TLfDI umgehend ein Ordnungswidrigkeitenverfahren gegen die betroffene Mitarbeiterin eingeleitet, die die Aufnahmen gemacht hatte. Im Rahmen der Anhörung gemäß § 55 Ordnungswidrigkeitengesetz, § 163a Abs. 1 Strafprozessordnung erklärte sie, die Videoaufnahme angefertigt zu haben, um ihre Kollegen über den Gesundheitszustand und das Verhalten der von der Datenverarbeitung betroffenen Patientin zu informieren.
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 die betroffene Mitarbeiterin mit der Anfertigung und Speicherung der Videoaufnahme sowie deren späteren Versand an Dritte personenbezogene Daten im Sinne des Art. 4 Nr. 1 DS-GVO erhoben und durch Übermittlung gegenüber Dritten offengelegt und damit im Sinne des Art. 4 Nr. 2 DS-GVO verarbeitet. Hierbei war trotz der Tatsache, dass die Anfertigung und der Versand der Videoaufnahme mit dem privaten Mobiltelefon der Betroffenen erfolgten, der sachliche Anwendungsbereich der Datenschutz-Grundverordnung eröffnet. Zwar findet gemäß Art. 2 Abs. 2 Buchstabe c) DS-GVO die Verordnung keine Anwendung auf die Verarbeitung personenbezogener Daten zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten. Allerdings ist der Begriff „ausschließlich“ eng auszulegen und erlaubt nicht die Vermischung privater und wirtschaftlicher beziehungsweise dienstlicher Tätigkeiten. Da die Betroffene die Videoaufnahme im Rahmen ihrer beruflichen Tätigkeit als Mitarbeiterin der Pflegeeinrichtung angefertigt hatte, stand die privat erfolgte Anfertigung und Speicherung im Zusammenhang mit ihrer dienstlichen Tätigkeit, weshalb die sogenannte „Haushaltsausnahme“ gemäß Art. 2 Abs. 2 Buchstabe c) DS-GVO nicht zur Anwendung gelangte. Auch war in Bezug auf die Datenverarbeitungen nicht etwa das Unternehmen, das die Pflegeeinrichtung betreibt, sondern die Betroffene als Verantwortliche gemäß Art. 4 Nr. 7 DS-GVO anzusehen. Vorliegend hatte das Unternehmen seinen Mitarbeitern durch entsprechende Dienstanweisung nachweislich untersagt, Foto- und Videoaufnahmen von Patienten anzufertigen. Auch waren auf der Videoaufnahme abfällige Bemerkungen der Betroffenen über die Patientin sowie Gelächter zu hören, weshalb von rein privaten Motiven hinsichtlich der Anfertigung und des Versands der Videoaufnahme auszugehen war. Dementsprechend entschied ausschließlich die Betroffene über die Zwecke und Mittel der Verarbeitung der personenbezogenen Daten der Patientin. Diese Datenverarbeitungen erfolgten 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. Vorliegend konnte die Verarbeitung der personenbezogenen Daten nicht auf eine Einwilligung nach Art. 6 Abs. 1 Satz 1 Buchstabe a) DS-GVO gestützt werden. Hierzu wäre es erforderlich gewesen, dass die Patientin vorab und in Kenntnis des Zweckes in die

Verarbeitung eingewilligt hätte. Eine solche Einwilligung lag der Betroffenen jedoch nicht vor. Die Zulässigkeit der Datenverarbeitung ergab sich auch nicht aus dem einzig noch in Betracht zu ziehenden Art. 6 Abs. 1 S. 1 Buchstabe f) DS-GVO, da bereits aufgrund der privaten Motive der Betroffenen das Vorliegen eines berechtigten Interesses zweifelhaft war. In jedem Fall überwogen jedoch die schützenswerten Interessen der von der Datenverarbeitung betroffenen Patientin deutlich, die auf ihrer Beziehung zu dem Verantwortlichen beruhen. Vorliegend musste die Patientin nicht damit rechnen, dass sie während ihres Aufenthaltes in einer Pflegeeinrichtung, die aufgrund des gesundheitlichen Zustandes der dort befindlichen Patienten einen besonders geschützter Raum darstellt, von dem dort arbeitenden Pflegepersonal zu rein privaten Zwecken gefilmt wird. Im Ergebnis trat daher ein gegebenenfalls bestehendes berechtigtes Interesse hinsichtlich der Datenverarbeitung hinter die schützenswerten Interessen der Patientin zurück.
Aufgrund dieser Sach- und Rechtslage erging ein Bußgeldbescheid gegen die Betroffene.
Bei der Bemessung der Geldbuße wurde ein vorsätzliches Handeln berücksichtigt. Auch die Eingriffsintensität in die Persönlichkeitsrechte der Patientin wirkte sich zu Lasten der Betroffenen aus, da diese die personenbezogenen Daten unter Ausnutzung ihrer beruflichen Stellung erlangt hatte und sich die von der Datenverarbeitung betroffene Person zum Tatzeitpunkt in einem besonders geschützten Raum aufhielt und darüber hinaus desorientiert und hilflos war. Mildernd wurde demgegenüber berücksichtigt, dass die Betroffene ihr Bedauern über die Tat zum Ausdruck gebracht hatte. Die festgesetzte Geldbuße im unteren vierstelligen Bereich war damit zugleich wirksam, verhältnismäßig wie ausreichend abschreckend für die Zukunft.

3.9 Videoüberwachung auf dem Friedhof

Die Videoüberwachung auf einem Friedhof ist in der Regel als unzulässig zu bewerten, da es sich um einen Ort handelt, an dem Besucher ein hohes Maß an Privatsphäre erwarten dürfen. Eine solche Überwachung darf nicht den Kernbereich der privaten Lebensgestaltung, der auch den Besuch eines Friedhofs umfasst, unzulässig beeinträchtigen. Die Videoüberwachung ist nur dann zulässig, wenn sie rechtmäßig,

zwingend erforderlich und zweckgebunden ist und keine weniger eingriffsintensiven Mittel zur Erreichung des beabsichtigten Zwecks zur Verfügung stehen.

Im Berichtszeitraum erlangte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) Kenntnis darüber, dass ein Bürger eine Wildkamera versteckt in einem Strauch auf einem Friedhof nahe dem Grab seines verstorbenen Angehörigen installierte. Die Kamera war so ausgerichtet, dass nicht nur das Grab, sondern auch umliegende Gräber sowie die dazwischen befindlichen Wege erfasst wurden. Zusätzlich war die Kamera so konfiguriert, dass sie bei Bewegungen im Erfassungsbereich sowohl Video- als auch Tonaufnahmen anfertigte.
Der Betreiber begründete die Installation mit wiederkehrenden Beschädigungen und Entwendungen am Grab seines Angehörigen. Ziel war es, potenzielle Täter zu identifizieren und Beweise zu sichern.
Der TLfDI prüfte vorliegend, ob der Betreiber gegen die Grundsätze für die Verarbeitung, einschließlich der Bedingungen für die Einwilligung, gemäß den Artikeln 5, 6, 7 und 9 Datenschutz-Grundverordnung (DS-GVO) verstoßen hatte.
Durch die Anfertigung von Video- und Tonaufnahmen kam es zur Verarbeitung von personenbezogenen Daten im Sinne des Art. 4 Nr. 2 DS-GVO. So konnte der Betreiber mithilfe seiner Kamera Angaben über persönliche und sachliche Verhältnisse einzelner Personen erfassen, die nicht allgemein zugänglich waren. Hierzu zählten Angaben darüber, wo sich eine bestimmte oder bestimmbare Person aufhält, mit wem sie sich traf und worüber sie sich unterhielt.
Nach Art. 5 Abs. 1 Buchstabe a) DS-GVO müssen personenbezogene Daten auf rechtmäßige Weise verarbeitet werden. Die Rechtmäßigkeit der Verarbeitung richtet sich nach Art. 6 Abs. 1 DS-GVO. Nur unter den dort genannten Bedingungen ist eine Datenverarbeitung zulässig. Es handelt sich somit um ein Verbot mit Erlaubnisvorbehalt. Eine Einwilligung aller betroffenen Personen nach Art. 6 Abs. 1 Satz 1 Buchstabe a) DS-GVO lag dem Betreiber nicht vor, sodass für die Datenverarbeitung nur der Erlaubnistatbestand nach Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO in Betracht kam, wonach die Verarbeitung zur Wahrnehmung der berechtigten Interessen des Betreibers erforderlich sein musste und nicht die Interessen oder Grundrechte und Grundfreiheiten der von der Datenverarbeitung betroffenen Personen zum Schutz ihrer personenbezogenen Daten überwiegen durften.

Die Erforderlichkeit einer Verarbeitung von personenbezogenen Daten besteht jedoch nur, wenn der beabsichtigte Zweck nicht genauso gut mit milderen Mitteln erreicht werden kann, die weniger in die Rechte der Betroffenen eingreifen und dabei wirtschaftlich und organisatorisch zumutbar sind.
Die Prüfung ergab, dass mildere Mittel wie das irreversible Ausblenden, Schwärzen oder Verpixeln von Bereichen, die nicht dem Zweck der Beweissicherung dienten, zur Verfügung standen. Auch das Beschränken auf bestimmte Betriebszeiten der Kamera, das Deaktivieren von Tonaufnahmen sowie eine Beobachtung in Echtzeit, wären weniger eingriffsintensiv gewesen. Die vom Betreiber angebrachte Kamera überschritt damit den von ihm benannten Zweck der Beweissicherung. Mithilfe der vom Betreiber installierten Kamera wurden öffentliche Bereiche und Personen erfasst, die in keiner Verbindung zu seinem Beweissicherungsinteresse standen. Auch diente das Anfertigen von Tonaufnahmen nicht dem von ihm benannten Zweck. Die Datenverarbeitung war daher unter keinen Umständen erforderlich und griff zusätzlich in den Kernbereich privater Lebensgestaltung von Besuchern des Friedhofs ein. Dieser Bereich umfasst Handlungen und Äußerungen, die der Intim- und Privatsphäre zuzuordnen sind und einer besonderen Vertraulichkeit bedürfen. Auf einem Friedhof, einem sensiblen Ort der Trauer und Besinnung, gehören hierzu Gespräche, Rituale und persönliche Momente der Trauerbewältigung. Besucher müssen nicht damit rechnen, heimlich gefilmt oder belauscht zu werden.
Der Eingriff in die Persönlichkeitsrechte der betroffenen Personen nach Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 Grundgesetz in Ausformung des informationellen Selbstbestimmungsrechts – siehe auch Art. 6 Abs. 1 Thüringer Verfassung – war unverhältnismäßig.
Die Interessen der betroffenen Personen überwogen deutlich gegenüber den Interessen des Betreibers. Auch kam kein rechtfertigender Notstand im Sinne des § 16 Gesetz über Ordnungswidrigkeiten in Betracht. So stellt der Eingriff in das Persönlichkeitsrecht bei einer Vielzahl von unbeteiligten Personen gegenüber den Beschädigungen und Entwendungen am Grab ein höherrangiges Rechtsgut dar. Der rechtfertigende Notstand setzt ein Mindestmaß an gegenseitiger Solidarität in der Gesellschaft voraus. Dabei wird vom Einzelnen erwartet, dass er bereit ist, seine eigenen Rechtsgüter aufzugeben, wenn dies dazu beiträgt, eine erheblich schwerer wiegende Gefahr für andere abzuwenden (vergleiche BeckOK OWiG/Coen, 41 Ed. 1.1.2024, OWiG

§ 16 Rn. 36). Vorliegend war es unzumutbar von einer Vielzahl von Personen, die in den Fokus der Videoüberwachung geraten konnten, eine Aufopferung ihres Persönlichkeitsrechts in Ausformung des informationellen Selbstbestimmungsrechts abzuverlangen, da es sich nicht um die Abwendung einer wesentlich schwerer wiegenden Gefahr handelte. Des Weiteren war die Handlung des rechtfertigenden Notstands nicht erforderlich, da ein rechtlich geordnetes Verfahren in Form der Einschaltung der Polizei zur Verfügung stand, wodurch die drohende Gefahr hätte abgewendet werden können (vergleiche BeckOK OWiG/Coen, 41 Ed. 1.1.2024, OWiG § 16 Rn. 33).
Infolge des Verstoßes gegen die Grundsätze für die Verarbeitung, einschließlich der Bedingungen für die Einwilligung, gemäß den Artikeln 5, 6, 7 und 9 DS-GVO wurde gegen den Betreiber der Wildkamera ein Bußgeld rechtskräftig verhängt. Ein Strafverfahren wegen heimlich erstellter Tonaufnahmen gemäß § 201 Abs. 1 Nummer 1 Strafgesetzbuch wurde mangels eines fristgerechten Strafantrags der Geschädigten bei der zuständigen Staatsanwaltschaft nicht geführt, sodass der TLfDI die Erstellung von Video- und Tonaufnahmen ahndete. Andere Maßnahmen waren nicht angezeigt, da der Betreiber die Wildkamera bereits vor Eröffnung des Bußgeldverfahrens abgebaut hatte.

4. Vorträge und Veranstaltungen

Lernen Schulung Training - Pixabay

4.1 Der neue TLfDI stellt sich vor und ist präsent

Der Staffelstab ist übergeben, der Weg ist bereitet und die Ziele sind gesteckt. Es gilt Bewährtes fortzusetzen und Neues zu integrieren. Auch in diesem Berichtsjahr lag eine Priorität wieder bei Schule und Bildung. Das Thema Künstliche Intelligenz fand verstärkt Eingang in die Öffentlichkeitsarbeit des TLfDI.

Podium und Vorträge:
Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) beteiligte sich als Referent und Vortragender auf verschiedenen Podien und Veranstaltungen. Hervorzuheben ist die gemeinsame Teilnahme an einem Stand des Arbeitskreises „Schule und Bildungseinrichtungen“ der Datenschutzkonferenz bei der Bildungsmesse *didacta* in Köln. Einzelheiten dazu sind in dem Beitrag 1.9 zu finden.
Es gab weitere Vorträge, unter anderem bei der Gesellschaft für Paritätische Soziale Arbeit in Thüringen mbH (parisat) zu „Künstlicher Intelligenz in der Gründungsberatung“ und bei der „Kommunalen Informationsverarbeitung Thüringen GmbH“, jeweils in Erfurt. Hier referierte der TLfDI zu den „Hot Topics beim Datenschutz“.

Bei der Verbraucherzentrale Bundesverband (vzbv) hielt der TLfDI im Rahmen eines Seminars zum Datenschutzrecht in Göttingen einen Impulsvortrag zum Datenschutz, um den Beraterinnen und Beratern der Verbraucherzentralen aktuelle Themen des Datenschutzes in praxisnaher Form zu vermitteln und so die Beratung von Verbraucherinnen und Verbrauchern weiter zu verbessern. Der Verband der Wirtschaft Thüringens e. V. (VWT) hatte den TLfDI zum Thema: „Datenschutz zwischen Beratung und Kontrolle – ein Paradigmenwechsel?“ in die Veranstaltung *VIRTUELLES CAFÉ – auf ein Wort mit einem Vertreter aus der Wirtschaft* und vielen virtuellen Gästen des Verbandes eingeladen. Auch am 9. Datenschutztag der Karl-Volkmar-Stoy-Schule in Jena nahm der TLfDI wieder aktiv teil, und das bereits zum neunten Mal in Folge. Auch der Einladung zum Medienfachtag „Künstliche Intelligenz in der pädagogischen Praxis“ im Kultur- und Kongresszentrum Bad Langensalza für Fachkräfte der Kinder- und Jugendhilfe sowie Lehrerinnen und Lehrer ist der TLfDI gefolgt.
Die gemeinsame Videokonferenzreihe mit dem ThILLM „Datenschutz beim digitalen und häuslichen Lernen“ wurde mit vier Fortbildungsveranstaltungen und einem weiteren Fortbildungsangebot durch die Fachreferate „Schule“ und „Technische und organisatorische Maßnahmen“ fortgesetzt beziehungsweise ergänzt. Außerdem gab es hierzu weiterführende Vorträge beim „Staatlichen Studienseminar für Lehrerausbildung“ in Erfurt. Links für Lehrkräfte finden Sie unter: https://tlfdi.de/im-bildungswesen/schule/.

Folgende Materialen wurden aus gegebenem Anlass aktualisiert und auf den neuesten Stand gebracht:

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

Nachzuschlagen unter:
https://www.tlfdi.de/fileadmin/tlfdi/Infothek/Internet_Gesetzesbroschuere_05.2024.pdf

Aktualisierung der Handreichung „Digitale Selbstverteidigung“:

Nachzuschlagen unter:
https://tlfdi.de/fileadmin/tlfdi/Infothek/Digitale_Selbstverteidigung__Stand_Oktober_25.PDF

Der TLfDI beantwortete **31 Presseanfragen** von Journalistinnen und Journalisten sowie verschiedenen Redaktionen. Es gab weitere **41 allgemeine Anfragen zur Öffentlichkeitsarbeit** der Behörde. Der TLfDI gab **diverse Interviews** bei Funk und Fernsehen und veröffentlichte **14 Pressemitteilungen**. Der **Tag der offenen Tür** im Thüringer Landtag fiel durch eine Schlechtwetterwarnung im Berichtsjahr 2023 leider buchstäblich ins Wasser.

5. Entschließungen und Beschlüsse

Konferenz Erde Welt - Pixabay

5.1 Besserer Schutz von Patientendaten bei Schließung von Krankenhäusern

Entschließung
der Konferenz der unabhängigen Datenschutzaufsichtsbehörden
des Bundes und der Länder
am 15. Mai 2024

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) fordert sowohl alle relevanten Stakeholder – insbesondere Leitungen, Träger und Interessenvertretungen der Krankenhäuser – als auch die verantwortlichen Akteure in Politik und Verwaltung sowie die Gesetzgeber des Bundes und der Länder dazu auf, sich frühzeitig mit den datenschutzrechtlich relevanten Auswirkungen der für die Zukunft zu befürchtenden weiteren Krankenhausschließungen zu befassen.
In den vergangenen Monaten hat die Zahl an Schließungen und Insolvenzen von Krankenhäusern bundesweit stark zugenommen. Die DSK nimmt dies insbesondere im Hinblick auf die in den Einrichtungen

vorgehaltenen besonders schutzbedürftigen Behandlungsdokumentationen der Patientinnen und Patienten mit Sorge zur Kenntnis. Wiederholt wurden die Datenschutzaufsichtsbehörden mit Fällen konfrontiert, in denen eine sichere Aufbewahrung und der Zugang der Betroffenen zu den Patientendaten nicht gewährleistet waren. Teilweise bestand sogar die Gefahr, dass sich Unbefugte Zugang zu den Krankenakten verschaffen konnten.

Die DSK weist in diesem Zusammenhang auf Folgendes hin:

Datenschutzrelevante Herausforderungen für Klinikbetreiber und Insolvenzverwalter im Zusammenhang mit Krankenhausschließungen

Die Erfahrungen der Aufsichtsbehörden zeigen, dass mangels Insolvenzmasse die Kosten zur weiteren Aufbewahrung der Patientenakten häufig ab einem gewissen Zeitpunkt nicht mehr durch den Insolvenzverwalter getragen werden können. Hat die Suche nach anderen rechtlich Verantwortlichen keinen Erfolg, gibt es im Bereich der Krankenhausbehandlung keine bundes- oder landesgesetzlichen Festlegungen, durch wen und in welcher Form die weitere Aufbewahrung einschließlich der Löschung der Patientendaten erfolgen muss und in welcher Weise die Patientinnen und Patienten Zugang zu den sie betreffenden Behandlungsdokumentationen erhalten. Insbesondere fehlen hier vergleichbare Regelungen, wie sie sich vereinzelt in Heilberufsgesetzen der Länder finden, in denen unter bestimmten Voraussetzungen eine Notverantwortung der Heilberufskammern bei der Schließung ambulanter Arztpraxen festgelegt wurde (z. B. § 22 Abs. 2 des rheinland-pfälzischen Heilberufsgesetzes, § 4 Abs. 1 Satz 4 ff. HBKG BW, § 7 Abs. 3 SächsHKaG).

Aus Sicht der DSK hat dieser Zustand starke nachteilige Auswirkungen auf den datenschutzrechtlich gebotenen Schutz der Gesundheitsdaten und die effektive Wahrnehmung der Betroffenenrechte der Patientinnen und Patienten:

Patientenakten enthalten Gesundheitsdaten im Sinne von Artikel 4 Nr. 15 der DS-GVO, die eine besondere Kategorie personenbezogener Daten nach Artikel 9 DS-GVO darstellen. Aufgrund ihrer Sensibilität muss ihnen ein besonderer Schutz zukommen. Dies ist derzeit im Falle der Insolvenz von Krankenhausträgern oder ungeplanter Schließungen von einzelnen Einrichtungen nur unzureichend rechtlich geregelt. Nur sofern ein Insolvenzverfahren läuft, können Patientinnen und Patienten regelmäßig über den Insolvenzverwalter Einsicht in ihre Akte

erlangen. Sobald das Insolvenzverfahren jedoch beendet ist oder mangels Masse nicht eröffnet wird, ist aufgrund fehlender Regelungen offen, durch wen und unter welchen technisch-organisatorischen Anforderungen Krankenhausakten aufzubewahren, datenschutzkonform zu löschen und wie Patientenrechte zu gewährleisten sind. Dies ist sowohl aus datenschutzrechtlicher Sicht als auch im Interesse einer im Einzelfall gebotenen medizinischen Weiterbehandlung nicht hinzunehmen. Es bedarf deshalb zeitnaher effektiver Lösungen, die den weiteren Umgang sowohl mit papiergebundenen als auch mit elektronisch geführten Patientenakten im Falle von Klinikschließungen datenschutzkonform festlegen. Denn die datenschutzrechtlichen Vorgaben, wie sie beim fortlaufenden Krankenhausbetrieb zu beachten sind, gelten auch nach einer Betriebseinstellung fort.

Denkbare Lösungsansätze aus datenschutzrechtlicher Sicht

Die DSK hält unter anderem folgende Bausteine für geeignet, um eine datenschutzkonforme Lösung der aufgezeigten Problematik zu finden:

- In Anlehnung an bereits bestehende Regelungen in den Landeskrankenhausgesetzen von Nordrhein-Westfalen (§ 34c Abs. 1 KHGG NRW) und Hessen (§ 12 Abs. 5 HKHG) sollten die Krankenhäuser bundesweit dazu verpflichtet werden, entsprechende Konzepte zur weiteren Verwahrung der Patientenakten für den Fall der Insolvenz oder der ungeplanten Schließung anzufertigen. Diese sollten der zuständigen Fachaufsicht vorgelegt werden.
- Aufgrund der aufgezeigten Probleme im Kontext von Insolvenzen regt die DSK an, dass sich die Länder mit einer Finanzierungs-Lösung befassen, damit in dringenden Fällen Aufbewahrungen und Sicherungen von Patientenakten für einen Übergangszeitraum weiter finanziert werden können. So sieht z. B. das Krankenhausgestaltungsgesetz des Landes Nordrhein-Westfalen in § 34c Abs. 2-6 KHGG NRW die Einrichtung von Patientenaktensicherungsfonds vor.
- Solange keine geeigneten landesrechtlichen Regelungen existieren, sollten die relevanten Stakeholder, insbesondere Leitungen, Träger und Interessenvertretungen der Krankenhäuser, gemeinsam datenschutzkonforme Lösungen entwickeln, um im Bedarfsfall die kurzfristige sichere Aufbewahrung von Patientenakten geschlossener Kliniken sicherzustellen. Dabei könnten auch Vertreter der Datenschutzaufsicht beratend beteiligt werden.

- Die DSK regt an, dass sich die Gesundheitsministerkonferenz bei ihrer nächsten Zusammenkunft mit der Thematik befasst und Lösungsmöglichkeiten erarbeitet. Dabei sollte eine lückenlose Regelung der Notverantwortung für Patientendaten geschlossener Krankenhäuser angestrebt werden – etwa wie dies in den Heilberufsgesetzen oder Pflegekammergesetzen einzelner Länder durch die Zuständigkeit der Kammern geschehen ist.

Die DSK appelliert nachdrücklich an die Entscheidungsträger, bestehende Regelungslücken zu schließen und im Interesse der betroffenen Patientinnen und Patienten für Rechtsklarheit und Rechtssicherheit zu sorgen.

5.2 Vorsicht bei dem Einsatz von Gesichtserkennungssystemen durch Sicherheitsbehörden

Entschließung
der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder
am 20. September 2024

Bereits jetzt setzen einige Behörden automatisierte biometrische Gesichtserkennungssysteme im öffentlichen Raum ein und berufen sich dabei auf unspezifische strafprozessuale Normen.[2] Hierbei werden nach Ansicht der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) der einschlägige Rechtsrahmen und die Freiheitsrechte der Betroffenen – also potentiell aller Bürgerinnen und Bürger – nicht hinreichend beachtet. Die bestehenden Regelungen in der Strafprozessordnung bieten für biometrische Gesichtserkennung im öffentlichen Raum keine Grundlage. Aktuell gibt es zudem Bestrebungen der Politik, das Instrument der automatisierten biometrischen Gesichtserkennung in unterschiedlichen rechtlichen Zusammenhängen zu erlauben.
Eine Regelung durch den Gesetzgeber wäre hierbei nur in einem engen Rahmen mit den europäischen und nationalen Grundrechten der

[2] So wurde etwa im Frühjahr 2024 bekannt, dass eine sächsische Polizeidirektion über ein Gesichtserkennungssystem verfügt, welches bereits für Ermittlungsverfahren in verschiedenen Bundesländern genutzt wurde. Als Rechtsgrundlagen wurden §§ 100h, 163f StPO für die Aufzeichnung von Bildern auf öffentlichen Straßen und § 98a StPO für den Abgleich mittels automatisierter Gesichtserkennung herangezogen.

betroffenen Personen vereinbar. Der Einsatz von Gesichtserkennungssystemen kann ein sehr intensiver Eingriff in die Grundrechte der betroffenen Personen sein. Die Intensität hängt insbesondere von der Art der ausgewerteten Daten, der eingesetzten Technik und dem Grad der Automatisierung ab. Von besonderer Bedeutung ist die Streubreite der Maßnahme, wie z. B. beim Einsatz von Gesichtserkennungssystemen im öffentlichen Raum. Erfasst die Analyse viele Menschen und zudem solche, die dafür keinerlei Anlass gegeben haben, führt dies zu einem noch intensiveren Eingriff. Relevant sind ferner eine eventuelle Heimlichkeit der Maßnahme und das erhebliche Risiko von Fehlerkennungen. Diese können auch für unschuldige Menschen zu intensiven Folgeeingriffen, wie z. B. Freiheitsentziehungen, führen.
Aus diesem Grund hat der europäische Gesetzgeber in der KI-Verordnung[3] bestimmte Anwendungen ausgeschlossen und für andere Anwendungen enge Grenzen bestimmt
Sofern nach der KI-Verordnung und dem Verfassungsrecht Regelungsspielraum für den nationalen Gesetzgeber verbleibt und er den entsprechenden Einsatz als zwingend erforderlich betrachtet, muss er spezifische, verhältnismäßige Rechtsgrundlagen für den Einsatz von Gesichtserkennungssystemen schaffen. Hierin sind in Abhängigkeit von der Eingriffsintensität hinreichende Eingriffsschwellen, ausreichende Anforderungen an den Rechtsgüterschutz und zusätzliche Schutzmechanismen festzulegen.
Zu dieser Thematik hat der Europäische Datenschutzausschuss (EDSA) Leitlinien erlassen. Auch nach Ansicht des EDSA darf Gesichtserkennungstechnologie nur unter strikter Einhaltung des einschlägigen Rechtsrahmens und ausschließlich in solchen Fällen verwendet werden, in denen die Anforderungen an die Erforderlichkeit und Verhältnismäßigkeit belegbar erfüllt sind.
Sofern und soweit der Gesetzgeber den entsprechenden Einsatz nach sorgfältiger Prüfung als unbedingt erforderlich betrachtet, fordert die DSK, sich mit den rechtlichen Vorgaben intensiv auseinanderzusetzen und diese zu beachten.

[3] Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz).

5.3 Menschenzentrierte Digitalisierung in der Daseinsvorsorge sicherstellen![4]

Entschließung
der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder
am 19. Dezember 2024

Die Gesetzgeber und Regierungen der EU, des Bundes und der Länder streben einen digitalen Wandel an, in dessen Mittelpunkt der Mensch steht (siehe z. B. Europäische Erklärung zu den digitalen Rechten und Grundsätzen in der digitalen Dekade; 2023/C 23/1). Die Konferenz der Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz, DSK) erkennt das Potential, das der digitale Wandel in allen Lebensbereichen für Wirtschaft und Gesellschaft birgt. Sie unterstützt deswegen das Leitbild einer menschenzentrierten Digitalisierung als ein wichtiges politisches Ziel in der Europäischen Union. Seine Umsetzung und Verwirklichung durch unterschiedliche Akteure muss das Grundrecht auf informationelle Selbstbestimmung im Blick behalten und insbesondere die allgemeinen Grundsätze für die Verarbeitung personenbezogener Daten beachten. Speziell in der Daseinsvorsorge sieht die Datenschutzkonferenz daher die Notwendigkeit, diesen menschenzentrierten Ansatz zum Schutz derjenigen, die nicht digital agieren können oder wollen, gesetzlich zu flankieren. Seien es zentrale Verkehrsdienstleistungen, die Energie- oder Wasserversorgung oder öffentlich geförderte kulturelle Dienstleistungen, der Trend zur Digitalisierung hält überall Einzug. Wenn für die Inanspruchnahme solcher Dienstleistungen die Nutzung elektronischer Kommunikationswege (z. B. Internet), die Eröffnung eines digitalen Kontos oder die Nutzung einer Smartphone-App vorausgesetzt werden, kann das dazu führen, dass bestimmte Menschen von der Inanspruchnahme solcher Daseinsvorsorgeleistungen ausgeschlossen werden. Das betrifft all diejenigen, die aufgrund körperlicher oder geistiger Beeinträchtigung, ihres Alters (Minderjährige ebenso wie Ältere), Technikferne oder fehlender Mittel nicht in der Lage sind, die digitale Technik zu nutzen, oder die in Ausübung ihres Grundrecht auf informationelle Selbstbestimmung ihre Daten nicht preisgeben wollen.

[4] Der Bayerische Landesbeauftragte für den Datenschutz und die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit haben die Entschließung abgelehnt.

Dieser Trend ist auch eine Herausforderung für die Grundrechte auf Datenschutz und Achtung des Privatlebens aus Art. 8 und Art. 7 der Charta der Grundrechte der Europäischen Union (GRCh) sowie auf informationelle Selbstbestimmung gemäß Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 Grundgesetz (GG) in ihrem jeweiligen Anwendungsbereich.
Vor diesem Hintergrund weist die Datenschutzkonferenz darauf hin, dass bei der Leistungserbringung gemäß Art. 6 Abs. 1 Buchst. b DSGVO nur die Verarbeitung der für einen Vertrag erforderlichen personenbezogenen Daten zulässig ist. Die Erforderlichkeit der Datenverarbeitung bezieht sich auf den Hauptgegenstand des Vertrags – sie muss also für die Inanspruchnahme der Leistung der Daseinsvorsorge unerlässlich sein. Außerdem ist der Grundsatz der Datenminimierung gemäß Art. 5 Abs. 1 Buchst. c DSGVO zu berücksichtigen, wobei die Verarbeitung auf den für den Zweck erforderlichen Umfang zu begrenzen ist. Bei einer auf Einwilligung basierenden Datenverarbeitung ist deren Freiwilligkeit und mithin die Rechtmäßigkeit der Verarbeitung in Frage zu stellen, wenn die betroffenen Personen einer sozialen oder ökonomischen Drucksituation ausgesetzt sind, die ihnen eine „echte oder freie Wahl“ (vgl. Erwägungsgrund 42 Satz 5 DSGVO) unmöglich machen.
Vor diesem Hintergrund macht die Datenschutzkonferenz auch auf die besondere Bedeutung der Prinzipien von Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Data Protection by Design and Default) nach Art. 25 DSGVO aufmerksam. Der Verantwortliche hat bereits bei der Planung von Digitalisierungsprojekten, aber auch bei ihrer Realisierung insbesondere geeignete Maßnahmen zur Datenminimierung zu treffen. Die Datenschutzkonferenz unterstreicht, dass solche Maßnahmen nachhaltig zur Vertrauenswürdigkeit digitaler Angebote beitragen können. Zugleich sind die in Art. 25 DSGVO verbindlich ausgestalteten Prinzipien kein optionales Angebot der Verantwortlichen, sondern die notwendige Voraussetzung für ein datenschutzkonformes digitales Angebot der Daseinsvorsorge.
Allein mit Mitteln des Datenschutzes sind allerdings befriedigende Lösungen für die Menschen, die wegen fehlender digitaler Möglichkeiten von wichtigen Leistungen der Daseinsvorsorge ausgeschlossen sind, nicht erreichbar. Zum einen kann die rechtliche Durchsetzung des Datenschutzes in möglichen gerichtlichen Auseinandersetzungen viel Zeit in Anspruch nehmen, in denen Betroffene keine schnelle

Teilhabe erhalten. Zum anderen sind auch nicht alle gesellschaftspolitischen Aspekte einer menschenzentrierten Digitalisierung an Datenschutzregelungen gebunden. Es bedarf hier vielmehr klarer gesetzlicher Leitplanken, um die menschenzentrierte Digitalisierung voranzubringen. Die Notwendigkeit solcher Maßnahmen aus Verbraucherschutzsicht hat jüngst die 20. Verbraucherschutzministerkonferenz vom 14. Juni 2024 unterstrichen (vgl. Beschluss Nr. 25 + 27: Sicherstellung einer nichtdigitalen Kundenkommunikation und analogen Teilhabe am wirtschaftlichen Leben).
Die Datenschutzkonferenz appelliert an die Gesetzgeber von Bund und Ländern, flankierende gesetzliche Maßnahmen im Bereich der Daseinsvorsorge zu prüfen, die die Rahmenbedingungen einer fairen Teilhabe derjenigen regeln, die keinen digitalen Zugang zu unverzichtbaren Dienstleistungen der Daseinsvorsorge haben oder nicht haben wollen.

5.4 Nationale Zuständigkeiten für die Verordnung zur Künstlichen Intelligenz (KI-VO)

Beschluss
der Konferenz der unabhängigen Datenschutzaufsichtsbehörden
des Bundes und der Länder
am 3. Mai 2024

Positionspapier der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 3. Mai 2024

Die KI-VO sieht bereits in einigen Fällen die sektorspezifische Zuständigkeit der Datenschutzbehörden als Marktüberwachungsbehörden vor. Aufgrund ihrer bestehenden Zuständigkeiten nach der DSGVO, ihrer langjährigen Expertise im digitalen Grundrechtsschutz und etablierten, kooperativen Aufsichts- sowie Abstimmungsmechanismen sollte diese Kompetenz ausgeweitet werden. Die Datenschutzaufsichtsbehörden sind bereit, die Aufgabe der nationalen Marktüberwachung für KI-Systeme zu übernehmen.
Im März 2024 hat das Europäische Parlament die Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz angenommen. Nach Inkrafttreten der KI-VO muss in Deutschland innerhalb von 12 Monaten eine behördliche Aufsichtsstruktur eingerichtet

werden. Damit besteht Handlungsbedarf für die Gesetzgeber in Bund und Ländern.
Aufgrund der bereits jetzt durch die DSGVO begründeten Aufgaben und Befugnisse der Datenschutzaufsichtsbehörden sowie der langjährigen Erfahrung im Bereich der Beratung, Beschwerdebearbeitung und Kooperation auf nationaler wie europäischer Ebene sollten in Deutschland grundsätzlich die nationalen Datenschutzaufsichtsbehörden als Marktüberwachungsbehörden benannt werden. Das Ziel einer einheitlichen Anwendung der KI-VO wäre mit der Einrichtung weiterer Marktüberwachungsbehörden kaum zu erreichen. Sowohl im Bereich der KI- als auch der Datenschutzaufsicht hätten Unternehmen, Behörden und Bürger:innen es bei einer Bündelung der Zuständigkeiten im Regelfall nur mit *einer* Aufsichtsbehörde zu tun. Zudem verfügen die Datenschutzaufsichtsbehörden nicht nur über einschlägige Fachkunde und die von der KI-VO geforderte Unabhängigkeit, sondern auch über funktionierende Kooperations- und Kohärenzmechanismen.
Ohnehin bleibt die Datenschutzaufsicht – jedenfalls bei KI-Systemen, die personenbezogene Daten verarbeiten, wie dies in der Praxis regelmäßig auftreten wird – vollständig bestehen, da die KI-VO die DSGVO in ihrem Anwendungsbereich nicht ersetzt. Auch die KI-VO erkennt die Expertise der Datenschutzbehörden an: Für Kernelemente der demokratischen Ordnung sind sie bereits zuständige Marktüberwachungsbehörden (Strafverfolgung, Wahlen, Grenzkontrolle und Justizverwaltung, Art. 74 Abs. 8 i. V. m. Anhang III Nr. 1, 6, 7, 8 KI-VO). Als für den Grundrechtsschutz zuständige Behörde erhält die Datenschutzaufsicht im Rahmen ihrer bestehenden Zuständigkeiten zudem zusätzliche Befugnisse für KI-Systeme, die personenbezogene Daten verarbeiten (Art. 77, EG 157 KI-VO). Daher liegt es nahe, den Datenschutzaufsichtsbehörden auch darüber hinaus nach innerstaatlichem Recht Zuständigkeiten zur Durchsetzung der KI-VO zuzuweisen.
Strukturell handelt es sich bei der KI-VO im Wesentlichen um ein Regelwerk der Produktregulierung im Ordnungsrahmen des „New Legislative Frameworks“. Künstliche Intelligenz kann dabei nur auf Basis digitaler Rechte und namentlich eines hohen Datenschutzniveaus prosperieren. Als Produktregulierungsverordnung wird die Zuständigkeit für die Marktüberwachung nach der KI-VO Bund und Ländern zugewiesen werden müssen: Während Landesbehörden im Grundsatz

die Aufsicht führen, wird eine Bundesbehörde für die einheitliche Regelung gesamtstaatlicher Sachverhalte zuständig sein (Art. 83, 72 Abs. 2 GG). Dies entspricht auch der Struktur der Behörden im Produktsicherheitsrecht, welche die Marktüberwachungs-Verordnung umsetzen (§ 4 MÜG, § 25 ProdSG).

Nationale Regelung der Zuständigkeiten für die KI-VO

Die Benennung der jeweiligen allgemeinen Marktüberwachungsbehörden in den Mitgliedstaaten ist in der KI-VO nicht dediziert geregelt. Es finden sich nur vereinzelt Vorgaben, die bei der nationalen Bestimmung zu berücksichtigen sind. Für Deutschland muss – wie in anderen Mitgliedstaaten auch – in einem nationalen Umsetzungsgesetz festgelegt werden, welcher oder welchen unabhängigen nationalen Behörden die jeweiligen Zuständigkeiten zugewiesen werden (Art. 70 Abs. 1 KI-VO). Dabei muss gleichzeitig auch eine hinreichende Bereitstellung aufgabengerechter zusätzlicher Ressourcen mitgedacht werden.

Die DSK empfiehlt, die allgemeinen Marktüberwachungsbehörden für die Zwecke der KI-VO in Deutschland wie folgt zu benennen:

- Marktüberwachungsbehörden: BfDI und Landesdatenschutzbehörden
  Hinweis: Wird ein KI-System bundesweit als Produkt angeboten oder aus dem internen Gebrauch heraus zum externen Vertrieb auf den Markt gebracht, liegt die Zuständigkeit hierfür beim Bund. Insbesondere die Nutzung oder die Entwicklung von KI-Systemen für den internen Gebrauch durch Unternehmen und Behörden wird von den Landesdatenschutzbehörden bzw. der Bundesdatenschutzbehörde in ihrer jeweiligen Zuständigkeit überwacht.
- Europäischer Ausschuss für KI: BfDI
  Hinweis: Der Vertreter der Mitgliedstaaten im europäischen Ausschuss für KI wird automatisch der zentrale Ansprechpartner gegenüber dem Ausschuss, der Öffentlichkeit und den anderen Akteuren der KI-VO auf nationaler und europäischer Ebene.
- Unberührt bleiben sektorale Zuständigkeiten (z. B. Kraftfahrzeuge, Finanzsektor, KRITIS), soweit sie bereits in dem Verordnungstext vorgesehen sind oder vom Bundesgesetzgeber aufgrund der Sachnähe aufgegriffen werden.

5.5 Positionspapier Anforderungen an die Sekundärnutzung von genetischen Daten zu Forschungszwecken

Beschluss
der Konferenz der unabhängigen Datenschutzaufsichtsbehörden
des Bundes und der Länder
am 15. Mai 2024

„Genetische Daten“ sind nach Artikel 4 Nummer 13 der Datenschutz-Grundverordnung (DS-GVO) personenbezogene Daten zu den ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser natürlichen Person liefern und insbesondere aus der Analyse einer biologischen Probe der betreffenden natürlichen Person gewonnen wurden.
Die Nutzung genetischer Daten ist die Grundlage für eine personalisierte, auf die individuelle Patientin oder den individuellen Patienten angepasste Präzisionsmedizin. Die Forschung mit genetischen Daten kann den biomedizinischen Fortschritt wesentlich voranbringen und zu einer verbesserten medizinischen Versorgung beitragen.[5] Insbesondere in der Krebsforschung und der Erforschung seltener Erkrankungen kann die Analyse genetischer Daten zu vielversprechenden Behandlungs- oder sogar Heilungsmöglichkeiten führen.
Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) fordert daher eine datenschutzkonforme wissenschaftliche biomedizinische Forschung mit genetischen Daten zum Wohle der Patientinnen und Patienten, indem dazu ein gesetzlicher Rahmen geschaffen wird, der sanktionsbewehrte hohe Schutz- und Vertrauensanforderungen und wirksame Mitwirkungs- und Kontrollmöglichkeiten der betroffenen Personen vorsieht.
Forschung mit körpereigenen Substanzen, wie z. B. Blut, Haaren oder Speichel, die ohne Kenntnis der betroffenen Person erlangt wurden, muss verboten bleiben.

I. Besonders hohe Risiken

Genetische Daten sind von äußerster Sensibilität und bergen ein „hohes prädiktives Potential“ mit Blick auf die betroffene Person und bi-

[5] Vgl. z. B. https://www.gesundheitsforschung-bmbf.de/de/medizinische-genomforschung-6640.php.

ologische Verwandte. Aus genetischen Daten lassen sich unter anderem Erkenntnisse über gesundheitliche Prädispositionen, Gesundheitsrisiken und vererbliche Erkrankungen ableiten. Diese Erkenntnisse betreffen nicht nur die betroffene Person selbst, sondern können sich auch auf leibliche Familienangehörige erstrecken. Anhand der Analyse genetischer Daten lassen sich damit Wahrscheinlichkeitsaussagen über das Auftreten von Krankheiten der leiblich miteinander verwandten Personen treffen.
Das Diskriminierungs- und Stigmatisierungsrisiko bei Kenntnis dieser Daten, z. B. durch Versicherungen und Arbeitgeber, ist daher enorm. Risikoerhöhend wirkt sich außerdem die Tatsache aus, dass genetische Daten durch die betroffenen Personen nicht verändert werden können, sondern diesen ihr Leben lang und auch darüber hinaus anhaften.
Die Weiterverarbeitung genetischer Daten in der medizinischen Sekundärnutzung (insbesondere zur Forschung) betrifft daher aufgrund von Rückschlüssen auf persönlichkeitsrelevante Merkmale wie Erbanlagen und (potentielle) Krankheiten regelmäßig den absolut geschützten Kernbereich der Persönlichkeit.
In diesem Zusammenhang muss zudem berücksichtigt werden, dass eine wirksame Anonymisierung genetischer Daten in der Regel daran scheitert, dass – etwa über einen Abgleich mit anderen genetischen Daten der betroffenen Person – eine Identifizierung möglich ist. Der Personenbezug lässt sich daher aus genetischen Daten in der Regel nicht entfernen. Genetische Daten sind deshalb schon aufgrund ihres potentiellen Informationsgehalts regelmäßig als personenbezogene Daten zu behandeln.

II. Besondere Regeln: ausdrückliche Einwilligung

Aus diesen Gründen muss der Umgang mit genetischen Daten qualifizierten datenschutzrechtlichen Regeln unterliegen, die die Rechte und Freiheiten der betroffenen Person in ausreichendem Maße wahren.
Für die datenschutzkonforme Verarbeitung genetischer Daten bedarf es daher grundsätzlich der ausdrücklichen Einwilligung der betroffenen Personen. Denn gerade in diesem äußerst sensiblen Bereich vermag nur die datenschutzrechtliche Einwilligung als Grundlage für

eine individuelle Rechtsausübung dem hohen Gut des Rechts auf informationelle Selbstbestimmung unmittelbar Ausdruck verleihen.[6]
Die DSK hat bereits 2001 auf die besondere Sensibilität genetischer Daten hingewiesen und eine gesetzliche Regelung von genetischen Untersuchungen gefordert.[7] Mit dem Gendiagnostikgesetz (GenDG) wurde eine solche gesetzliche Regelung zum 1. Februar 2010 geschaffen. Zu Recht bestimmt das Gendiagnostikgesetz, dass bei genetischen Untersuchungen oder Analysen eine Verarbeitung genetischer Daten nur mit ausdrücklicher und schriftlicher Einwilligung der betroffenen Personen erfolgen darf.
Das Gendiagnostikgesetz gilt aber ausdrücklich nicht für die Verarbeitung von Daten zu Forschungszwecken (§ 2 Absatz 2 Nr. 1 GenDG). Für die Verarbeitung genetischer Daten zu Forschungszwecken gelten bislang deshalb lediglich die allgemeinen Regelungen für die Forschung mit besonderen Kategorien personenbezogener Daten. Die wirksame informierte, freiwillige und ausdrückliche Einwilligung der betroffenen Personen allein ist aber im absolut geschützten Kernbereich der Persönlichkeit noch kein ausreichender Schutzgarant des Rechts auf informationelle Selbstbestimmung. Vielmehr muss bei jeglicher Verarbeitung genetischer Daten im Rahmen einer Sekundärnutzung zu Forschungszwecken zusätzlich sichergestellt sein, dass erforderliche angemessene und spezifische Garantien und technische sowie organisatorische Schutzmaßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person vorgeschrieben sind und einer regelmäßigen Prüfung und Aktualisierung unterliegen.
Im Bereich der genetischen Forschung ist ein vielfältiger Datenaustausch und die Vernetzung der genetischen Datenbestände das erklärte Ziel vieler Vorhaben. Häufig können zum Zeitpunkt der Informationsbereitstellung die Zwecke der Verarbeitung bezogen auf konkrete Forschungsprojekte im Einzelnen noch nicht vollständig und präzise angegeben werden, sodass die Einwilligung mangels ausreichender Bestimmtheit möglicherweise an rechtliche Grenzen stößt. Die Nutzung

[6] DSK: Petersberger Erklärung zur datenschutzkonformen Verarbeitung von Gesundheitsdaten in der wissenschaftlichen Forschung vom 24.11.2022, S. 5, https://www.datenschutzkonferenz-online.de/media/en/20221124_en_06_Entschliessung_Petersberger_Erklaerung.pdf.

[7] DSK-Entschließung zur „Gesetzlichen Regelung von genetischen Untersuchungen“ vom 24.10.2001, https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DSK/DSK-Entschliessungen/62DSK-GesetzlicheRegelungVonGenetischenUntersuchungen.pdf.

einer breiten Einwilligung (Broad Consent) im Sinne des Erwägungsgrunds 33 DS-GVO zur Verarbeitung genetischer Daten kann hier eine Lösung bieten. Jedoch sollten auch die Anforderungen und Grenzen der breiten Einwilligung gesetzlich geregelt werden, um die hier bestehende Rechtsunsicherheit zu beseitigen. Außerdem müssen zusätzliche Sicherungsmaßnahmen zur Gewährleistung von Transparenz, Vertrauensbildung, Partizipation und Datensicherheit getroffen werden.[8]

Die Notwendigkeit der ausdrücklichen Einwilligung für die Sekundärnutzung zu Forschungszwecken ergibt sich schon daraus, dass die Erhebung der genetischen Probe und die genetische Untersuchung selbst nach Artikel 3 Absatz 2 Buchst. a EU-Grundrechte-Charta und dem Gendiagnostikgesetz einer Einwilligung bedürfen. Es wäre daher treuwidrig, entgegen der eingeholten Einwilligung die genetischen Daten auch für andere Zwecke zu verarbeiten (Artikel 5 Absatz 1 Buchst. a und b DS-GVO).

Sowohl bei einer spezifischen Einwilligung als auch bei der breiten Einwilligung darf es im besonders sensiblen Bereich der Sekundärnutzung genetischer Daten nicht den Verantwortlichen überlassen werden, welche flankierenden technischen und organisatorischen Schutzmaßnahmen zu treffen sind. Stattdessen bedarf es gesetzlicher Vorgaben über das zu realisierende hohe Schutz- und Vertrauensniveau, gerade auch mit Blick auf die Mitbetroffenheit von biologischen Verwandten.

Die DSK ist aufgrund der genannten Erwägungen der Auffassung, dass für die Sekundärnutzung genetischer Daten zu Forschungszwecken eine differenzierte und rechtsklare gesetzliche Regelung geschaffen werden muss, um das Interesse an der wissenschaftlichen Nutzung genetischer Daten mit dem Recht auf informationelle Selbstbestimmung und dem Recht auf Nichtwissen im hier betroffenen, absolut geschützten Kernbereich der Persönlichkeit in Einklang zu bringen.

Artikel 9 Absatz 4 DS-GVO wie auch voraussichtlich die EHDS-Verordnung sehen ausdrücklich eine entsprechende Öffnungsklausel für

[8] Vgl. Beschluss der 97. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zu Auslegung des Begriffs „bestimmte Bereiche wissenschaftlicher Forschung“ im Erwägungsgrund 33 der DS-GVO vom 03.04.2019, https://www.datenschutzkonferenz-online.de/media/dskb/20190405_auslegung_bestimmte_bereiche_wiss_forschung.pdf.

zusätzliche Bedingungen, einschließlich Beschränkungen, zur Verarbeitung genetischer Daten vor.

III. Besonders hohe Schutzmaßnahmen

In einer solchen gesetzlichen Regelung zur Sekundärnutzung genetischer Daten zu Forschungszwecken sollte die ausdrückliche Einwilligung als notwendige Voraussetzung der Verarbeitung vorgesehen werden. Gleichzeitig ist durch wirksame technische und organisatorische Garantien im Sinne der Konzepte des „data protection by design" und „data protection by default" sicherzustellen, dass nach einem Widerruf der Einwilligung die Verarbeitung der genetischen Daten der betroffenen Personen endet und die Betroffenenrechte stets wirksam ausgeübt werden können.

Die gesetzliche Regelung sollte zudem zwischen den verschiedenen Verarbeitungszwecken der Sekundärnutzung, wie der Forschung und der Qualitätssicherung, differenzieren. Bei dieser Differenzierung ist auch zu berücksichtigen, dass Erwägungsgrund 33 DS-GVO die Möglichkeit der breiten Einwilligung nur für die wissenschaftliche Forschung und nicht für die Qualitätssicherung eröffnet.

Eine gesetzliche Regelung über die Verarbeitung genetischer Daten zur Sekundärnutzung sollte im Hinblick auf die Grundsätze der Zweckbindung und Datenminimierung (Artikel 5 Absatz 1 Buchst. b und c DS-GVO) außerdem widerspiegeln, dass eine Qualitätssicherung und Evaluation der medizinischen Nutzung genetischer Daten die Verarbeitung nur legitimieren kann, wenn die Ziele der zu sichernden Qualität bzw. die Zwecke der Evaluation genau bestimmt sind und solange und soweit die Verarbeitung für diese Zwecke zwingend erforderlich ist.

Zudem hält es die DSK für geboten, dass eine gesetzliche Regelung für die Verarbeitung genetischer Daten zu Zwecken der Sekundärnutzung besondere Schutzmaßnahmen vorsieht. Dabei sollte insbesondere Folgendes gewährleistet werden:

- Verpflichtung zur Einhaltung einer Mindestbedenkzeit zwischen Informationsbereitstellung und Abgabe einer Einwilligungserklärung i. V. m. Hilfsangeboten für betroffene Personen und deren Angehörige (z. B. psychosoziale Beratung).
- Aufklärung und Beratung für die Entscheidung der betroffenen Personen über den Umgang mit individuell relevanten Forschungsergebnissen und Zufallsbefunden („Recht auf Nichtwissen") nach Information über mögliche Risiken und Auswirkun-

gen der Kenntnisnahme für die betroffene Person und den biologisch Verwandten sowie Hinweis auf die Möglichkeit zur Änderung dieser Entscheidung.

- Transparenz der Datenverarbeitung durch Festlegung umfassender Informations- und Aufklärungspflichten zu Zwecken, Reichweite und Risiken der Verarbeitung für die Rechte und Freiheiten natürlicher Personen.
- Erweiterte Kontroll- und Mitwirkungsmöglichkeiten für betroffene Personen, z. B. durch aktive, rechtzeitige und leicht zugängliche Bereitstellung aktueller Informationen über neue Forschungsvorhaben und barrierefreie Ausübung von Widerrufsrechten und Betroffenenrechten über digitale Managementsysteme.[9]
- Genehmigungspflicht von Forschungsvorhaben durch eine Ethikkommission.
- Die Rechtsgrundlage einer breiten Einwilligung ist nur unter strengen Vorgaben zulässig: Es bedarf spezifischer Aufklärungs- und Beratungsanforderungen und einer zeitlichen Begrenzung der Gültigkeit von Einwilligungen.
- Verschlüsselte Verarbeitung genetischer Daten und frühestmögliche Pseudonymisierung unter Einbindung unabhängiger Vertrauensstellen ggf. i. V. m. weiteren standardisierten Vorgaben zu den technischen und organisatorischen Maßnahmen einschließlich der Sicherheitsmaßnahmen und technisch implementierten Speicherbegrenzung und Löschung.[10]
- Lösch- und Vernichtungspflichten für die genetischen Daten und biologischen Proben mit einer gesetzlich festgelegten Aufbewahrungsdauer.
- Festlegung spezifischer sanktionsbewehrter Offenlegungs- und Übermittlungsverbote, insbesondere an Arbeitgeber oder Versicherungen und Strafbarkeit missbräuchlicher, zweck- und gesetzwidriger Nutzung genetischer Daten. Ein effektiver Schutz gegen die Beschaffung und Verwendung genetischer Proben ohne Kenntnis der betroffenen Personen sollte strafrechtlich geregelt werden.

[9] Petersberger Erklärung und Beschluss der DSK vom 27.04.2020, abrufbar unter: https://datenschutzkonferenz-online.de/media/dskb/20200427_Beschluss_MII.pdf.

[10] Arbeitspapier über genetische Daten, Artikel 29-Datenschutzgruppe, 12178/03/DE, 17.03.2004, S. 12.

- Zugang zu genetischen Daten von berechtigten Dritten nur nach einem Use & Access-Verfahren, das auch die datenschutzrechtlichen Grundsätze wie die Beschränkung des Zugangs für einen bestimmten wissenschaftlichen Forschungszweck, für eine bestimmte Zeit und für qualifizierte Forscherinnen und Forscher umfasst. Ein Datenzugriff berechtigter Dritter ist im Rahmen einer sicheren Verarbeitungsumgebung zu gewähren.
- Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung.
- Besonderer Schutz von Ungeborenen, Minderjährigen und nicht einwilligungsfähigen Personen, beispielsweise durch die Beschränkung bestimmter Forschungsziele sowie durch spezifische Aufklärung und Informationsbereitstellung für die gesetzlichen Vertreter (u. a. Personensorgeberechtigte, Vormunde, Betreuer).
- Vorgaben zur Wahrung der Anonymität der betroffenen Personen bei Publikation von Forschungsergebnissen.

Die DSK hat in ihrer Entschließung „Datenschutz in der Forschung durch einheitliche Maßstäbe stärken“ vom 23.11.2023 weitere angemessene und spezifische Maßnahmen für eine gesetzliche Regelung zur Verarbeitung von Gesundheitsdaten zu Forschungszwecken dargestellt, die zudem beachtet werden müssen.[11]

[11] DSK-Entschließung „Datenschutz in der Forschung durch einheitliche Maßstäbe stärken“ vom 23.11.2023, abrufbar unter https://www.datenschutzkonferenz-online.de/media/en/2023-11-23_DSK-Entschliessung_DS.pdf

5.6 Positionspapier Datenschutzrechtliche Grenzen des Einsatzes von Bezahlkarten zur Leistungsgewährung nach dem Asylbewerberleistungsgesetz (AsylbLG)

Beschluss
der Konferenz der unabhängigen Datenschutzaufsichtsbehörden
des Bundes und der Länder
am 19. August 20204

In einigen Kommunen ist eine sog. Bezahlkarte für die Auszahlung von Leistungen nach dem Asylbewerberleistungsgesetz (AsylbLG) bereits im Einsatz, in vielen anderen ist ihre Einführung in naher Zukunft vorgesehen. Auf Bund-Länder-Ebene wurden am 31. Januar 2024 bundeseinheitliche Mindeststandards[12] beschlossen. Aus diesen geht hervor, wie die Bezahlkarte ausgestaltet werden und welche technischen Möglichkeiten sie bieten soll. Seit dem 16. Mai 2024 ist zudem eine Änderung des AsylbLG in Kraft, wonach die Leistungsgewährung in bestimmten Konstellationen auch mithilfe einer Bezahlkarte erfolgen kann.[13] Bei der Bezahlkarte handelt es sich um eine guthabenbasierte Karte mit Debit-Funktion, aber ohne Verknüpfung mit einem herkömmlichen Girokonto. Die Einführung der Bezahlkarte erfolgt in der Praxis unter Einbindung eines Dienstleisters in Gestalt eines privatrechtlichen Bankunternehmens. Durch diese Art der Leistungsgewährung sowie die avisierten weiteren Funktionsmöglichkeiten der Karte entstehen zwangsläufig datenschutzrechtlich relevante Verarbeitungsvorgänge der personenbezogenen Daten von Leistungsberechtigten. Damit wird in das Recht der Leistungsberechtigten auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 Grundgesetz (GG) in Verbindung mit Art. 1 Abs. 1 GG eingegriffen, welches im Lichte des Rechts auf den Schutz personenbezogener Daten nach Art. 8 Charta der Grundrechte der EU (GRCh) in Verbindung mit Art 7 GRCh auszulegen ist.[14] Dieses Recht gilt gleichermaßen für deutsche wie ausländische Staatsangehörige, die sich in der Bundes-

[12] Siehe https://cdn.netzpolitik.org/wp-upload/2024/02/016-Anlage-2-Anforderungen-an-die-Bezahlkarte-Bundeseinheitliche-Mindeststandards.pdf (zuletzt abgerufen am 10. Juli 2024).

[13] BGBl. 2024 I Nr. 152 vom 15.05.2024, S. 29 f

[14] Siehe zu diesem Grundrechtsverständnis BVerfG, Beschluss vom 6.11.2019 – 1 BvR 16/13 Rn. 46, ff.

republik Deutschland aufhalten. Aus dem Grundrecht folgen Bedingungen und Grenzen, die bei der Umsetzung der Leistungsgewährung mittels Bezahlkarten zu berücksichtigen sind.

I. Datenschutzrechtliche Zulässigkeit der Leistungsmethode „Bezahlkarte“

Der Bundesgesetzgeber hat die Bezahlkarte in den §§ 2, 3 und 11 AsylbLG als eine Methode zur Leistungserbringung nun ausdrücklich gesetzlich normiert.[15] Dabei hat der Gesetzgeber darauf verzichtet, eine spezifische Rechtsgrundlage für die in den Leistungsbehörden bei Umsetzung der Bezahlkarte nunmehr anfallenden Verarbeitungen von personenbezogenen Daten zu schaffen. Für diese Vorgänge wird jedoch eine Rechtsgrundlage benötigt, die den Anforderungen von Art. 6 Abs. 1 UAbs. 1 Buchst. e, Abs. 3 DSGVO genügt. Deswegen hängt die datenschutzrechtliche Zulässigkeit der Leistungsmethode „Bezahlkarte“ davon ab, ob ein Rückgriff auf die Generalklauseln des Landesdatenschutzrechts5[16] erfolgen darf. Angesichts der in Bezug auf das Recht auf Schutz personenbezogener Daten hier als moderat zu bewertenden Eingriffsintensität ist dies prinzipiell möglich: Die behördliche Verarbeitungstätigkeit einschließlich der Datenweitergabe an den Dienstleister kann grundsätzlich auf die jeweilige landesdatenschutzrechtliche Generalklausel gestützt werden.[17]

Dies gilt allerdings nur, soweit ausschließlich die zur Leistungserbringung erforderlichen personenbezogenen Daten verarbeitet werden. Entscheidend für die Zulässigkeit der Verarbeitung personenbezogener Daten beim Einsatz der Bezahlkarte ist somit, welche Zwecke das AsylbLG fachrechtlich vorgibt und welche Verarbeitungsvorgänge zur Erreichung dieser Zwecke zwingend benötigt werden.

II. Datenschutzrechtliche Grenzen bei Umsetzung der Bezahlkarte

Die für Behörden geltenden rechtlichen Grenzen für die Verarbeitung von personenbezogenen Daten dürfen bei der Einbindung des privaten Zahlungsdienstleisters nicht überschritten werden. Insbesondere ist zu

[15] Siehe BT-Drucksache 20/1106.

[16] Siehe § 4 Abs. 1 BayDSG; § 5 Abs. 1 BbgDSG; § 3 BlnDSG; § 3 Abs. 1 BremDSGVOAG; § 4 DSAG LSA; § 4 Abs. 1 DSG M-V; § 3 DSG NRW; § 3 Abs. 1 HDSIG; § 4 HmbDSG; § 4 LDSG BW; § 3 LDSG RLP; § 3 Abs. 1 LDSG SH; § 3 NDSG; § 3 Abs. 1 SächsDSDG; § 4 Abs. 1 SDSG; § 16 Abs. 1 ThürDSG

[17] Von der Eingriffsintensität zu trennen ist die Risikobewertung, wie sie im Rahmen einer Datenschutz-Folgenabschätzung anhand der konkreten Funktionen der Bezahlkarte vorzunehmen ist.

beachten, dass es gemäß Art. 6 Abs. 1 UAbs. 2 DSGVO Behörden selbst nicht gestattet ist, eine Datenverarbeitung unter Verweis auf ein überwiegendes berechtigtes Interesse gemäß Art. 6 Abs. 1 Buchst. f DSGVO durchzuführen. Diese Vorgabe des europäischen Gesetzgebers darf nicht durch eine Auslagerung der Datenverarbeitung an eine nicht-öffentliche Stelle umgangen werden. Es wäre daher datenschutzrechtlich unzulässig, den Dienstleister – unter Verweis auf Art. 6 Abs. 1 UAbs. 1 Buchst. f DSGVO – bestimmte Datenverarbeitungen im Interesse der Behörden vornehmen zu lassen, wenn die Behörde diese nicht selbst, gestützt auf eigene Rechtsgrundlagen, durchführen darf.

Wird also im Folgenden erläutert, dass ein angestrebter Verarbeitungsvorgang nicht von einer Leistungsbehörde ausgeführt werden darf, so gilt dies auch für den jeweiligen Dienstleister, soweit er die Verarbeitung lediglich für Leistungsbehörden durchführt

1. Keine Einsichtnahme in den Guthabenstand

Eine eigenständige Einsichtnahme in den Guthabenstand von leistungsberechtigten Personen durch die Leistungsbehörden ist nach derzeitiger Rechtslage unzulässig. Ein solcher Abruf dieser Information ist eine Verarbeitung personenbezogener Daten, die eine Rechtsgrundlage benötigt. In Betracht käme hierfür einzig die o. g. datenschutzrechtliche Generalklausel nach dem jeweiligen Landesrecht. Deren Voraussetzung der Erforderlichkeit dieser Verarbeitung für die Gewährung der Leistungen nach dem AsylbLG ist jedoch nicht erfüllt. Durch Einfügen des Wortes „Bezahlkarte“ in die §§ 2, 3 und 11 AsylbLG hat der Gesetzgeber zwar deutlich gemacht, dass die zuständigen Behörden Leistungen durch den Einsatz einer guthabenbasierten Karte mit Debit-Funktion erbringen dürfen. Weder im Gesetzestext noch in der dazugehörigen Begründung findet sich jedoch ein Hinweis darauf, dass Leistungsbehörden Einsicht in den Guthabenstand nehmen dürfen.[18] Der Gesetzgeber hat gerade nicht vorgesehen, dass die Bezahlkarte den Leistungsbehörden ein Mehr an Informationen über die Leistungsberechtigten verschafft, als es bisher der Fall war. Eine vergleichbare Kontrollmöglichkeit bei der Ausgabe von Sachleistungen, Wertgutscheinen oder Bargeld existiert nicht. Dementsprechend würde durch eine Einsichtnahme-Funktion ein zusätzli-

[18] Siehe BT-Drucksache 20/11006, S. 101 ff

cher Eingriff erfolgen, der geeignet ist, den betroffenen Leistungsberechtigten das Gefühl ständiger Überwachung zu vermitteln und der offenkundig nicht benötigt wird, um die Leistung zu gewähren.
Selbst wenn im Einzelfall eine Leistungsbehörde Kenntnis über einen Guthabenstand benötigt, etwa weil die leistungsberechtigte Person ihre Karte verloren hat und ein bestehendes Guthaben auf eine neue Karte übertragen werden soll, bedarf es keines technischen Direktzugriffs für die Behörde. Als milderes Mittel kann die leistungsberechtigte Person über die Mitwirkungspflichten nach § 9 Abs. 3 AsylbLG i. V. m. §§ 60 ff. SGB I dazu angehalten werden, der Behörde beispielsweise vor Ort an einem Behördencomputer die Einsicht in den Guthabenstand zu ermöglichen.

2. Keine pauschale Einschränkung auf Postleitzahlen-Gebiete

Für die räumliche Einschränkung der Einsatzmöglichkeit der Bezahlkarte muss die Information verarbeitet werden, dass für betroffene Leistungsberechtigte Aufenthaltsbeschränkungen bestehen. Diese Information stellt auch dann ein personenbezogenes Datum dar, wenn sie über die Karte nur mittelbar mit der leistungsberechtigten Person verknüpft wird. Denn jede Karte ist eindeutig einer nach dem AsylbLG leistungsberechtigten Person zugeordnet und würde im Falle einer räumlichen Einsatzbeschränkung zugleich die Information enthalten, inwiefern die betroffene Person in ihrer Freizügigkeit eingeschränkt ist, mithin asyl- oder aufenthaltsrechtlichen Beschränkungen unterliegt. Für die Verarbeitung dieser Information wird daher eine Rechtsgrundlage benötigt. Auch hier kommt allein die Generalklausel des jeweiligen Landesdatenschutzrechts in Betracht, da keine bereichsspezifischen Rechtsgrundlagen existieren.
Die Voraussetzungen der Generalklausel(n) liegen jedoch in der Regel nicht vor. Der Verarbeitungsvorgang ist zur Leistungsgewährung grundsätzlich nicht erforderlich. Erforderlich kann nur eine Datenverarbeitung sein, die den Zweck der Leistungsgewährung gemäß dem AsylbLG verfolgt. Mit einer Beschränkung auf Postleitzahlengebiete werden jedoch über die Leistungsgewährung hinausgehende Zwecke verfolgt, namentlich die Durchsetzung räumlicher Aufenthaltsbeschränkungen nach dem Asyl- oder dem Aufenthaltsgesetz. Diese sind jedoch keine Voraussetzung für die Bewilligung von Grundleistungen nach den für die Bezahlkarte maßgeblichen Regelungen (§ 2 Abs. 2, § 3 Abs. 2, 3 u. 5 AsylbLG). Zum Zeitpunkt der Bewilligungsentscheidung fehlt es daher grundsätzlich an dem notwendigen fach-

rechtlichen Anknüpfungspunkt und somit an der Erforderlichkeit der Datenverarbeitung.[19]
Dies steht auch im Einklang mit § 11 Abs. 2 AsylbLG, der eine Verbindung zwischen dem Leistungsbezug und der Verletzung räumlicher Aufenthalts- und Wohnsitzpflichten herstellt. Das Vorliegen einer solchen Verletzung muss allerdings zunächst im Einzelfall festgestellt werden, bevor auf der Grundlage von § 11 Abs. 2 AsylbLG Leistungsbeschränkungen erfolgen dürfen. Dies ist schon deswegen geboten, weil ein Aufenthalt außerhalb des zugewiesenen Bereichs nicht zwingend gegen räumliche Beschränkungen verstößt, wie sich etwa aus den Möglichkeiten nach § 12 Abs. 5 AufenthG sowie § 57 AsylG zum rechtskonformen Verlassen des Aufenthaltsbereichs ergibt. Anders verhält es sich im Übrigen mit einer Einschränkung der Einsatzmöglichkeit der Bezahlkarte auf das Bundesgebiet. Der Aufenthalt im Bundesgebiet ist gemäß § 1 Abs. 1 Hs. 1 AsylbLG Voraussetzung für die Leistungsberechtigung. Diesbezüglich besteht folglich ein unmittelbarer Bezug zwischen dem Zweck des AsylbLG und der Datenverarbeitung, sodass die mit dieser Einschränkung einhergehende Datenverarbeitung keinen datenschutzrechtlichen Bedenken begegnet.

3. Trennung der Datensätze

Für den praktischen Einsatz von Bezahlkarten muss die Verwaltung auf einen Dienstleister zugreifen, der die Durchführung aller Transaktionen auf Bankebene übernimmt. Ist ein Dienstleister leistungsbehördenübergreifend tätig, werden durch ihn die Datensätze einer Vielzahl von Verantwortlichen verarbeitet. Es darf dadurch aber nicht dazu kommen, dass ein behördenübergreifendes Register auf Seiten des Dienstleisters entsteht. Denn in Gestalt des Ausländerzentralregisters existiert bereits ein bundesweites Register aller Personen mit ausländischer Staatsangehörigkeit mit dem Ziel, durch eine zentrale Datenhaltung divergierende ausländer- oder asylrechtliche Entscheidungen zur gleichen Person zu vermeiden. Es besteht folglich zur Erreichung dieses Zwecks kein Bedarf für ein weiteres Register. Insbesondere ist noch auf Folgendes hinzuweisen:

a) Angemessene technische und organisatorische Maßnahmen, insbesondere: Mandantentrennung

[19] Das Erfordernis eines fachrechtlichen Anknüpfungspunkts führt i.Ü. dazu, dass auch sonstige, dem AsylbLG fremde Zwecke nicht berücksichtigt werden dürfen, um eine PLZ-Beschränkung zu begründen. Dies gilt beispielsweise für die Erwägung, Kaufkraft innerhalb der jeweiligen Kommune halten zu wollen.

Mit Blick auf die Verpflichtung zur Gewährleistung der Sicherheit der Datenverarbeitung, Art. 32 DSGVO, ist zudem durch eine Mandantentrennung auf Seiten des Dienstleisters die Integrität und Vertraulichkeit der Daten der jeweiligen Leistungsbehörde sicherzustellen.

b) Kein behördenübergreifender Datenabgleich außerhalb der behördlichen Befugnisse

Die bei einem Dienstleister zusammenfallenden Datenbestände mehrerer Behörden dürfen nach derzeitiger Rechtslage zudem nicht durch diesen abgeglichen werden. Für einen solchen Datenabgleich beim Dienstleister steht keine Rechtsgrundlage zur Verfügung. Die spezialgesetzlichen Regelungen des Ausländerzentralregistergesetzes (AZRG) versperren den Zugriff auf datenschutzrechtliche Generalklauseln.

Überdies ergibt sich kein Mehrwert durch einen solchen Datenabgleich, insbesondere nicht hinsichtlich der Ermittlung eines etwaigen Leistungsmissbrauchs. Der Einsatz der Bezahlkarte ist eine Methode der Leistungsgewährung. Vor der Kartenausgabe, mithin auch vor der Weitergabe der Daten der Asylbewerber:innen an den Dienstleister, muss die Leistungsbehörde deren Leistungsberechtigung ohnehin prüfen. Bezöge die jeweilige Person bereits an anderer Stelle Leistungen, so würde sich dies aus dem Ausländerzentralregister ergeben. Ein Mehr an Erkenntnis könnte der Dienstleister nicht ermitteln. Vielmehr entstünde durch einen solchen Abgleich eine Parallelstruktur ohne erkennbaren Nutzen, dafür mit erheblichen Risiken für die Betroffenen und mit Blick auf die Datenrichtigkeit auch für die öffentlichen Stellen.

4. Keine Weitergabe der Ausländerzentralregister-Nummer an den Dienstleister

Nach gegenwärtiger Rechtslage ist eine Weitergabe der Ausländerzentralregister-Nummer (AZR-Nummer) an den Dienstleister rechtswidrig.

Die Übermittlung der AZR-Nummer an eine nicht-öffentliche Stelle sehen weder das AZRG noch die AZRG-Durchführungsverordnung für mit der hiesigen Konstellation vergleichbare Fälle vor. Die nach den §§ 25 und 27 AZRG zulässigen Übermittlungen von Informationen aus dem AZR an nicht-öffentliche Stellen sind nicht einschlägig.

Ferner ergibt sich aus § 10 Abs. 4 AZRG, dass die AZR-Nummer grundsätzlich nur im Verkehr mit dem vom Bundesamt für Migration und Flüchtlinge (BAMF) geführten Ausländerzentralregister genutzt werden darf. Zwar bestehen Ausnahmen nach § 10 Abs. 4 S. 2 AZRG.

Diese beinhalten jedoch keine Weitergabe der AZR-Nummer an nicht-öffentliche Stellen.
Angesichts der abschließenden, spezialgesetzlichen Regelungen des AZRG ist der Rückgriff auf die datenschutzrechtlichen Generalklauseln gesperrt. Im Übrigen würde es auch hier an der Erforderlichkeit in Bezug auf die Verfügbarkeit der AZR-Nummer für den Dienstleister fehlen (vgl. Nr. 3.b): Es ist Aufgabe der Leistungsbehörden, die Leistungsberechtigung einer Person festzustellen. Zu diesem Zweck werden diesen Daten aus dem Ausländerzentralregister zur Verfügung gestellt, § 18a AZRG. Nach Feststellung der Leistungsberechtigung wird der Bezahlkarten-Dienstleister zur Ausführung dieser Entscheidung herangezogen. Ein dann stattfindender Abgleich der AZR-Nummer kann gegenüber der bereits erfolgten Prüfung keine neuen Erkenntnisse liefern und ist daher auch nicht erforderlich
5. Zugriff der Sicherheitsbehörden auf Buchungsdaten
Infolge der Nutzung der Bezahlkarte werden personenbezogene Daten der leistungsberechtigten Personen erhoben und gespeichert, die erheblichen Aufschluss über die private Lebensgestaltung geben können. Zugriffe durch Sicherheitsbehörden dürfen vor diesem Hintergrund nur nach den gesetzlichen Maßgaben der einschlägigen Sicherheitsgesetze, z. B. der Strafprozessordnung erfolgen, die auch für andere Personen und deren Bankaktivitäten gelten:

5.7 DS-GVO privilegiert wissenschaftliche Forschung Positionspapier zum Begriff „wissenschaftliche Forschungszwecke“

Beschluss
der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder
am 11. September 2024

Viele Regelungen der Datenschutz-Grundverordnung (DS-GVO) beziehen sich auf den Begriff der „wissenschaftlichen Forschungszwecke“. Hierzu zählen Art. 5 Abs. 1 Buchst. b DS-GVO (Zweckbindung), Art. 9 Abs. 2 Buchst. j DS-GVO (Öffnungsklausel für die Verarbeitung besonderer Kategorien personenbezogener Daten), Art. 14 Abs. 5 Buchst. b DS-GVO (Einschränkung der Informationspflichten), Art. 17 Abs. 3 Buchst. d DS-GVO (Einschränkung des Rechts auf Löschung), Art. 21 Abs. 6 DS-GVO (Widerspruchsrecht) und

Art. 89 DS-GVO (besondere Garantien und Ausnahmen). Diese Regelungen privilegieren Datenverarbeitungen zu wissenschaftlichen Forschungszwecken und sehen bestimmte Ausnahmen und Einschränkungen von datenschutzrechtlichen Anforderungen vor.
Um festzustellen, ob diese privilegierenden Regelungen anwendbar sind, muss geprüft werden, ob eine Verarbeitung tatsächlich zu wissenschaftlichen Forschungszwecken erfolgt. Dies kann regelmäßig nur in einer Einzelfallbeurteilung erfolgen. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder möchte mit den folgenden Kriterien eine Hilfestellung bei dieser Beurteilung geben.
Auf europäischer Ebene entwirft der Europäische Datenschutzausschuss (EDSA) derzeit Leitlinien zur wissenschaftlichen Forschung. Sofern diese Leitlinien weitergehende oder ergänzende Kriterien vorsehen werden, werden diese zusätzlich zu beachten sein.
Nach Erwägungsgrund 159 S. 2 DS-GVO soll die Verarbeitung personenbezogener Daten zu wissenschaftlichen Forschungszwecken im Sinne der DS-GVO weit ausgelegt werden und die technologische Entwicklung und Demonstration, die Grundlagenforschung, die angewandte Forschung und die privat finanzierte Forschung einschließen. Zugleich soll diese Forschung nach Erwägungsgrund 159 S. 3 DS-GVO den festgelegten Zielen aus Art. 179 Abs. 1 AEUV Rechnung tragen, was den sozialen Fortschritt, ein ausgewogenes Wirtschaftswachstum, die Verbesserung der Lebensqualität und Themen der öffentlichen Daseinsvorsorge umfasst.[20] Damit schließt das Verfolgen begleitender wirtschaftlicher Motive nicht die wissenschaftliche Forschung im Sinne der DS-GVO aus, solange die Tätigkeit auf Erzielung eines gesellschaftlichen Nutzens gerichtet ist.
Bei der Auslegung des Begriffes der wissenschaftlichen Forschung sind die Bestimmungen der Europäischen Grundrechtecharta (GRCh) zu berücksichtigen. Die Regelungen der DS-GVO dienen dem Schutz des Grundrechts auf Datenschutz nach Art. 8 GRCh[21] unter Berücksichtigung der übrigen Grundrechte[22]; die forschungsbezogenen Regelungen der DS-GVO sollen den Ausgleich mit der Forschungsfreiheit nach Art. 13 GRCh gewährleisten. Maßgaben für die gesetzliche

[20] vgl. Grabitz/Hilf/Nettesheim/Eikenberg AEUV Art. 179 Rn. 30 f.

[21] Vgl. Jarass, Charta der Grundrechte der EU Art. 8 Rn 19.

[22] Art. 1 DS-GVO und Erwägungsgrund 4, der allerdings in seiner nicht abschließenden Aufzählung der von der DSGVO geachtet Freiheiten und Grundsätze die Forschungsfreiheit nicht ausdrücklich erwähnt

Ausgestaltung der Grundrechte ergeben sich aus Art. 52 GRCh, wonach Einschränkungen unter Wahrung des Verhältnismäßigkeitsgrundsatzes nur zulässig sind, wenn sie den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen entsprechen oder dem Schutz der Rechte und Freiheiten anderer dienen. Diese Maßgaben sind bei Auslegung und Anwendung der Regelungen so zu berücksichtigen, dass die kollidierenden Grundrechte unter Achtung ihres Wesensgehaltes miteinander in Einklang gebracht werden.[23]
Der EuGH hat sich bisher nur am Rande zur Forschungsfreiheit geäußert.[24] Bei der unionsrechtsautonomen Auslegung ist Art. 13 GRCh zu berücksichtigen. Da Art. 13 GRCh allerdings als vom deutschen Grundgesetz „inspiriert" gilt, kann die Rechtsprechung des Bundesverfassungsgerichts[25] zu einem gewissen Grad auch zur Auslegung von Art. 13 GRCh herangezogen werden.[26] Als Forschung gilt nach der Rechtsprechung des Bundesverfassungsgerichts und der Kommentarliteratur zu Art. 13 GRCh jede geistige Tätigkeit mit dem Ziel, in methodischer, systematischer sowie nachprüfbarer Art und Weise neue Erkenntnisse zu gewinnen.[27]
Der Begriff der Forschung ist personen- und institutionsunabhängig und umfasst auch die Ressort- und Industrieforschung, soweit diese die Forschungsfreiheit in Anspruch nehmen kann.[28]
Damit die privilegierenden Vorschriften der DS-GVO für die Verarbeitung personenbezogener Daten zu Zwecken wissenschaftlicher Forschung zur Anwendung kommen, müssen nach Feststellung der DSK folgende Kriterien erfüllt sein:

I. Methodisches und systematisches Vorgehen

Wissenschaftliche Forschung verlangt eine methodische und systematische Vorgehensweise.[29] Dabei sind fachspezifische Eigenarten und

[23] Jarass, Charta der Grundrechte der EU Art. 52 Rn 43 m.w.N.

[24] Roßnagel, ZD 2019, 157, 158 m. w. N.; im Zusammenhang mit Zollbestimmungen findet sich außerdem im Urteil vom 29.01.1985 (C-234/83, Gesamthochschule Duisburg) der Befund, dass mit "dem Begriff „wissenschaftliche Arbeiten", der sich auf die zu nicht kommerziellen Zwecken betriebene Forschung bezieht, (…) die Erlangung und Vertiefung wissenschaftlicher Erkenntnisse gemeint" sei.

[25] vgl. z. B. BVerfG, BVerfGE 35, 79, 112 f.; BVerfGE 47, 327, 367.

[26] Roßnagel, ZD 2019, 157, 158.

[27] BVerfG, BVerfGE 35, 79; Artikel 13 GRCh: Jarass, Charta der Grundrechte der Europäischen Union, 4. Aufl. 2021, Art. 13 Rn. 8.

[28] vgl. Maunz/Dürig, Stand: August 2023, Art. 5 Abs. 3 GG Rn. 102.

[29] BVerfG, BVerfGE 35, 79.

Besonderheiten zur Ermittlung der rationalen Wahrheit zu berücksichtigen.

II. Erkenntnisgewinn

Ein weiteres Kriterium für Forschung ist nach der Rechtsprechung des BVerfG das mit dem jeweiligen Vorhaben verbundene Ziel des Erkenntnisgewinns.

Die bloße Anwendung bereits gewonnener Erkenntnisse fällt demgegenüber ebenso wenig unter den Begriff der wissenschaftlichen Forschung wie der Einsatz wissenschaftlicher Methoden zu reinen Aufsichts-, Kontroll- Organisations- oder Werbezwecken.

III. Nachprüfbarkeit

Nach der Rechtsprechung des BVerfG ist auch das Kriterium der „Nachprüfbarkeit" wesentlich für wissenschaftliche Forschung.[30]

Eine Veröffentlichung (als Publikationen, Vorträge o. Ä.) der Forschungsergebnisse ist keine zwingende Voraussetzung wissenschaftlicher Forschung.

Gleichwohl dürfte eine auf Erkenntnisgewinnung gerichtete Tätigkeit dann aus dem Anwendungsbereich der Vorschriften der DS-GVO, die wissenschaftliche Forschung privilegieren, herausfallen, wenn bewusst eine Geheimhaltung der Ergebnisse beabsichtigt ist, um sie so systematisch einer Überprüfung durch die Fachgemeinschaft zu entziehen.

Denn grundsätzlich ist die Öffentlichkeit der Wissenschaft eine Funktionsbedingung für einen offenen wissenschaftlichen Diskurs. Die Öffentlichkeit ermöglicht die kritische Auseinandersetzung mit der angewandten Forschungsmethode und den Forschungsergebnissen und die Überprüfbarkeit im Fachkreis (Peer Review).

Im Rahmen des Kriteriums der Nachprüfbarkeit wird man deshalb verlangen, dass die Durchführung und die Ergebnisse des Forschungsvorhabens nach wissenschaftlichen Standards dokumentiert werden und nicht von vornherein eine Geheimhaltungsabsicht der oben beschriebenen Art besteht.

Dabei ist zu berücksichtigen, dass einer Veröffentlichung im Einzelfall Betriebs- oder Geschäftsgeheimnisse oder andere schutzwürdige Geheimhaltungsinteressen entgegenstehen können.

Für die Öffentlichkeit kann es z. B. ausreichend sein, dass eine Erfindung patentiert wird.

IV. Unabhängigkeit und Selbstständigkeit

[30] BVerfG, BVerfGE 35, 79.

Wissenschaftliche Forschung erfordert Unabhängigkeit und Selbstständigkeit.[31] Die Forschungsfreiheit hat daher auch gegenüber Auftraggebern zu bestehen. Zwar kann die wissenschaftliche Arbeit weisungsbegleitet sein, sie muss gleichzeitig aber autonom möglich sein.[32]
Soweit Auftraggeber weisend Einfluss auf den Untersuchungsverlauf oder den Umgang mit erlangten Ergebnissen nehmen und den Forschenden damit Spielräume nehmen so dass ihre Unabhängigkeit gefährdet wird, wird man wohl regelmäßig nicht von einer forschenden Tätigkeit des Auftragnehmers ausgehen können.
Eine bloße Kritik des Auftraggebers an der Forschung des Auftragnehmers ist hingegen unschädlich.

V. Gemeinwohlinteresse

Ein weiteres sich auch aus Art. 52 Abs. 1 GRCh ergebendes Kriterium für wissenschaftliche Forschungszwecke im Sinne der DS-GVO sind der gesellschaftliche Nutzen bzw. die Gemeinwohleffekte des Vorhabens.
Die in der DS-GVO vorgesehenen Privilegierungen wissenschaftlicher Forschungszwecke und die entsprechenden Einschränkungen der Rechte betroffener Personen sind nur dadurch zu rechtfertigen, dass wissenschaftliche Forschung dem Gemeinwohl zugutekommt und nicht ausschließlich kommerziellen oder sonstigen Einzelinteressen dient.

[31] Roßnagel, ZD 2019, 157, 158.
[32] vgl. Maunz/Dürig, Stand: August 2023, Art. 5 Abs. 3 GG Rn. 102.

5.8 Übermittlungen personenbezogener Daten an die Erwerberin oder den Erwerber eines Unternehmens im Rahmen eines Asset-Deals

Beschluss
der Konferenz der unabhängigen Datenschutzaufsichtsbehörden
des Bundes und der Länder
am 11. September 2024

Die Veräußerung eines Unternehmens kann grundsätzlich auf zwei Wegen erfolgen, nämlich entweder durch Übertragung von Anteilen an einer Gesellschaft als „Share Deal" oder durch Übertragung von Vermögenswerten und/oder Wirtschaftsgütern als „Asset Deal". Während die Verarbeitung von personenbezogenen Daten im Rahmen eines „Share Deals", abgesehen von Prüfungshandlungen während einer Due Diligence Prüfung, unproblematisch möglich ist, da nur die Anteile an einer Gesellschaft übertragen werden, diese ansonsten unverändert fortgeführt wird und mangels Änderung in der Person der oder des Verantwortlichen grds. keine Übermittlung personenbezogener Daten erfolgt, bedarf es bei der Übermittlung von personenbezogenen Daten im Rahmen eines „Asset Deals" in datenschutzrechtlicher Hinsicht einer differenzierten Betrachtung, die im Folgenden dargestellt wird.

Unter dem Begriff des Asset Deals ist dabei ein Unternehmenskauf zu verstehen, bei dem Wirtschaftsgüter/Vermögenswerte (engl.: Assets) eines Unternehmens wie beispielsweise Grundstücke, Gebäude, Maschinen, Kundenstamm, Rechte etc., im Rahmen der Singularsukzession auf die Erwerberin oder den Erwerber übertragen werden. Ein Asset Deal liegt zum Beispiel vor, wenn eine Einzelunternehmerin oder ein Einzelunternehmer (Veräußerer)[33] ihren bzw. seinen Betrieb an eine Nachfolgerin oder einen Nachfolger (Erwerber) übergibt und dabei beispielsweise die Maschinen, den Kundenstamm, die Firmierung etc. übernimmt und den Betrieb fortführt.

Insbesondere Einzelkaufleute, Handwerkerinnen und Handwerker oder Personengesellschaften sind bei einem Betriebsübergang mit zusätzlichen datenschutzrechtlichen Herausforderungen konfrontiert,

[33] Die Begriffe Veräußerer und Erwerber, Gläubiger und Schuldner, Zedent und Zessionar werden im Folgenden ausschließlich rechtstechnisch verwendet und weisen nicht auf das Geschlecht der Personen hin, die tatsächlich an dem Rechtsgeschäft beteiligt sind.

die sich bei dem – allein Kapitalgesellschaften möglichen – Share Deal gar nicht stellen. Die nachfolgenden Hinweise sollen den Betriebsinhaberinnen und -inhabern helfen, diesen Anforderungen gerecht zu werden.

I. Übermittlung personenbezogener Daten vor Abschluss des Asset Deals, sog. Due Diligence

Zum Zeitpunkt der Vertragsverhandlungen zwischen Veräußerern und potentiellen Erwerbern – also vor Abschluss eines Vertrages (des Asset Deals) – ist die Übermittlung von personenbezogenen Daten grundsätzlich unzulässig. Das bezieht sich insbesondere auf Daten von Kundinnen und Kunden, Lieferantinnen und Lieferanten und von Beschäftigten. Die Übermittlung dieser Daten an den potenziellen Erwerber ist aber zulässig aufgrund einer im Einzelfall vorliegenden freiwillig erteilten Einwilligung der von der Übermittlung betroffenen Personen. Im Rahmen der fortgeschrittenen Übernahmeverhandlungen kann im Einzelfall ein berechtigtes Interesse die Übermittlung von Daten besonders hervorgehobener Personen aus den vorgenannten Gruppen gemäß Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO rechtfertigen. Bspw. kann es sich dabei um Hauptvertragspartnerinnen und -partner, Personal mit Führungsverantwortung und/oder für das Geschäft zentralen Kompetenzen handeln.

Im Beschäftigungsverhältnis ist bei der Beurteilung der Freiwilligkeit die Abhängigkeit der Beschäftigten zu berücksichtigen. Freiwilligkeit kann ausnahmsweise vorliegen, wenn von Veräußerern und ihren Beschäftigten gleichgerichtete Interessen verfolgt werden. Die Einwilligung hat hier in aller Regel schriftlich oder elektronisch zu erfolgen, siehe § 26 Abs. 2 BDSG

II. Daten von Kundinnen und Kunden

Bei der Übermittlung von Daten der Kundinnen und Kunden vom Veräußerer an den Erwerber im Rahmen eines Asset Deals ist zwischen den Stadien einer Vertragsanbahnung, einer laufenden vertraglichen Beziehung des Veräußerers mit der jeweiligen Kundin oder dem jeweiligen Kunden und einer vollständig erfüllten oder beendeten vertraglichen Beziehung zwischen Veräußerer und der Kundin oder dem Kunden zu unterscheiden.

1. Vertragsanbahnung

Eine Vertragsanbahnung liegt vor, wenn zwischen dem Veräußerer und der Kundin oder dem Kunden konkrete Vertragsverhandlungen geführt werden. Führt die Kundin oder der Kunde die Verhandlungen mit dem Erwerber von sich aus rügelos fort, so ist die Verarbeitung

der für die Fortsetzung erforderlichen personenbezogenen Daten gerechtfertigt durch Art. 6 Abs. 1 UAbs. 1 Buchst. b DS-GVO. Im Übrigen ist eine Übermittlung nur dann zulässig, wenn eine Überprüfung durch den Veräußerer ergibt, dass den eigenen berechtigten Interessen an der Übermittlung keine überwiegenden Interessen der Kundin oder des Kunden entgegenstehen (Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO). Den berechtigten Interessen der Kundin oder des Kunden kann in aller Regel durch eine Widerspruchslösung Rechnung getragen werden. Den Kundinnen und Kunden wird dazu die Datenübermittlung an den Erwerber mit einer angemessenen Frist (etwa 6 Wochen) für einen möglichen Widerspruch angekündigt.

2. Laufende vertragliche Beziehungen

Eine laufende vertragliche Beziehung zwischen Veräußerer und der Kundin oder dem Kunden im hier gemeinten Sinne liegt vor, wenn der Veräußerer Verpflichtungen gegenüber einer Kundin oder einem Kunden aus einem Vertragsverhältnis (beispielweise Erbringung einer Leistung, Herstellung eines Werkes, Übergabe einer Kaufsache, Zahlung des Kaufpreises, Zahlung des Dienst- oder Werklohnes, Erfüllung etwaiger Mängelgewährleistungspflichten) hat, die noch nicht erloschen sind (beispielsweise durch Erfüllung) bzw. deren gesetzliche Verjährungs- oder vertragliche Garantiefristen noch nicht abgelaufen sind. Hierbei ist insbesondere darauf zu achten, dass beispielsweise Mängelgewährleistungsansprüche regelmäßig erst nach mehreren Jahren verjähren, so dass bis zu diesem Zeitpunkt von einer laufenden vertraglichen Beziehung auszugehen ist. Der Veräußerer sollte daher im Vorfeld des Abschlusses des „Asset Deals“ sorgfältig prüfen, zu welchen Kundinnen und Kunden noch eine laufende vertragliche Beziehung besteht und zu welchen nicht.

Werden die laufenden Verträge zwischen dem Veräußerer und den jeweiligen Kundinnen und Kunden mit der zivilrechtlich erforderlichen Genehmigung letzterer auf den Erwerber übertragen, so dass dieser die Verträge übernimmt und selbst neuer Schuldner und Gläubiger der jeweiligen Kunden wird (Vertragsübernahme), so erfüllt der Erwerber den Vertrag mit dem Kunden. Damit kann der Erwerber die für die durch ihn vorzunehmende Vertragserfüllung erforderliche Verarbeitung der Daten des Kunden auf Art. 6 Abs. 1 UAbs. 1 Buchst. b DS-GVO stützen. Entsprechendes gilt für den Fall der bloßen Schuldübernahme nach § 415 Abs. 1 BGB.

Soll allerdings der Erwerber lediglich den Veräußerer von dessen Schuld gegenüber den jeweiligen Kundinnen und Kunden freistellen,

handelt es sich hierbei um eine bloße Erfüllungsübernahme. Wird eine Erfüllungsübernahme zwischen Erwerber und Veräußerer vereinbart, ist zu prüfen, ob einer Übertragung der Daten der Kundinnen und Kunden vom Veräußerer auf den Erwerber überwiegende Interessen der Kundin oder des Kunden i. S. v. Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO entgegenstehen. Dies dürfte regelmäßig hinsichtlich der für die Erfüllung erforderlichen Daten nicht der Fall sein, weil die Kundin oder der Kunde vor allem an der Erfüllung interessiert sein dürfte und diese in der Regel durch den Erwerber besser gewährleistet werden kann, als durch den Veräußerer. Überwiegen allerdings im Einzelfall die Interessen an der Nichtübertragung der Daten, ist eine wirksame Einwilligung der betroffenen Kundin oder des Kunden erforderlich.

3. Beendete vertragliche Beziehung

Sofern der Veräußerer beabsichtigt, Daten ehemaliger Kundinnen und Kunden ohne laufende Verträge (Altdaten) dem Erwerber zur Erfüllung der gesetzlichen Aufbewahrungsfristen zu übermitteln, ist der Abschluss eines Vertrages über eine Auftragsverarbeitung gemäß Art. 28 Abs. 3 DS-GVO erforderlich. Diese Daten dürfen zwar übermittelt werden, aber eben nur zum Zwecke gesetzlicher Aufbewahrungsfristen genutzt werden. Der Erwerber hat diese Daten zwingend von den Daten der Kundinnen und Kunden mit einer laufenden vertraglichen Beziehung zu trennen („Zwei-Schrank-Lösung“).

Denkbare Alternative ist, dass entsprechende Daten der Kundinnen und Kunden beim Veräußerer verbleiben. Dieser kann die Daten als Verantwortlicher entweder selbst bis zum Ablauf der gesetzlichen Aufbewahrungsfristen speichern oder ein Dienstleistungsunternehmen im Wege einer Auftragsverarbeitung damit beauftragen.

Der Erwerber darf die zur Erfüllung der Aufbewahrungsfristen übergebenen Daten nur dann zu eigenen Zwecken nutzen, wenn hierfür eine wirksame Einwilligung der Kundinnen und Kunden jeweils vorliegt. (Die Daten können dann aus dem „Aufbewahrungsschrank“ in den „Schrank für aktive Kundinnen- und Kundenbetreuung“ übernommen werden.)

4. Werbung durch den Erwerber

Soweit Kontaktdaten der Kundinnen und Kunden nach den unter 2.1 und 2.2 genannten Kriterien vom Erwerber verarbeitet werden durften, können diese regelmäßig gemäß Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO in dem Umfang für Werbezwecke genutzt werden, wie dies auch durch den Veräußerer zulässig gewesen wäre. Dies ist dann nicht der Fall, wenn überwiegende Interessen der Kundin oder des Kunden

entgegenstehen. Insbesondere bei Werbemaßnahmen mithilfe elektronischer Post oder Telefon ist § 7 des Gesetzes gegen den unlauteren Wettbewerb (UWG) zu beachten. Danach erfordert insbesondere die Werbung per Telefon oder per E-Mail grundsätzlich eine vorherige ausdrückliche Einwilligung. Soweit es sich bei der kontaktierten Person nicht um eine Verbraucherin oder einen Verbraucher handelt, reicht im Falle von Werbung mittels eines Telefonanrufes eine mutmaßliche Einwilligung aus. Die Ausnahme des § 7 Abs. 3 UWG (elektronische Werbung ohne Einwilligung) findet regelmäßig keine Anwendung, da nach § 7 Abs. 3 Nr. 1 UWG derjenige, der die elektronische Postadresse verwendet, diese im Rahmen eines Vertragsabschlusses direkt bei der Kundin oder dem Kunden erhoben haben muss. Bei einem vorvertraglichen Schuldverhältnis besteht noch kein Vertragsverhältnis. Soweit eine bestehende Schuld gem. § 415 BGB durch den Erwerber übernommen wird, erhält dieser die E-Mail-Adresse in der Regel vom Veräußerer und nicht von der Kundin oder vom Kunden selbst. Im Übrigen wird auf die Orientierungshilfe der DSK zur „Verarbeitung von personenbezogenen Daten für Zwecke der Direktwerbung unter Geltung der DS-GVO“ verwiesen.[34]

5. Besondere Kategorien nach Art. 9 Abs. 1 DS-GVO der Daten von Kundinnen und Kunden

Besondere Kategorien von Daten der Kundinnen und Kunden, wie beispielsweise Gesundheitsdaten, können nur im Wege der informierten und ausdrücklichen Einwilligung nach Art. 9 Abs. 2 Buchst. a, Art. 7 DS-GVO vom Veräußerer auf den Erwerber übermittelt werden.

6. Bankdaten

Die Bankverbindungen (IBAN) können in den Fallgruppen der Ziffern 2.1 (Vertragsanbahnung) und 2.2 (laufende vertragliche Beziehungen) – soweit die tatbestandlichen Voraussetzungen vorliegen – über Art. 6 Abs. 1 UAbs. 1 Buchst. b DS-GVO an den Erwerber mit übermittelt werden, im Übrigen aber nur nach ausdrücklicher Einwilligung der Kundin oder des Kunden. Soweit vom Erwerber kein vom Veräußerer übergeleiteter Vertrag abzuwickeln ist, kann er kein berechtigtes Interesse an den Daten zur Bankverbindung geltend machen. Unabhängig von der Übermittlung der Bankverbindungsdaten benötigt der Erwerber neue Einzugsermächtigungen der Inhaberinnen

[34] Die Orientierungshilfe ist. u. a. aufrufbar unter https://datenschutz.sachsen-anhalt.de/fileadmin/Bibliothek/Landesaemter/LfD/Informationen/orientierungshilfen/OH_Werbung.pdf .

und Inhaber der Kontoverbindung, wenn er einen Bankeinzug von Forderungen beabsichtigt.

7. Daten von Kundinnen und Kunden im Falle offener Forderungen

Die Übertragung offener Forderungen richtet sich zivilrechtlich nach den §§ 398 ff BGB (Forderungsabtretung). In diesem Zusammenhang stehende Daten darf der Zedent (Alt-Gläubiger/Alt-Unternehmen) an den Zessionar (Neu-Gläubiger/Neu-Unternehmen) – gestützt auf Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO – übermitteln. Überwiegende Gegeninteressen bestehen dann, wenn die Abtretung durch Vereinbarung ausgeschlossen ist (§ 399 2. Alt. BGB). In diesen Fällen bleibt allerdings die Möglichkeit, den Erwerber oder einen Dritten zur Einziehung der Forderung im fremden Namen zu ermächtigen. Auch hier dürfen die zum Einzug erforderlichen personenbezogenen Daten gem. Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO übermittelt werden.

III. Personenbezogene Daten von Lieferantinnen oder Lieferanten und deren Beschäftigten

Soweit keine schutzwürdigen Gegeninteressen erkennbar sind, können aktuelle und für den Erwerber relevante personenbezogene Daten von Lieferantinnen und Lieferanten oder deren Beschäftigten nach Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO vom Veräußerer auf den Erwerber übermittelt werden. Insbesondere bei geschäftlichen Kontaktdaten dürften der Übermittlung regelmäßig keine überwiegenden Interessen entgegenstehen. Die Lieferantinnen oder Lieferanten dürften in der Regel sogar ein Interesse daran haben, dass eine bestehende Geschäftsbeziehung mit einem neuen Erwerber fortgesetzt wird.

IV. Beschäftigtendaten

Die Übermittlung von Beschäftigtendaten zur Vertragsdurchführung im Rahmen von „Asset-Deals“ vom Veräußerer auf den Erwerber kann – wenn es sich um einen Betriebs- oder Betriebsteilübergang nach § 613a BGB handelt – zum Zeitpunkt des Betriebs- oder Betriebsteilübergangs regelmäßig jedenfalls auf Art. 6 Abs. 1 UAbs. 1

Buchst. b DS-GVO[35] und, soweit besondere Kategorien von personenbezogenen Daten betroffen sind, auf § 26 Abs. 3 BDSG[36] gestützt werden. Der Veräußerer verarbeitet die Beschäftigtendaten dabei zur Erfüllung des Vertrages mit der oder dem Beschäftigten und zwar für die Beendigung beziehungsweise Abwicklung des Beschäftigungsverhältnisses zwischen ihm sowie den betroffenen Beschäftigten.
Der Erwerber darf die Beschäftigtendaten spiegelbildlich zur Erfüllung des Arbeitsvertrages nach § 613a BGB in Verbindung mit Art. 6 Abs. 1 UAbs. 1 Buchst. b DS-GVO und Art. 9 Abs. 2 Buchst. b DS-GVO in Verbindung mit § 26 Abs. 3 BDSG verarbeiten.
Allerdings kann es auch besondere Fallkonstellationen geben, in denen eine Datenübermittlung durch den Veräußerer auf den Erwerber nicht oder nicht vollständig erlaubt sein wird, unter anderem:

• Vertragsverhandlungen

Zum Zeitpunkt von bloßen Vertragsverhandlungen zwischen Veräußerern und potentiellen Erwerbern – also vor Abschluss eines Vertrages über den Übergang eines Betriebs und/oder Betriebsteils gemäß § 613a BGB – ist die Übermittlung von Beschäftigtendaten grundsätzlich unzulässig. Eine Übermittlung wird im Einzelfall möglicherweise nur mit einer wirksamen[37] Einwilligung der Beschäftigten zulässig sein.[38]

• Information der Beschäftigten durch Erwerber vor dem Betriebs-/Betriebsteilübergang

Beschäftigte, die von einem Betriebs- oder Betriebsteilübergang nach § 613a BGB betroffen sind, müssen hiervon nach § 613a Abs. 5 BGB

---

[35] Es bestehen – etwa aus Sicht des BAG, vgl. Az. 1 ABR 14/22, Beschluss vom 09.05.2023, Tz. 64 – Zweifel an der Europarechtskonformität und damit Anwendbarkeit des § 26 Abs. 1 Satz 1 BDSG im Zusammenhang mit einen Betriebs- oder Betriebsteilübergang nach § 613a BGB; vgl. EuGH, Rs. C-34/21, vom 30.03.2023 sowie BAG, a. a. O., Tz. 64.
Über Art. 288 AEUV gilt die DS-GVO als Verordnung der EU – und damit zumindest Art. 6 Abs. 1 Buchst. b DS-GVO – als Rechtsgrundlage für die Verarbeitung von personenbezogenen Daten zur Erfüllung (unter anderem) eines Arbeitsvertrages unmittelbar in allen Mitgliedstaaten.

[36] Gegen § 26 Abs. 3 BDSG bestehen keine unionsrechtlichen Bedenken; vgl. BAG, a. a. O., Tz. 48 ff.

[37] Es müssen die gesetzlich geregelten Voraussetzungen für eine freiwillige und damit rechtswirksame Einwilligung beachtet werden, § 26 Abs. 2, Abs. 3 Satz 2 BDSG. Weitere Hinweise hierzu finden Sie in dem Kurzpapier Nummer 20 der DSK zur „Einwilligung nach der DS-GVO“ unter dsk_kpnr_20.pdf (datenschutzkonferenz-online.de).

[38] Datenverarbeitungen im Rahmen einer „Due Diligence-Prüfung“ werden vorliegend nicht behandelt, vgl. hierzu Ausführungen auf Seite 1 dieses Dokuments.

in Textform unterrichtet werden. Die Information kann dabei durch den Veräußerer oder aber den Erwerber erfolgen, § 613a Abs. 5 BGB. Nach Zugang dieser Unterrichtung haben die betroffenen Beschäftigten einen Monat Zeit, dem Übergang ihres Arbeitsverhältnisses auf den Erwerber zu widersprechen, § 613a Abs. 6 BGB. Vereinbaren Veräußerer und Erwerber, dass der Letztere die betroffenen Beschäftigten nach § 613a Abs. 5 Alternative 2 BGB informieren soll, darf der Veräußerer bis zum Übergang des Betriebs- oder des Betriebsteils zunächst nur die erforderlichen Daten der Beschäftigten zur Abwicklung des Beschäftigungsverhältnisses an den Erwerber übermitteln, Art. 6 Abs. 1 UAbs. 1 Buchst. b DS-GVO. Eine Übermittlung von besonderen Kategorien personenbezogener Daten, wie zum Beispiel Arbeitsunfähigkeitsbescheinigungen als Personaldaten, ist hierfür nicht erforderlich.

• Widerspruch der oder des Beschäftigten vor dem Betriebs-/Betriebsteilübergang

Soll die Information der betroffenen Beschäftigten – wie regelmäßig üblich – durch den Veräußerer nach § 613a Abs. 5 Alternative 1 BGB erfolgen und widersprechen betroffene Beschäftigte bevor der Betrieb oder der Betriebsteil auf den Erwerber übergegangen ist, ist eine Übermittlung der Daten der widersprechenden Beschäftigten durch den Veräußerer auf den Erwerber nicht erforderlich und damit unzulässig.

• Kein Betriebs- oder Betriebsteilübergang nach § 613a BGB

Liegt ein Asset-Deal vor, der keinen Betriebs- oder Betriebsteilübergang nach § 613a BGB darstellt, sind für eine Übermittlung von Beschäftigtendaten individuelle Vereinbarungen zwischen Veräußerer, Erwerber und Beschäftigten zu treffen. Auch in diesen Fällen wird eine Übermittlung von Beschäftigtendaten regelmäßig nur mit einer freiwilligen und damit rechtswirksamen Einwilligung der betroffenen Beschäftigten möglich sein.[39]

V. Sonstige Hinweise

1. Bei allen Fallgruppen ist zu beachten:

• Die datenschutzrechtliche Verantwortung für die Übermittlung personenbezogener Daten an den Erwerber trifft den Veräußerer. Insbesondere muss der Veräußerer neben der Erfüllung der vorstehenden Anforderungen bei der Übermittlung ein angemessenes Schutzniveau

[39] Wegen der weiteren Einzelheiten zu einer rechtswirksamen Einwilligung wird auf die Ausführungen in der Fußnote 35 verwiesen.

gem. Art. 32 DS-GVO gewährleisten. Verarbeitet der Veräußerer weiterhin personenbezogene Daten seiner Kundinnen und Kunden (einschließlich des Falles, dass er den Erwerber als Auftragsverarbeiter einsetzt), ist er insoweit weiterhin für die Einhaltung seiner datenschutzrechtlichen Pflichten verantwortlich. Die Daten der Kundinnen und Kunden sind zu löschen, wenn die Voraussetzungen des Art. 17 DS-GVO vorliegen, es sei denn, Art. 17 Abs. 3 DS-GVO ist einschlägig (z. B. bei handels- oder steuerrechtlichen Aufbewahrungsfristen).
• Die datenschutzrechtliche Verantwortung für die Verarbeitung beim Erwerber trifft diesen.
Der Erwerber muss die Pflichten als „Verantwortlicher" (Art. 4 Nr. 7 DS-GVO) erfüllen, soweit er nicht als Auftragsverarbeiter für den Veräußerer tätig ist. Unter anderem muss er ein angemessenes Schutzniveau gewährleisten und bei Vorliegen der entsprechenden Voraussetzungen die Betroffenenrechte erfüllen.
• Soweit die Voraussetzungen von Art. 14 Abs. 5 DS-GVO nicht vorliegen, muss der Erwerber, innerhalb einer angemessenen Frist, spätestens innerhalb eines Monats nach Erhalt der Datensätze vom Veräußerer, die Kundinnen und Kunden gem. Art. 14 DS-GVO informieren, insbesondere hat er sie auch nach Art. 14 Abs. 2 Buchst. c DS-GVO auf ihr Widerspruchsrecht nach Art. 21 DS-GVO hinzuweisen. Ein Widerspruch wirkt sich nur auf die Datenverarbeitung nach dem Zeitpunkt des Widerspruchs aus.

2. Übermittlung von Daten der Kundinnen und Kunden als einziges „Asset"

Eine Übermittlung im Rahmen eines Verkaufs von Daten der Kundinnen und Kunden als losgelöstes „Asset" (Verkauf von Kundendatenbanken) ist regelmäßig nur mit vorheriger Einwilligung der betroffenen Kundinnen und Kunden möglich. Dies gilt insbesondere dann, wenn die Datenbanken zur Werbung für Geschäftstätigkeiten genutzt werden soll, die in keinem Zusammenhang mit dem ursprünglichen Unternehmen stehen.
Nur wenn Kleinstunternehmen (weniger als 10 Beschäftigte) oder Kleinunternehmen (weniger als 50 Beschäftigte und ein Jahresumsatz von höchstens 10 Mio. Euro)[40] aufgrund der Beendigung der eigenen

[40] Definition des Statistischen Bundesamts.

wirtschaftlichen Tätigkeit untereinander die Daten ihrer Kundinnen und Kunden einem Kleinst- oder Kleinunternehmen desselben Wirtschaftszweigs[41] übergeben, kann ausnahmsweise die einmalige Übermittlung ausschließlich der Postadressen im Wege einer Widerspruchslösung realisiert werden (z. B. der schließende Malerbetrieb A übergibt die Kundenadressen an einen bestehenden Malerbetrieb B, der aber weder Ausrüstung von Betrieb A übernimmt, noch in laufende Geschäftsbeziehungen eintritt).
Über die Übertragung ihrer Postadressen werden in diesem Fall die betroffenen Kundinnen und Kunden vom Veräußerer unterrichtet und ihnen wird mitgeteilt, dass sie innerhalb einer angemessenen Frist (i.d.R. 4 – 6 Wochen) formlos gegenüber dem Veräußerer widersprechen können. Im Falle des Ausbleibens eines Widerspruchs kann die Übermittlung der Postadressen als einziges Asset ausnahmsweise auf Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO gestützt werden. Diese Abwägung kann darauf gestützt werden, dass entsprechend Erwägungsgrund 13 Satz 4 der DS-GVO den Interessen der Kleinst- und Kleinunternehmen wegen der engen Kundenbeziehung und des besonderen Interesses an einer wirtschaftlich tragfähigen Regelung der Unternehmensnachfolge regelmäßig erhöhtes Gewicht zukommt und dem Schutz der Erwartungen und Interessen der Betroffenen durch ein voraussetzungsloses Widerspruchsrecht Rechnung getragen wird. Dem Veräußerer bleibt es unbenommen, Einwilligungen seiner bisherigen Kundinnen und Kunden auch zur Übermittlung von Telefonnummern und E-Mail-Adressen einzuholen.

[41] Nach den Festlegungen des Statistischen Bundesamts.

Stichwortverzeichnis