Tätigkeitsbericht Datenschutz

Berichtszeitraum:
1. Januar bis 31. Dezember 2025

Meine Daten.
Meine Freiheit.

SÄCHSISCHE
DATENSCHUTZ- UND
TRANSPARENZBEAUFTRAGTE

Freistaat
SACHSEN

Tätigkeitsbericht Datenschutz 2025 der Sächsischen Datenschutz- und Transparenzbeauftragten

Berichtszeitraum:
1. Januar bis 31. Dezember 2025

Rechtsstand: 31. Dezember 2025

Liebe Leserinnen und Leser,

2025 war vieles, aber gewiss nicht langweilig. Denn die Welt befindet sich in einer Phase des technologischen Umbruchs – maßgeblich beeinflusst durch die Entwicklungen auf dem Gebiet der Künstlichen Intelligenz. Solche Zäsuren sind Teil der Menschheitsgeschichte. Immer wieder gab es technische Fortschritte, die nicht nur einschneidend unsere Wirtschaft, sondern maßgeblich unser Leben verändert haben. Elektrizität und Autos gehören dazu. Auch Computer, das Internet und Smartphones waren Innovationen, die die vergangenen drei Jahrzehnte geprägt haben – und damit die Arbeit der Datenschutzbeauftragten. Damals wie heute dreht sich vieles, mit dem wir uns befassen, um die Frage: Wie kann eine Technologie oder Anwendung so genutzt werden, dass das Grundrecht auf Datenschutz in angemessener Weise gewahrt wird?

Die Antworten liegen nicht immer auf der Hand, die Abwägung im Spannungsfeld von Chancen und Risiken ist anspruchsvoll. Manchmal bedarf es gar gesetzlicher Änderungen. So hat die EU-Kommission im November ihren Vorschlag für eine Omnibus-Verordnung für den Digitalbereich vorgelegt, mit dem die bestehenden Vorschriften unter anderem im Bereich Datenschutz, Künstliche Intelligenz und Cybersicherheit geändert werden sollen (1.4). Als Mitglied der Datenschutzkonferenz befürworte ich zielführende Anpassungen der Datenschutz-Grundverordnung (DSGVO). Beispielsweise sollten Anbieter bzw. Hersteller von Standard-Hard- und Software datenschutzrechtlich mehr in die Verantwortung genommen werden. Auch die Rechte von Kindern gilt es zu stärken. Ebenso begrüße ich es, wenn die verschiedenen Digital- und Datenakte besser aufeinander abgestimmt werden, um mehr Rechtssicherheit und eine Vereinfachung für die Praxis zu erreichen. Das darf allerdings nicht dazu führen, dass unsere Grund- und Freiheitsrechte ausgehebelt werden. Bei der Datennutzung durch die Wirtschaft muss die Verhältnismäßigkeit ebenso gewahrt werden wie bei der staatlichen Datenverarbeitung, zum Bei-

spiel bei der Novellierung von Sicherheitsgesetzen wie dem Sächsischen Polizeivollzugsdienstgesetz (8.5). Der Wunsch nach möglichst umfassenden Befugnissen und ausgedehnter Datennutzung ist nicht nur auf staatlicher Seite erkennbar, sondern ebenso bei privaten Stellen. Hierzu sind mir wiederkehrend Fälle von Videoüberwachung bekannt geworden, bei denen Kamerabetreiberinnen und Kamerabetreiber schilderten, dass sie öffentliche Bereiche filmten, um zur Aufklärung von Straftraten beizutragen. Bei entsprechenden Vorfällen würde die Polizei die Aufzeichnungen anfordern. Um es klar zu sagen: Privatpersonen sind keine Sachwalter öffentlicher Interessen. Die Videoüberwachung des öffentlichen Raums bleibt unter engen Voraussetzungen allein öffentlichen Stellen vorbehalten: Selbst die Polizei bzw. die Polizeibehörden (Gemeinden) dürfen nur ganz bestimmte öffentliche Räume und nur unter strengen rechtlichen Anforderungen überwachen. (1.1, 1.2).

Froh bin ich, dass es mir mit meinem Team im Berichtszeitraum wieder gelungen ist, teils gravierende Datenschutzverstöße zu verfolgen und abzustellen. Eingegriffen haben wir beispielsweise bei einem extremen Fall der Videoüberwachung in einer Flüchtlingsunterkunft (2.2.8) und bei einem Sushi-Restaurant, das 3.000 Bestellungen mit den zugehörigen personenbezogenen Daten über das Internet offen zugänglich hatte (4.2.1). In einem anderen Fall hatte ein Mitarbeiter eines Krankenhauses ausgesonderte Computer des Arbeitgebers erworben und diese weiterverkauft. Einer der Käufer hat nach Wiederherstellung einer Partition Röntgenbilder und Befunde von Patientinnen und Patienten gefunden (4.2.2). Diese kleine Auswahl an Fällen deutet bereits an, wie vielseitig meine Tätigkeit ist. Oft unbeachtet bleibt die Tatsache, dass ich mit meiner Arbeit auch auf europäischer Ebene wirke. Über IMI – die Kommunikationsplattform der europäischen Aufsichtsbehörden – werde ich in einigen grenzüberschreitenden Verfahren tätig (6.2.7, 7.9).

Dass den Bürgerinnen und Bürgern der Schutz ihrer persönlichen Daten wichtig ist, belegt der Anstieg bei Beschwerden und Kontrollanregungen. Der Zuwachs betrug 29 Prozent

(6.2.2). Diese Flut an Eingaben führt leider zu längeren Bearbeitungszeiten – die Bürgerinnen und Bürger müssen länger auf eine Antwort warten. Auch die Zahl der Beratungsanfragen hat deutlich zugenommen. Bleibt das Beschwerdeaufkommen auf diesem Niveau, kann ich die Anforderungen der Datenschutz-Grundverordnung mit der derzeitigen Personalausstattung kaum mehr erfüllen (6.2.8).
Mit meinem nachfolgenden Bericht möchte ich Ihnen einen Einblick in meine Arbeit geben. Die zahlreichen Beiträge sollen zu rechtlicher Klarheit und dem Schutz personenbezogener Daten als unverzichtbarem Bestandteil einer freiheitlichen demokratischen Grundordnung beitragen. Wenn Sie an weiteren Informationen rund um „Datenschutz und Transparenz in Sachsen" interessiert sind, dann lege ich Ihnen meinen Newsletter ans Herz. Sie können ihn auf datenschutz.sachsen.de abonnieren.

Ich wünsche Ihnen eine erkenntnisreiche Lektüre!

Ihre

Dr. Juliane Hundert

Inhaltsverzeichnis

Abbildungsverzeichnis

Abkürzungsverzeichnis

Nachstehend werden Gesetze und andere Vorschriften nach der alphabetischen Reihenfolge der amtlichen, in Ausnahmefällen auch nichtamtlichen Abkürzung, ersatzweise der amtlichen Kurzbezeichnung aufgeführt.

Vorschriften

AO	Abgabenordnung
BDSG	Bundesdatenschutzgesetz
BGB	Bürgerliches Gesetzbuch
BKAG	Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten
BRAO	Bundesrechtsanwaltsordnung
DSGVO	Datenschutz-Grundverordnung
EEG	Gesetz für den Ausbau erneuerbarer Energien
EFZG	Entgeltfortzahlungsgesetz
EG	Erwägungsgrund
GG	Grundgesetz für die Bundesrepublik Deutschland
KI-VO	KI-Verordnung
KpS	Richtlinien des Sächsischen Staatsministeriums des Innern für die Führung Kriminalpolizeilicher personenbezogener Sammlungen in den Polizeidienststellen des Freistaates Sachsen
KunstUrhG	Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie
MBO	(Muster-)Berufsordnung
OWiG	Gesetz über Ordnungswidrigkeiten
OZG	Onlinezugangsgesetz
PersVG	Personalvertretungsgesetz
SächsAZVO	Sächsische Arbeitszeitverordnung
SächsBRKG	Sächsisches Gesetz über den Brandschutz, Rettungsdienst und Katastrophenschutz
SächsDSDG	Sächsisches Datenschutzdurchführungsgesetz
SächsDSG	Sächsisches Datenschutzgesetz

SächsDSUG	Sächsisches Datenschutz-Umsetzungsgesetz
SächsFrTrSchulG	Sächsisches Gesetz über Schulen in freier Trägerschaft
SächsGemO	Sächsische Gemeindeordnung
SächsJOrgVO	Sächsische Justizorganisationsverordnung
SächsJVollzDSG	Sächsisches Justizvollzugsdatenschutzgesetz
SächsLJHG	Sächsisches Landesjugendhilfegesetz
SächsLKrO	Sächsische Landkreisordnung
SächsPBG	Sächsisches Polizeibehördengesetz
SächsPVDG	Sächsisches Polizeivollzugsdienstgesetz
SächsSchulG	Sächsisches Schulgesetz
SächsStVollzG	Sächsisches Strafvollzugsgesetz
SächsVermKatG	Sächsisches Vermessungs- und Katastergesetz
SächsVSG	Sächsisches Verfassungsschutzgesetz
Sächs. VwV	Sächsische Verwaltungsvorschrift
SächsVwVfZG	Gesetz zur Regelung des Verwaltungsverfahrens- und des Verwaltungszustellungsrechts für den Freistaat Sachsen
SBGG	Gesetz über die Selbstbestimmung in Bezug auf den Geschlechtseintrag
SGB	Sozialgesetzbuch
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
StVG	Straßenverkehrsgesetz
StVollzG	Strafvollzugsgesetz
TDDDG	Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz
UWG	Gesetz gegen den unlauteren Wettbewerb
VwZG	Verwaltungszustellungsgesetz
WaffG	Waffengesetz
ZPO	Zivilprozessordnung

Sonstiges

a. a. O.	am angegebenen Ort
a. F.	alte Fassung
Abs.	Absatz
AK	Arbeitskreis
Art.	Artikel
Az.	Aktenzeichen

BAG	Bundesarbeitsgericht
BayVGH	Bayerischer Verwaltungsgerichtshof
BfDI	Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
BGH	Bundesgerichtshof
BKA	Bundeskriminalamt
BT-Drs.	Bundestags-Drucksache
Buchst.	Buchstabe
BVerwG	Bundesverwaltungsgericht
BZSt	Bundeszentralamt für Steuern
DSK	Konferenz der unabhängigen Datenschutzbeauftragten des Bundes und der Länder – Datenschutzkonferenz
EDSA	Europäischer Datenschutzausschuss
ePrivacy-RL	ePrivacy-Richtlinie
EU	Europäische Union
EuGH	Europäischer Gerichtshof
IMI	Internal Market Information System
JCAS	Joint Communication and Sensing
JVA	Justizvollzugsanstalt
KI	Künstliche Intelligenz
LDS	Landesdirektion Sachsen
LfV	Landesamt für Verfassungsschutz
LG	Landgericht
LKA	Landeskriminalamt
LT-Drs.	Landtags-Drucksache
MBl. SMK	Ministerialblatt des Sächsischen Staatsministeriums für Kultus
NADIS	Nachrichtendienstliches Informationssystem des Bundesamtes und der Landesbehörden für Verfassungsschutz
OLG	Oberlandesgericht
OVG	Oberverwaltungsgericht
PASS	Polizeiliches Auskunftssystem Sachsen
Rn.	Randnummer
SächsABl SDr.	Sächsisches Amtsblatt Sonderdruck
S.	Seite
SMI	Sächsisches Staatsministerium des Innern
SMJus	Sächsisches Staatsministerium der Justiz
VG	Verwaltungsgericht

VGH	Verwaltungsgerichtshof
VwV	Verwaltungsvorschrift
ZASt	Zentrale Anlaufstelle
ZVR	Zeugnisverweigerungsrecht

Sachgebietsregister

mit „*“ ausschließlich öffentlicher Bereich
ohne „*“ nichtöffentlicher Bereich bzw.
öffentlicher und nichtöffentlicher Bereich

Verzeichnis von Verarbeitungstätigkeiten, Kooperationspflicht	
Videografie und Bildverarbeitung	
• Behördliche Überwachung/Verarbeitung*	1.2
• Beschäftigte, vgl. ansonsten *Beschäftigtendatenschutz*	
• Dashcam, Drohnen	vgl. 6.4.3
• Handel, Gewerbe	2.2.6, 2.2.7
• Wohnbereiche	2.2.8
• Sonstiges, Allgemeines	1.1, 2.2.5, 2.3.4, vgl. 6.4.2
Wahlrecht*	
Zertifizierung, Akkreditierungen, Prüfsiegel	

Richtlinie (EU) 2016/680

Polizei*	1.1, 6.4.1, 8.2, 8.5, 8.6
Ordnungswidrigkeitenbehörden*	2.2.11, 2.2.12, 2.2.13
Strafverfolgung*	8.3
Straf- und Justizvollzug*	2.4.1, 8.4

Sonstige Bereiche (außerhalb Verordnung 2016/679 und Richtlinie EU 2016/680)

Sächsischer Landtag als Parlament	
Verfassungsschutz	8.1
Weitere datenverarbeitende Stellen	

1 Datenschutz im Freistaat Sachsen

1.1 Private Videoüberwachung zum Zweck der Verfolgung von Straftaten und Weitergabe von Videosequenzen an Ermittlungsbehörden

↗ §2 Abs. 1 SächsPBG; § 2 Abs. 1, § 4 Nr. 1 und 2 SächsPVDG; Art. 6 Abs. 1 Buchst. c, e, f DSGVO

Private Kamerabetreiber/innen begründen ihre Videoüberwachung meistens damit, dass diese der Prävention, Aufdeckung und Verfolgung von Straftaten dienen würde. Im gewerblichen Kontext kommt es nicht selten vor, dass sie dabei nicht nur Straftaten, die ihr Eigentum betreffen, im Blick haben. Vielmehr heben sie besonders hervor, dass sie damit (auch) einen Beitrag zum Schutz der öffentlichen Sicherheit und Ordnung und damit der Allgemeinheit leisten wollen.

Gerade Betreiber/innen von Einkaufsmärkten, Diskotheken oder Spielhalleninhaber/innen beabsichtigen mit dieser Argumentation, die Videoüberwachung öffentlich-zugänglicher Bereiche und öffentlicher Verkehrsflächen mit dort vorkommenden Straftaten wie Drogenhandel, -missbrauch, Körperverletzungsdelikten oder auch Diebstahl (Smartphone, Geldbörse, Fahrräder) oder Sachbeschädigung (Kraftfahrzeug) des Eigentums von Kunden bzw. Kundinnen zu rechtfertigen. Sie berichten in diesem Zuge von regelmäßigen Anfragen der Polizei, an die sie einzelne Videosequenzen nach vorheriger Nennung der jeweiligen Tagebuchnummern herausgeben. Gefragt nach dem Ausgang möglicher Ermittlun-

gen, räumen sie dann allerdings ein, in diesen Fällen keine Kenntnis zu haben.

Als Rechtfertigung für eine Videoüberwachung kommen zwar grundsätzlich alle der in Art. 6 Abs. 1 DSGVO enthaltenen Erlaubnisgründe infrage. Bei genauerer Betrachtung ist jedoch nur die Wahrung berechtigter Interessen überhaupt denkbar (Art. 6 Abs. 1 Buchst. f DSGVO). Danach ist die Verarbeitung personenbezogener Daten zulässig, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

Zwar können jegliche rechtlichen, tatsächlichen, wirtschaftlichen und ideellen Interessen berechtigte Interessen darstellen, wenn sie mit der Rechtsordnung in Einklang stehen. Die Vorschrift sieht aber eine Einschränkung vor, muss es sich doch um das „berechtigte Interesse des Verantwortlichen oder eines Dritten" handeln. Im Rahmen des Gesetzgebungsverfahrens zum Erlass der Datenschutz-Grundverordnung hat sich der Unionsgesetzgeber explizit mit dem Begriff des berechtigten Interesses befasst. Allerdings hat gerade der Vorschlag, auch Verarbeitungen im Interesse der öffentlichen Sicherheit zu erlauben, gerade keinen Niederschlag in Art. 6 Abs. 1 Buchst. f DSGVO gefunden. Folglich sind nur subjektive Interessen des Verantwortlichen oder Dritten von der Vorschrift gedeckt. Ohnehin ist nach dem Begriffsverständnis eine Bezugnahme auf öffentliche Interessen auszuschließen.

In der Meta-Entscheidung vom 4. Juli 2023 (Az. C-252/21) stellte der Europäische Gerichtshof klarstellend fest, dass das Ziel der Information von Strafverfolgungs- und Strafvollstreckungsbehörden, um Straftaten zu verhindern, aufzudecken und zu verfolgen oder festzustellen, grundsätzlich kein berechtigtes Interesse des Verantwortlichen im Sinne der Vorschrift darstellen kann. Im konkreten Fall resümierte das höchste europäische Gericht weiter, dass ein privater

„Achtung Kamera!" als PDF:
↗ sdb.de/achkam

„Achtung Kamera!" als gedruckte Broschüre:
↗ publikationen.sachsen.de/bdb/artikel/43382

Wirtschaftsteilnehmer sich nicht auf ein solches berechtigtes Interesse berufen kann, das mit seiner wirtschaftlichen und kommerziellen Tätigkeit nichts zu tun hat.

Demzufolge begründet die Information von Strafverfolgungs- und Strafvollstreckungsbehörden über Straftaten ohne Bezug zu eigenen schutzwürdigen Interessen und damit letztlich Allgemeininteressen grundsätzlich kein berechtigtes Interesse von Privatpersonen oder privaten Wirtschaftsteilnehmern und -teilnehmerinnen. Anders stellt sich der Fall dar, wenn ein Allgemeininteresse den persönlichen Interessen des Verantwortlichen entspricht, welche auch in der Abwehr einer Gefährdung für eigene Rechtsgüter bestehen und mithin schutzwürdige Interessen des Verantwortlichen belegen können. Beispiele sind die Verhinderung von Betrug (Erwägungsgrund 47 Satz 6) oder die Information der zuständigen Behörden über mögliche Straftaten oder eine Bedrohung der öffentlichen Sicherheit, wenn sich aus der eigenen Verarbeitung von Daten durch den Verantwortlichen entsprechende Anhaltspunkte ergeben (Erwägungsgrund 50 Satz 9).

Andere mögliche Rechtfertigungsgründe aus dem Katalog des Art. 6 Abs. 1 DSGVO scheiden aus. So gibt es für private Stellen keine rechtliche Verpflichtung, personenbezogene Daten präventiv zu erheben und zu speichern, um auf die Erlangung bestimmter Daten abzielende Anfragen einer nationalen Behörde – mithin im Vorliegenden der Strafverfolgungsbehörden – beantworten zu können, Art. 6 Abs. 1 Buchst. c DSGVO.

Nach den Wertungen des Bundesverwaltungsgerichts im Urteil vom 27. März 2019 (Az. 6 C 2.18) kann eine Videoüberwachung von vornherein auch nicht auf Art. 6 Abs. 1 Buchst. e DSGVO gestützt werden. Dies wäre nur dann der Fall, wenn der Private eine Aufgabe wahrnimmt, die im öffentlichen Interesse liegt oder die in Ausübung öffentlicher Gewalt erfolgt und die Privaten übertragen worden ist. Eine darauf beruhende Verarbeitung ist auf behördliche oder staatlich veranlasste Verarbeitungsvorgänge beschränkt. Um anstelle einer Behörde zu handeln, bedarf es eines wie auch immer gestalteten staatlichen Übertragungsakts an eine Privat-

person. Jedoch kann eine Privatperson sich nicht selbst zum Sachwalter des öffentlichen Interesses erklären.

Die Aufrechterhaltung der öffentlichen Sicherheit und Ordnung ist eine rein hoheitliche Aufgabe, die nur den damit betrauten staatlichen Stellen überlassen ist. Per Gesetz ist die Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung explizit auf die Polizeibehörden sowie die Polizei übertragen, § 2 Abs. 1 Sächsisches Polizeibehördengesetz (SächsPBG), § 2 Abs. 1 Sächsisches Polzeivollzugsdienstgesetz (SächsPVDG). Privatpersonen sind hierzu nicht berufen. Der Polizei obliegt zudem der Schutz der freiheitlichen demokratischen Grundordnung, § 2 Abs. 1 Satz 2 SächsPVDG. Die öffentliche Sicherheit umfasst unter anderem die Unverletzlichkeit der Rechtsordnung, der subjektiven Rechte und Rechtsgüter einzelner Personen. Öffentliche Ordnung meint die Gesamtheit der im Rahmen der verfassungsmäßigen Ordnung liegenden ungeschriebenen Regeln für das Verhalten von Personen in der Öffentlichkeit, deren Beachtung (§ 4 Nr. 1 und 2 SächsPVDG). Wollte man nach alldem gleichwohl eine in diese Richtung zielende Auslegung der Vorschrift des Art. 6 Abs. 1 Buchst. f DSGVO implizieren, würde zwangsläufig die in Art. 6 Abs. 1 Buchst. e DSGVO geregelte (ausdrückliche) Übertragung hoheitlicher Aufgaben auf private Stellen als Rechtsgrund für eine Datenverarbeitung leerlaufen und wäre letztlich obsolet. In gleicher Weise müsste hinterfragt werden, wozu es überhaupt klar und eng umrissener Vorschriften für staatliche Akteure bedarf.

Anzumerken ist auch, dass es aus rechtsstaatlichen Gründen mehr als bedenklich wäre, wenn Private dort eine Videoüberwachung vornehmen könnten, wo staatliche Stellen auf der Basis des ihnen zur Verfügung stehenden rechtlichen Instrumentariums daran gehindert sind. Es ist schlicht nicht die Aufgabe privater Stellen, fehlende Befugnisse staatlicher Stellen durch eigene Videoüberwachung auszugleichen oder zu ergänzen. Umgekehrt ist es dem Staat rechtlich nicht gestattet, ohne ausdrückliche Rechtsgrundlage Handeln auf Private auszulagern, um sich ihrer informationell zu bedienen. Staatliche Gewalt ist gesetzlich determiniert und be-

grenzt. Insoweit darf es auch keine durch „stillschweigendes Einverständnis" zwischen privaten und staatlichen Stellen vereinbarte Auslagerung von Datenverarbeitungsvorgängen, die im staatlichen Interesse liegen, auf Private geben, wenn hierfür keine ausdrückliche gesetzliche Grundlage existiert. Ansonsten käme dies einer (unzulässigen) Ausweitung gesetzlicher Befugnisse der staatlichen Stellen quasi „durch die Hintertür" gleich, ein dem Rechtsstaatsgrundsatz widersprechender Akt.

Der Europäische Gerichtshof hat in Bezug auf die Videoüberwachung mit der Entscheidung vom 4. Juli 2023 zusätzlich dahingehend für Rechtsklarheit gesorgt und verdeutlicht, dass eine Videoüberwachung nicht permanent und flächendeckend erlaubt ist, sondern nur unter klar umrissenen Bedingungen. Dies gilt sowohl für öffentliche Stellen wie Kommunen oder die Polizei als auch für nichtöffentliche Stellen wie Privatpersonen, Unternehmen und Vereine.

In meiner Funktion als Aufsichtsbehörde treffe ich meine Entscheidungen auf der Grundlage bestehender Gesetze. Ich habe bei meiner Tätigkeit auch die Rechtsprechung zu beachten, die die oft unbestimmten Rechtsbegriffe mit Leben füllt und richtungsweisend für die Verwaltung ist. Als Teil der Exekutive ist meine Behörde von Verfassungs wegen an Recht und Gesetz und damit auch an höchstrichterliche Entscheidungen über die Anwendung des Rechts gebunden, Art. 20 Abs. 3 Grundgesetz. Das Legalitätsprinzip verpflichtet sowohl Behörden als auch die Justiz dazu, ihre Entscheidungen ausschließlich auf einer gesetzlichen Grundlage zu treffen. Eine Missachtung der höchstrichterlichen Rechtsprechung würde nichts weniger als einem Verstoß gegen die freiheitliche demokratische Grundordnung gleichkommen (Gesetzmäßigkeit der Verwaltung).

Ich bin mir daher bewusst, dass ich dabei nicht alle Ansprüche erfüllen kann, gerade in Fällen einer Videoüberwachung. Jedoch darf nicht vergessen werden, dass es bei dem Recht auf informationelle Selbstbestimmung als Grundlage des Datenschutzrechtes um nichts weniger als um eines der elementaren Freiheitsrechte jedes Einzelnen geht. Als im Grund-

gesetz verankertes Menschenrecht zählt das Recht auf informationelle Selbstbestimmung zu den Verfassungsprinzipien und damit unverzichtbaren Bestandteilen der freiheitlichen demokratischen Grundordnung.

Meine Ausführungen machen letztlich exemplarisch das Spannungsverhältnis zwischen den wechselseitigen Positionen – auf der einen Seite die Aufrechterhaltung und Sicherstellung der öffentlichen Sicherheit und Ordnung, auf der anderen Seite die Freiheitsrechte, namentlich das Recht auf informationelle Selbstbestimmung – evident. Was aus Sicht mancher und auch staatlicher Ermittlungsbehörden wünschenswert oder gar unabdingbar erscheint, stört wiederum andere Personen, die eine Rechtsverletzung (Recht auf informationelle Selbstbestimmung) darin ausmachen und ein datenschutzaufsichtliches Einschreiten verlangen.

Ich gebe an dieser Stelle ausdrücklich zu bedenken, dass – wollte man ernsthaft und in letzter Konsequenz einer flächendeckenden Videoüberwachung durch private Stellen Tür und Tor öffnen – kaum noch überwachungsfreie Räume bestehen würden; ein Umstand, der nicht ernsthaft in einer freiheitlichen Demokratie erstrebenswert ist. Deshalb können sich Bürger und Bürgerinnen weiter in großen Teilen der Öffentlichkeit überwachungsfrei bewegen. Sich daraus ergebende Spannungen und Widersprüche zwischen den unterschiedlichen Ansprüchen muss ein Rechtsstaat in letzter Konsequenz aushalten.

Zusammenfassend lässt sich feststellen, dass öffentliche und öffentlich zugängliche Bereiche von Privaten zur Verhütung und Verfolgung sowie Aufklärung von Straftaten, die in keinem Bezug zu eigenen subjektiven Interessen des Kamerabetreibers sowie Dritter stehen, nicht überwacht werden dürfen. Die Prävention und Verfolgung von Straftaten ist eine staatliche Aufgabe, die aus gutem Grund nicht in private Hände gegeben ist.

Was ist zu tun?

Die Prävention und Aufklärung von Straftaten ist eine hoheitliche Aufgabe, die einzig den Polizeibehörden und der Polizei obliegt. Private Stellen sind nicht Sachwalter öffentlicher Interessen. Sie nehmen bei einer Videoüberwachung öffentlich und öffentlich zugänglicher Bereiche und eine Weitergabe entsprechender Videosequenzen an staatliche Ermittlungsbehörden auch keine berechtigten Interessen wahr.

1.2 Videoüberwachung durch Kommunen auf öffentlichen Plätzen

↗ § 13 Abs. 1 SächsDSDG, § 3 SächsPBG, § 30 Abs. 1 SächsPBG, § 4 Nr. 3 Buchst. c SächsPVDG, § 57 Abs. 3 SächsPVDG

Videoüberwachung ist ein datenschutzrechtlicher Dauerbrenner. Im Bereich der Kommunen haben sich sowohl Beschwerden als auch Anfragen seitens der Verantwortlichen selbst zur Rechtmäßigkeit der Videoüberwachung erneut gehäuft.

Manche Gemeinden fragen mich zur geplanten Videoüberwachung an, auch wenn eigentlich kein Erlaubnisvorbehalt besteht und die Videoüberwachung stets in eigener Verantwortlichkeit betrieben wird. Auch wenn dies nicht per se notwendig ist, begrüße ich solche Anfragen dennoch. Es kommt nämlich auch vor, dass zu einer bereits betriebenen Videoüberwachung berichtet wird und diese sich nach eingehender Prüfung als rechtswidrig erweist. An dieser Stelle ist auch nicht ausgeschlossen, dass ich gezwungen bin, ein förmliches Aufsichtsverfahren gegen die verantwortliche Gemeinde zu führen, wenn trotz Intervention meinerseits eine Abschaltung nicht erfolgt. Auch hierzu gab es im Berichtszeitraum leider Anlass.

Deswegen ist es mir ein großes Anliegen, die gesetzlich vorgegebenen Anforderungen an eine kommunale Videoüberwachung im öffentlichen Raum zu betonen. Es stehen an dieser Stelle zwei Rechtsgrundlagen zur Verfügung, die aber ganz unterschiedliche Schutzzwecke verfolgen und daher auch in ihren Voraussetzungen unterschieden werden müssen – § 13 Abs. 1 Sächsisches Datenschutzdurchführungsgesetz (SächsDSDG) und § 30 Abs. 1 Sächsisches Polizeibehördengesetz (SächsPBG).[1]

Möchte nämlich die Gemeinde (oder eine andere öffentliche Stelle) die eigenen Dienstgebäude und andere in ihrem Besitz befindlichen Gebäude überwachen, so kann dies durchaus datenschutzrechtlich zulässig sein, wenn die gesetzlichen Anforderungen dazu eingehalten werden. Insbesondere ist der Beschäftigtendatenschutz in Bezug auf die eigenen Be-

1 Diese Regelung befindet sich derzeit in gesetzgeberischer Novellierung und soll demnächst wesentlich überarbeitet werden, es wird in diesem Beitrag indes nur der aktuelle Rechtsstand berücksichtigt. Es ist aber nicht zu erwarten, dass die Eingriffsschwelle abgesenkt wird, sodass der Beitrag auch über den Novellierungszeitpunkt hinaus mit hoher Wahrscheinlichkeit Gültigkeit haben wird.

diensteten zu wahren. Diese Videoüberwachung lässt sich mit dem Hausrecht und auch unter Umständen der Erforderlichkeit zur gemeindlichen Aufgabenerfüllung gemäß § 13 Abs. 1 SächsDSDG begründen. Diese Art der Videoüberwachung soll nicht im Fokus dieses Beitrags sein.

Problematisch ist vielmehr die Videoüberwachung im öffentlichen Raum, die die Gemeinden in ihrer Funktion als Polizeibehörde durchführen oder planen, und die auf die Rechtsgrundlage des (derzeit noch geltenden) § 30 Abs. 1 SächsPBG gestützt wird. Die gesetzliche Hürde dieser Regelung ist aber relativ hoch, sodass in den allermeisten Fällen die Sachlage eine Videoüberwachung an dieser Stelle nicht rechtfertigen kann.

Hierzu muss nämlich gemäß § 30 Abs. 1 Nr. 1 SächsPBG am zu überwachenden Ort **eine erhebliche Gefahr für die öffentliche Sicherheit** vorliegen.

Die Definition der erheblichen Gefahr ist der Regelung des § 4 Nr. 3 Buchst. c SächsPVDG zu entnehmen (über die Verweisungsvorschrift des § 3 SächsPBG gilt diese auch im Anwendungsbereich des SächsPBG):

> „erhebliche Gefahr: Eine Sachlage, bei der im Einzelfall die hinreichende Wahrscheinlichkeit besteht, dass in absehbarer Zeit ein Schaden für ein bedeutsames Rechtsgut, wie Bestand oder Sicherheit des Bundes oder eines Landes, Leben, Gesundheit, Freiheit einer Person oder bedeutende Sach- und Vermögenswerte, eintritt;"

Die Eingriffsschwelle ist somit bereits nach dem Gesetzeswortlaut sehr hoch.

Oft ist der Überwachungswunsch der Gemeinde besonders an solchen öffentlichen Orten gegeben, der als Ansammlungsort für verschiedene Gruppen bekannt ist und an dem es vermehrt zu Vandalismus, verbalen und auch mal tätlichen Auseinandersetzungen, Ruhestörung usw. kommt.

Auch wenn dieser Ansammlungsort als sehr störend empfunden wird, reicht diese Sachlage nicht, um die oben beschriebene Eingriffsschwelle zu überschreiten. Diese darf nämlich

nicht unter derjenigen für die Videoüberwachung durch den Polizeivollzugsdienst gemäß § 57 Abs. 3 Sächsisches Polizeivollzugsdienstgesetz (SächsPVDG) liegen. Hierbei muss tatbestandlich ein polizeilich festgestellter Kriminalitätsschwerpunkt vorliegen.

Die Faustformel lautet, dass die Gemeinde auf der Rechtsgrundlage des § 30 Abs. 1 Sächsisches Polizeibehördengesetz (SächsPBG) nur dann überwachen darf, wenn auch die Polizei dies dürfte, dies aber aus diversen Gründen (meist sind dies polizeitaktische Gründe) nicht tut.

Zur Videoüberwachung durch die Landespolizei und zu weiteren Ausführungen zum Kriminalitätsschwerpunkt verweise ich im Übrigen auf den Tätigkeitsbericht Datenschutz 2022, dort unter Punkt 1.1.

Auch kann die Gemeinde nicht auf Grundlage des § 13 SächsDSDG öffentliche Plätze derart überwachen, dass eine Überwachung des Dienstgebäudes so ausgeweitet wird, dass nicht nur ein 1 Meter breiter Streifen, so wie es zulässig wäre, erfasst wird, sondern auch die Wege bzw. der Platz vor dem Gebäude. Auch hierauf musste ich im Berichtszeitraum eine Gemeinde hinweisen. Diese hatte nämlich Kameras an nebenstehenden Gebäuden installiert, die das eigene Dienstgebäude samt Umgebung überwachten. Die Überwachung stützte die Gemeinde auf das Hausrecht. Dies ist in dem stattgefundenen Umfang aber nicht zulässig.

„Orientierungshilfe für die Videoüberwachung durch sächsische Kommunen nach § 13 SächsDSDG und § 30 SächsPBG als PDF:
↗ sdb.de/vue16

„Achtung Kamera!" als PDF:
↗ sdb.de/achkam

Was ist zu beachten?
Videoüberwachung durch Gemeinden auf öffentlichen Straßen und Plätzen ist nur dort möglich, wo auch ein Kriminalitätsschwerpunkt vorliegt, die Landespolizei aber aus verschiedenen Gründen keine Videoüberwachung betreibt.

1.3 Fach-AG KI in der Sächsischen Verwaltung

↗ DSGVO

Im letzten Jahr nahm die „Fach-AG KI in der sächsischen Verwaltung" ihre Arbeit in einer neuen Struktur wieder auf. Ich bin weiterhin an der Arbeitsgruppe beteiligt.

Ich befürworte ausdrücklich das Ziel der Arbeitsgruppe, den Beschäftigten des Freistaats klare Regeln an die Hand zu geben, anhand derer sie KI-Systeme bedienen können. Dafür sind zwei zentrale Voraussetzungen zu erfüllen. Zum einen müssen diese KI-Systeme im Arbeitsalltag eine wirkliche Hilfe und Zeitersparnis darstellen, zum anderen muss die Nutzung gesichert rechtskonform erfolgen. Diese Voraussetzungen sehe ich bei frei verfügbaren KI-Systemen, wie beispielsweise der freien Version von ChatGPT oder Gemini und anderen, nicht oder nur mit starken Einschränkungen gegeben. Die Erfahrungen aus dem Alltag zeigen, dass eine wirkliche Erleichterung für die Arbeit der großen Mehrheit der Beschäftigten einen Zugriff auf geschützte Systeme und Aktenbestände erfordert, welcher mit frei verfügbaren Systemen nicht rechtskonform möglich ist. Ich appelliere daher an die Staatsregierung, eigene KI-Systeme zur Verfügung zu stellen und für deren Nutzung eine gesetzliche Rechtsgrundlage zu schaffen. Nur dann können KI-Systeme den sächsischen Bürgerinnen und Bürgern in ihren Belangen mit der Verwaltung dienen, ohne dass sie dafür Einschränkungen ihrer Grundrechte akzeptieren müssen.

Mit diesem Ziel werde ich mich auch weiterhin gerne konstruktiv an der Arbeitsgruppe beteiligen und hoffe, dass im nächsten Jahr Einigkeit zu einem ersten Regelwerk gefunden werden kann, das diesen Anforderungen genügt.

Was ist zu tun?

Die sächsische Landesregierung erarbeitet mit meiner Beteiligung Regeln zum rechtskonformen Einsatz von KI in der öffentlichen Verwaltung.

Was ist zu tun?
Die sächsische Landesregierung erarbeitet mit meiner Beteiligung Regeln zum rechtskonformen Einsatz von KI in der öffentlichen Verwaltung.

1.4 Digital Omnibus der EU-Kommission

↗ DSGVO, KI-VO

Am 19. November 2025 hat die EU-Kommission zwei Verordnungsentwürfe veröffentlicht – einen zum Daten- und Datenschutzrecht: „Digital Omnibus", 2025/0360 (COD), und einen zur KI-Verordnung: „Digital Omnibus on AI", 2025/0359 (COD). Der Vorschlag befindet sich nun im offiziellen Gesetzgebungsverfahren der EU – von Änderungen ist auszugehen. Die Datenschutzkonferenz hat als Reaktion zwei eigene Vorschläge für gezielte Anpassungen der DSGVO beschlossen (siehe sdb.de/tb2501).

Der „Digital Omnibus" (COM{2025} 837) sieht zehn Artikel mit einer Vielzahl von Änderungen in verschiedenen Verordnungen und Richtlinien vor. Aus Datenschutzsicht vor allem relevant ist Artikel 3, da dieser Vorschläge für spezifische Änderungen der DSGVO enthält.

Unter anderem sollen danach Informationen, die sich auf eine natürliche Person beziehen, nicht allein deshalb für jede andere Person oder Stelle personenbezogene Daten darstellen, weil eine weitere Stelle diese natürliche Person identifizieren kann. Inhaltlich knüpft der Vorschlag eng an die aktuelle Rechtsprechung des Europäischen Gerichtshofs (Urteil vom 04.09.2025 – C-413/23 P – SRB/EDSB, siehe 9.2) zur Identifizierbarkeit an. Die EU-Kommission reagiert zudem mit einem neuen Art. 41a zur Pseudonymisierung auf diese Entscheidung des EuGH, indem sie sich die Möglichkeit einräumt, Durchführungsrechtsakte mit Regelbeispielen zu erlassen.

Weiterhin könnten Verantwortliche bei einem Auskunftsbegehren nach Artikel 15 auch dann, wenn es zu anderen Zwecken als dem Schutz der Daten von Betroffenen missbraucht wird, eine angemessene Gebühr verlangen oder es ablehnen, aufgrund des Antrags tätig zu werden. Auch sollen bei „nicht datenintensiven Tätigkeiten" die Informationspflichten nach Artikel 13 entfallen.

Daneben soll eine Ausnahme zur Verarbeitung sensibler Daten im Zusammenhang mit der Entwicklung und dem Betrieb

eines KI-Systems oder -Modells ebenso geschaffen werden wie unter bestimmten Voraussetzungen für die Verarbeitung biometrischer Daten zur Verifizierung.

Schließlich sollen Vorschriften für besondere Verarbeitungssituationen in die DSGVO aufgenommen werden: zum einen die Verarbeitung personenbezogener Daten im Endgerät einer natürlichen Person, zum anderen automatisierte und maschinenlesbare Angaben zu den Entscheidungen der betroffenen Person hinsichtlich der Verarbeitung personenbezogener Daten im Endgerät natürlicher Personen und schließlich die Verarbeitung personenbezogener Daten zu KI-Zwecken.

Ein neuer Artikel 88a DSGVO soll den bisherigen Artikel 5 Abs. 3 ePrivacy-RL – den zentralen Mechanismus zum Zugriff auf Endgeräte (wie beispielsweise Computer oder Mobiltelefone) – vollständig in die Verordnung übernehmen. Hierzu erfolgt auch die Aufnahme spezifischer technischer Terminologie in Artikel 4.

Mit Artikel 6 des Entwurfs soll zum einen im Zusammenhang mit Artikel 33 die Meldefrist für den Verantwortlichen von 72 Stunden auf 96 Stunden erhöht werden. Zum anderen soll nicht mehr direkt an die gemäß Art. 55 DSGVO zuständige Aufsichtsbehörde gemeldet werden, sondern über den nach Art. 23a RL (EU) 2022/2555 eingerichteten Single-Entry-Point. Hier wie auch bei der Datenschutz-Folgenabschätzung wird für eine europäische Harmonisierung vorgeschlagen, dass nicht mehr die nationalen Aufsichtsbehörden, sondern der EDSA eine Positiv- und eine Negativliste sowie eine einheitliche Vorlage und eine einheitliche Methodik ausarbeitet.

Der „Digital Omibus on AI" (COM{2025} 836) hat das selbsternannte Ziel der Vereinfachung, um eine zeitnahe, reibungslose und verhältnismäßige Umsetzung der Bestimmungen der KI-Verordnung sicherzustellen. Dies soll vor allem durch eine Ausweitung der bereits etablierten regulatorischen Erleichterungen, die bislang nur für Kleinstunternehmen sowie kleine und mittlere Unternehmen („KMU") galten, auf kleine Unternehmen mittlerer Kapitalisierung („Small Mid-Cap Enterprises" – „SMC") erreicht werden. Auch soll die

Verpflichtung für Anbieter und Betreiber, Maßnahmen zur Sicherstellung der KI-Kompetenz ihres Personals zu ergreifen, dahingehend geändert werden, dass Adressaten der Vorschrift nunmehr die EU-Kommission und die Mitgliedstaaten sein sollen, die zukünftig das Ergreifen von Maßnahmen durch Anbieter und Betreiber nur noch anregen bzw. diese dazu ermutigen („encourage") sollen.

Weiterhin soll die Verarbeitung besonderer Kategorien personenbezogener Daten zur Bias-Korrektur erweitert werden. Auch sollen die Registrierungspflichten bei KI-Systemen, die als nicht hochriskant eingestuft sind, entfallen. Schließlich sollen die Regelungen zur Kennzeichnungspflicht für KI-generierte Inhalte und zur Überwachung der entsprechenden Praxisleitfäden zugunsten einer ausgeweiteten Selbstregulierung geändert werden.

Die DSK hat sich mit einer teils kritischen Stellungnahme zu den einzelnen Änderungsvorschlägen an der Diskussion in den europäischen Aufsichtsbehörden und an einer gemeinsamen Stellungnahme des EDSA zum Gesetzentwurf beteiligt. Über diese Stellungnahme können Sie sich in meinem Internetangebot informieren.

Was ist zu tun?

Der Gesetzgebungsprozess ist noch nicht abgeschlossen, sodass abzuwarten bleibt, welche Änderungen auch auf sächsische Verantwortliche bzw. Bürgerinnen und Bürger zukommen.

2 Grundsätze der Datenverarbeitung

2.1 Datenverarbeitungsgrundsätze, Begriffsbestimmungen

2.1.1 Unzulässige Zweckänderung – Verwendung von Kundendaten zur Wahlwerbung

↗ Art. 5 Abs. 1 Buchst. b DSGVO, Art. 6 Abs. 4 DSGVO

Ein zentraler Grundsatz des Datenschutzrechts ist die Zweckbindung nach Art. 5 Abs. 1 Buchst. b DSGVO. Danach müssen personenbezogene Daten für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden, es sei denn, die Weiterverarbeitung erfolgt für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke. Der Zweck der Verarbeitung personenbezogener Daten ist dabei vor dem Beginn der Verarbeitung durch den Verantwortlichen festzulegen.

Den in der DSGVO kodifizierten Zweckbindungsgrundsatz hatte zurückliegend schon das Bundesverfassungsgericht in seinem wegweisenden Volkszählungsurteil vom 15. Dezember 1983 als verfassungsrechtliches Datenschutzprinzip herausgearbeitet und betont.

Ziel des Zweckvereinbarungsgrundsatzes der Verordnung ist es ebenso, zu verhindern, dass personenbezogene Daten für nicht abgesprochene Zwecke genutzt werden. Zugleich soll das Prinzip sicherstellen, dass die betroffenen Personen wissen und verstehen, wofür ihre Daten genutzt werden. Aus diesem Grund ist ein Verantwortlicher bei einer von ihm

beabsichtigten Zweckänderung auch verpflichtet, die betroffenen Personen hierüber vor der Weiterverarbeitung zu informieren (vgl. Art. 13 Abs. 3 sowie Art. 14 Abs. 4 DSGVO).
Im Vorfeld der Bundestagswahl, im Februar 2025, erreichten meine Behörde eine Vielzahl von Beschwerden, mit der die Beschwerdeführer eine zweckwidrige Nutzung ihrer Adressdaten durch zwei Unternehmen, die im Handel tätig und bei denen sie Kunden sind, geltend gemacht hatten.
Die beiden Unternehmen hatten die bei ihnen hinterlegten Kundenstammdaten genutzt, um diese mittels eines Rundschreibens anzuschreiben. Gegenstand der beiden Schreiben war jeweils die Bewerbung eines Direktkandidaten, der zur Wahl zum Bundestag kandidiert hatte. Eine Vorabinformation zur beabsichtigen Nutzung ihrer Adressdaten hatten die Beschwerdeführer von den beiden Unternehmen nicht erhalten.
Die mir mit den Beschwerden vorgelegten Schreiben waren den beiden Unternehmen zuordenbar, da diese darin jeweils als Absender benannt wurden.
Die Nutzung der Adressdaten der Beschwerdeführer für Wahlwerbung stellt hinsichtlich des Zwecks, für den diese von den beiden Unternehmen zunächst erhoben wurden, hier für den Abschluss und die Erfüllung von Kauf-, Werk- bzw. Dienstleistungsverträgen im Zusammenhang mit ihrem Unternehmenszweck, eine anderweitige Verarbeitung dar, welche auch nicht für Archiv-, Forschungs- oder statistische Zwecke erfolgt ist.
Neben den in Art. 5 Abs. 1 Buchst. b DSGVO genannten drei Ausnahmen ermöglichen auch die Regelungen in Art. 6 Abs. 4 DSGVO eine Durchbrechung des Grundsatzes der Zweckbindung.
Nach dem Willen des Verordnungsgebers soll eine Zweckänderung danach auch dann zulässig sein, wenn eine Einwilligung der betroffenen Person vorliegt, sie auf einer Rechtsvorschrift beruht oder die Verarbeitung mit den Zwecken, für welche die personenbezogenen Daten ursprünglich erhoben wurden, vereinbar ist (vgl. Erwägungsgrund 50 zur DSGVO). Mit Vereinbarkeit gemeint ist dabei eine inhaltliche Nähe

der neuen Verarbeitung zur vorherigen Zweckbestimmung. Dies war hier aufgrund des offenkundig nicht bestehenden Sachzusammenhangs zwischen dem Abschluss von Verträgen zwischen den beiden Unternehmen und seiner Handelskundinnen und -kunden sowie der Wahlwerbung für einen Direktkandidaten zu verneinen. Es lage keine Einwilligung oder eine Rechtsvorschrift vor, die die Unternehmen zu einer Verarbeitung der Adressdaten abweichend vom ursprünglichen Zweck hätte berechtigen können.

Ich habe daher gegenüber den beiden Unternehmen einen Datenschutzverstoß festgestellt. Zugleich habe ich diese darauf hingewiesen, dass sie im Wiederholungsfall mit weitergehenden Maßnahmen seitens meiner Behörde rechnen müssten. Verstöße gegen die datenschutzrechtlichen Grundsätze in Art. 5 DSGVO können ein hohes Bußgeld zur Folge haben, vgl. Art. 83 Abs. 5 Buchst. a DSGVO.

Was ist zu beachten?
Die Zweckvereinbarkeit ist ein zentraler Grundsatz im Datenschutzrecht, dessen Durchbrechung nur mit Einwilligung bzw. unter den gesetzlichen Bedingungen statthaft ist.

2.1.2 Nutzung von amtsübergreifenden Fachverfahren durch Behörden

↗ Art. 4 DSGVO, Art. 5 DSGVO, Art. 32 DSGVO, Erwägungsgrund 39 zur DSGVO

Im Rahmen meiner Beratungstätigkeit erreichte mich die Anfrage einer Gemeinde zur Nutzung eines Fachverfahrens (Fachsoftware) durch verschiedene Ämter bzw. Abteilungen. Geplant war, dass alle Bediensteten einen lesenden Zugriff auf das Fachverfahren erhalten sollten. Die Bearbeitungsmöglichkeiten im Fachverfahren seien jedoch entsprechend der Zuständigkeiten angepasst.

Von einem lesenden Zugriff spricht man, wenn eine Person zwar das Verfahren aufrufen und die darin enthaltenen Daten ansehen („lesen") kann, jedoch keinerlei Bearbeitung oder Veränderung der Daten vornehmen kann.

Die verschiedenen Fachämter einer Behörde oder öffentlichen Stelle (zum Beispiel auch der Landkreise) sind im formellen Sinne jeweils eigene Stellen. Dementsprechend ist der Zugriff auf die jeweiligen Fachämter zu begrenzen. Die Mitarbeiter der allgemeinen Verwaltung bzw. der anderen Fach-

ämter sind in diesem Zusammenhang „Dritte" im Sinne des Art. 4 Nr. 10 DSGVO.
Ein unabhängig von der tatsächlichen Zuständigkeit vorhandener Zugriff stellt daher einen Verstoß gegen den Grundsatz der Integrität und Vertraulichkeit gemäß Art. 5 Abs. 1 Buchst. f DSGVO dar. Die nichtzuständigen Fachämter bzw. Mitarbeitenden der Allgemeinen Verwaltung sind außerhalb ihrer jeweiligen ganz konkreten Zuständigkeiten daher nicht zur Verarbeitung von Daten befugt.
Besonders deutlich wird dies auch im Erwägungsgrund 39 zur DSGVO, in welchem in Satz 12 wörtlich ausgeführt wird:

> „Personenbezogene Daten sollten so verarbeitet werden, dass ihre Sicherheit und Vertraulichkeit hinreichend gewährleistet ist, wozu auch gehört, dass Unbefugte keinen Zugang zu den Daten haben und weder die Daten noch die Geräte, mit denen diese verarbeitet werden, benutzen können."

Ergänzt wird dies durch die Regelungen des Artikels 32 Abs. 1 Buchst. b und Abs. 4 DSGVO, welcher technische und organisatorische Maßnahmen zum Schutz vor den genannten Risiken fordert.
Im Übrigen besteht weiterhin das Erfordernis, dass zur Verarbeitung von Daten eine entsprechende Rechtsgrundlage bestehen muss. Nach Art. 4 Nr. 4 DSGVO ist sowohl das Abfragen als auch das Auslesen von Daten ausdrücklich als Teil der Verarbeitung benannt. Insoweit besteht keine Rechtsgrundlage für derart weitreichende Leseberechtigungen.
Da die Anfrage bereits vor dem Einsatz der Software gestellt wurde, passte die Gemeinde die Zugriffsberechtigungen entsprechend meiner Ausführungen an. Ein unbefugter Zugriff wurde damit von vornherein ausgeschlossen. Dieser Fall zeigt erneut, wie hilfreich eine frühzeitige Einbeziehung meiner Behörde in Datenschutzfragen ist.

Was ist zu tun?
Ein unabhängig von der fachlichen Zuständigkeit vorhandener Zugriff auf Daten, auch lesend, stellt eine unbefugte Verarbeitung dar. Die Zugriffsmöglichkeiten sind technisch so zu gestalten, dass sie den fachrechtlichen Zuständigkeiten entsprechen.

2.1.3 Schulsozialarbeit im Jugendhilfegesetz – Teil 2

↗ Art. 4 DSGVO, § 35b SächsSchulG, § 13a SGB VIII, § 61 SGB VIII, § 21 SächsLJHG

Tätigkeitsbericht Datenschutz 2024:
↗ sdb.de/tb2024

Zum Thema Datenschutz in der Schulsozialarbeit habe ich mich in meinem Tätigkeitsbericht Datenschutz 2024 (2.1.11, Seite 71 f.) grundlegend geäußert.

Hierzu erreichten mich im Berichtszeitraum verschiedene Nachfragen und Einwände. Ergänzend zu meinen bisherigen Ausführungen möchte ich daher auf Folgendes hinweisen:

Problematisch an der Datenverarbeitung durch Schulsozialarbeiter/innen ist, dass Daten von Schülerinnen und Schülern durch eine externe Person verarbeitet werden müssen. Dies folgt daraus, dass die Schulsozialarbeit keine originäre Aufgabe der Schulen darstellt, sondern ein eigenes Handlungsfeld der Kinder- und Jugendhilfe ist. Die Schulen sind daher zwar die Verantwortlichen (im Sinne des Art. 4 Nr. 7 DSGVO) für die Schülerdaten, jedoch nicht für die Daten der Schulsozialarbeit. Die Schulsozialarbeiter/innen unterstehen den jeweiligen freien oder öffentlichen Trägern der Jugendhilfe.

Vor diesem Hintergrund ist der Datenaustausch zwischen den Schulen und Kindern mit den Schulsozialarbeiter/innen kritisch zu betrachten. Die Offenlegung und Verarbeitung von Daten kann nur aufgrund einer gesetzlichen Regelung oder einer rechtmäßigen Einwilligung erfolgen.

So enthält § 35 b Abs. 1 Sächsisches Schulgesetz (Sächs SchulG) eine ausreichend normenklare Rechtsgrundlage für die Verarbeitung personenbezogener Daten ausschließlich in Bezug auf die Übermittlung personenbezogener Daten von Schülerinnen und Schülern, wobei in den Sätzen 2 und 3 des Absatzes 1 ausdrücklich und damit auch abschließend geregelt ist, welche Daten dabei von den Schulen an die Schulsozialarbeiter/innen offengelegt werden dürfen. Grundsätzlich sind dies: der Vornamen und Nachnamen des Kindes. Bei minderjährigen Schülerinnen und Schülern wird dies ergänzt um: Vorname, Namenszusatz, Nachname, Wohnanschrift, Telefonnummer und E-Mail-Adresse ihrer Eltern. Sämtliche

anderen Daten – insbesondere der Grund, weshalb die Schule den Kontakt zur Schulsozialarbeit herstellen möchte – sind nicht von der Regelung umfasst. Eine Weitergabe dieser Informationen kann daher nur aufgrund einer Einwilligung seitens der/des Betroffenen oder deren bzw. dessen Sorgeberechtigten erfolgen. Denn eine bloße „Zusammenarbeitsregelung", wie dies § 35 b SächsSchulG im Übrigen vorsieht, erfüllt nicht die Anforderungen an eine ausreichend normenklare Rechtsgrundlage für die Verarbeitung personenbezogener Daten.

Die Tätigkeit der Schulsozialarbeiter/innen richtet sich nach sozialrechtlichen Regelungen, insbesondere § 13 a und § 61 Achtes Buch Sozialgesetzbuch (SGB VIII) und § 21 Landesjugendhilfegesetz (SächsLJHG). Die Auffassung, eine Regelung zur Datenverarbeitung durch Sozialarbeiter/innen müsste daher im SächsSchulG verortet werden, geht fehl.

§ 13a SGB VIII stellt die Grundlage für den Aufgabenbereich der Schulsozialarbeit dar. Es ist die Zusammenarbeit mit den Schulen angelegt und – da es sich um ein Bundesgesetz handelt – eine Öffnungsklausel für die Länder eingefügt, um eigenständige Regelungen zur Schulsozialarbeit zu treffen.

Diese Regelungsmöglichkeit wurde in Sachsen genutzt und im Jahr 2024 § 21 Sächsisches LJHG eingeführt. Dieser definiert dabei, an welchen Schulen die Schulsozialarbeit stattfinden soll sowie die Ziele der Schulsozialarbeit. Datenschutzrechtliche Regelungen sind jedoch leider nicht enthalten, sodass weiterhin Rechtsfragen – auch zu den Betroffenenrechten – in der Praxis bestehen bleiben.

Meine Kollegin aus Schleswig-Holstein hat im Jahr 2022 eine Handreichung zu Datenschutz und Sozialarbeit in Schulen veröffentlicht.

Diese kann grundsätzlich auch in Sachsen genutzt werden. Allerdings sind anderslautende sächsische Regelungen zu beachten.

Handreichung „Datenschutz und Sozialarbeit an Schulen":
↗ sdb.de/tb2502

Was ist zu tun?
In der Datenverarbeitung durch Schulsozialarbeiter/innen trifft der besonders schützenswerte Bereich der Sozialdaten mit dem ebenfalls besonderen Bereich der Schuldaten aufeinander. Da es sich dabei auch um die Daten minderjähriger Kinder handelt, ist ein besonders intensiver Schutz zu gewährleisten. Alle Beteiligten sollten sich daher intensiv mit Datenschutz auseinandersetzen.

2.2 Rechtmäßigkeits-voraussetzungen der Datenverarbeitung

2.2.1 Einholung von Mieterselbstauskünften durch Wohnungsmakler

↗ Art. 6 Abs. 1 Buchst. b und f DSGVO, Art. 17 Abs. 1 Buchst. d DSGVO

Ein Mietinteressent hatte im Vorfeld einer Wohnungsbesichtigung von dem beauftragten zuständigen Wohnungsmakler eine detaillierte Selbstauskunft vorgelegt bekommen, die er dafür auszufüllen hatte. Der Mietinteressent hielt diese Selbstauskunft für zu weit gehend, da sie bereits in diesem frühen Stadium der Vertragsanbahnung eine Vielzahl an spezifischen personenbezogenen Daten abfragte. Er erhob deshalb bei meiner Behörde Datenschutzbeschwerde, hatte die Selbstauskunft aufgrund seiner Bedenken aber noch nicht ausgefüllt.

Die unzulässig erfragten Informationen in dieser Selbstauskunft betrafen beispielsweise die Staatsangehörigkeit, den Familienstand oder die geschäftliche Telefonnummer.

Die Frage der Zulässigkeit des Inhalts von Mieterselbstauskünften war schon häufig Gegenstand von Beschwerden und daher auch Prüfungen der Datenschutzaufsichtsbehörden, da sie in einem jede Bürgerin bzw. jeden Bürger betreffenden Lebensbereich, die Anmietung von Wohnungen betreffend, regelmäßig verwendet werden.

Da im vorliegenden Fall der Mietinteressent und Beschwerdeführer die Selbstauskunft noch nicht ausgefüllt hatte, lag noch kein feststehender Datenschutzverstoß vor.

Jedoch ließen die Schilderungen des Mietinteressenten die Annahme zu, dass der Wohnungsmakler bei anderen Mietinteressenten und Mietinteressentinnen in gleicher Weise verfährt. Deshalb nahm meine Behörde die vorliegende Selbstauskunft zum Anlass, den Wohnungsmakler auf die Rechtslage hinzuweisen, zumal die Mieterselbstauskunft zum einen inhaltlich nicht den datenschutzrechtlichen An-

forderungen entsprach und sie zum anderen bereits bei der Wohnungsbesichtigung zum Einsatz gebracht wurde.
Mit der Mieterselbstauskunft werden Informationen über die persönlichen und finanziellen Lebensverhältnisse der Mietinteressenten und Mietinteressentinnen und potenziellen Mieter und Mieterinnen und damit personenbezogene Daten erhoben, Art. 4 Nr. 1 DSGVO. Bereits die Abfrage dieser Daten stellt eine Erhebung, mithin eine Verarbeitung im Sinne des Art. 4 Nr. 2 DSGVO dar. Für eine rechtmäßige Verarbeitung personenbezogener Daten bedarf es einer rechtlichen Grundlage aus dem abschließenden Katalog des Art. 6 Abs. 1 DSGVO; dabei ist jede einzelne Verarbeitungstätigkeit gesondert zu betrachten.
Welcher Erlaubnistatbestand zutrifft, hängt entscheidend von dem Stadium ab, in dem sich die beteiligten Parteien befinden. Dieses hat auch Auswirkungen auf den Umfang der erhobenen personenbezogenen Daten. Grundsätzlich lassen sich drei verschiedene Stadien unterscheiden:

- Besichtigungstermin
- Erklärung von Mietinteressenten oder Mietinteressentinnen, eine Wohnung anmieten zu wollen
- Entscheidung der künftigen Vermieter/innen für bestimmte Mietinteressenten oder Mietinteressentinnen

1. Besichtigungstermin

Zum Zeitpunkt einer Besichtigung herrscht keine Klarheit darüber, ob die zur Vermietung anstehende Wohnung überhaupt den Erwartungen der Mietinteressenten und Mietinteressentinnen entspricht und diese in ein konkretes Anmietinteresse münden. Bei der ersten Interessenbekundung kommt einzig die Interessenabwägung als Rechtsgrund infrage, Art. 6 Abs. 1 Buchst. f DSGVO. Danach ist die Verarbeitung personenbezogener Daten zulässig, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern,

überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.
Der Umfang der von dem/der Bewerber/in erfragten Informationen wird durch das Erforderlichkeitsgebot begrenzt. Es dürfen nur die Daten erhoben und (weiter-)verarbeitet werden, die für den Verarbeitungszweck unbedingt notwendig sind. In der Phase des ersten Mietinteresses und der Anfrage zu einem Besichtigungstermin reicht es aus, wenn der/die Vermieter/in die Person, Wohnanschrift und Kontaktdaten des Interessenten oder der Interessentin kennt. Insbesondere im Hinblick auf die Vorgaben des Allgemeinen Gleichstellungsgesetzes (AGG) ist es nicht notwendig, die Staatsangehörigkeit des Mietinteressenten und der Mietinteressentin zu kennen. Auch Angaben zum Familienstand oder dem/der Vermieter/in der bisherigen Wohnung sind zu diesem Zeitpunkt nicht erheblich.

2. Erklärung eines Anmietinteresses

Bewirbt sich im Anschluss an die Wohnungsbesichtigung ein/e Mietinteressent/in um die Wohnung (konkretes Anmietinteresse), können von diesem/dieser weitere Daten erfragt werden. An dieser Stelle kommt häufig eine Mieterselbstauskunft zum Einsatz. Mit den darin enthaltenen Informationen soll eine Entscheidung getroffen werden, mit wem ein Vertrag geschlossen werden soll. Die Parteien befinden sich dann bereits in einer vorvertraglichen Phase, sodass sich die Verarbeitung personenbezogener Daten auf der Grundlage von Art. 6 Abs. 1 Buchst. b DSGVO vollzieht. Inhaltlich setzt aber auch dort das Erforderlichkeitsgebot enge Grenzen an die abgefragten Daten.
Bei der Wohnraumvermietung ist das maßgebliche Interesse auf Vermieterseite oder Vermieterinnenseite, dass der/die (künftige) Mieter/in zahlungsfähig ist. Dieses bildet die Ausgangsbasis für die personenbezogenen Daten; ausschließlich hierfür relevante Informationen dürfen dem/der potenziellen Mieter/in abverlangt werden. Weitere Informationen, die einen Gesamteindruck von dem/der potenziellen Mieter/in verschaffen können, inhaltlich aber keinen Mehrwert im

Hinblick auf dessen/deren Zahlungsfähigkeit liefern, sind mit dem Datenschutzrecht nicht vereinbar.
In dem mir vorliegenden Fall betraf dies die Kenntnis des Einkommens aller zum Haushalt gehörigen Personen, sind diese doch für eine Bonitätsbeurteilung des Wohnungsbewerbers oder der Wohnungsbewerberin nicht von Belang. Ziehen neben dem/der (Haupt-)Mieter/in andere Personen ein, darf nur deren Anzahl erfragt werden sowie, ob es sich dabei um Kinder oder Erwachsene handelt. Alle weiteren Angaben wie Alter und Verwandtschaftsgrad sind für die Beurteilung der Wohnungsnutzung nicht notwendig. Ferner sind Fragen nach den Kontaktdaten aktueller Vermieter/innen unzulässig. Diese haben für die Frage, mit wem ein Mietverhältnis abgeschlossen werden soll, keine Bedeutung.
Eine Eingrenzung des Bewerberfeldes zur Ermittlung der aussichtsreichen Kandidaten für einen Mietvertragsschluss lässt sich einzig auf Basis der in der Selbstauskunft enthaltenen Daten vornehmen. Nachweise, die eine Prüfung der dortigen Angaben ermöglichen, sind auf dieser Ebene nicht notwendig.

3. Entscheidung für bestimmte Mietinteressenten oder Mietinteressentinnen

Erst nach der Entscheidung für einen oder mehrere Mietinteressenten oder Mietinteressentinnen ist es notwendig und damit rechtlich zulässig, die erfragten Informationen mittels aussagefähiger Dokumente zu verifizieren. Im Normalfall lassen sich Vermieter/innen hierzu Einkommensnachweise, Identitätsdokumente (Personalausweis) sowie Mietschuldenfreiheits- bzw. Vorvermieterbescheinigungen oder Vorvermieterinnenbescheinigungen vorlegen.
Zu bedenken ist auch hier, dass diese Dokumente Angaben enthalten, die den/die Vermieter/in nichts angehen. So enthalten Rentenbescheide und Einkommensnachweise beispielsweise Geburtsort, Religionszugehörigkeit, Anzahl der unterhaltspflichtigen Kinder, Angaben zur Krankenkasse und Steuerklasse. Diese sind von dem Mietinteressenten oder der Mietinteressentin zu schwärzen; hierauf ist er/sie explizit

hinzuweisen. In Mieterselbstauskünften reicht die Anschrift des bisherigen Vermieters oder der bisherigen Vermieterin aus; anderweitiger Kontaktdaten bedarf es nicht. Bei Personalausweisen, die ebenfalls nicht relevante Daten enthalten (zum Beispiel Größe, Geburtsort, etc.), ist es ausreichend, wenn der/die Vermieter/in diese einsehen; einer Kopie bedarf es regelmäßig nicht.

Zurück zum konkreten Fall. Ich kam letztlich nicht umhin, den Wohnungsmakler aufzufordern, sein Verfahren anzupassen, insbesondere den Inhalt der Selbstauskunft zu ändern sowie auf deren vorzeitigen Einsatz bereits im Vorfeld von Besichtigungsterminen zu verzichten. Damit war sichergestellt, dass er sich künftig an die datenschutzrechtlichen Vorgaben hält.

Nachdem die datenschutzrechtswidrige Verarbeitung auch in die Vergangenheit reichte, galt es, auch insoweit rechtmäßige Zustände herzustellen. Deshalb gab ich ihm auf, alle unzulässig erhobenen und noch gespeicherten personenbezogenen Daten zu löschen. Dies ergibt sich bereits unmittelbar aus dem Gesetz, wonach alle unrechtmäßig verarbeiteten personenbezogenen Daten unverzüglich zu löschen sind, Art. 17 Abs. 1 Buchst. d DSGVO.

Die Datenschutzkonferenz hat zu diesem Thema eine Orientierungshilfe zur „Einholung von Selbstauskünften bei Mietinteressent:innen" veröffentlicht.

Sie enthält in detaillierter Form die auf der jeweiligen Stufe benötigten Informationen und ermöglicht damit eine vollständige Überprüfung der bisherigen Verarbeitungspraxis.

Orientierungshilfe „Einholung von Selbstauskünften bei Mietinteressent:innen":
↗ sdb.de/tb2503

Was ist zu tun?
Bei der Einholung von Mieterselbstauskünften hat der/die Vermieter/in sich auf streng bemessene, am Vertragsanbahnungsprozess erforderliche Angaben zu beschränken. Hinzuweisen ist auf die entsprechende Orientierungshilfe der Datenschutzkonferenz zu Mieterselbstauskünften.

2.2.2 Bereitstellung von Eigentümerdaten des amtlichen Vermessungswesens für Windenergieanlagen und Solaranlagen

↗ § 2 EEG, § 11 SächsVermKatG, Art. 6 DSGVO

Im Rahmen meiner Beratungstätigkeit kann ich nicht nur Betroffene und Verantwortliche, sondern auch Parlamente, die Regierung und andere Einrichtungen und Gremien beraten. So bat auch das Staatsministerium für Infrastruktur

und Landesentwicklung um meine Einschätzung hinsichtlich einer Handreichung an die unteren Vermessungsbehörden. Dem vorausgegangen waren mehrere Entscheidungen von sächsischen Verwaltungsgerichten zur Anwendung des § 11 des Sächsischen Vermessungs- und Katastergesetzes (SächsVermKatG). Diese Entscheidungen sollten in einer Handlungsanleitung umgesetzt werden und – da die Entscheidung die Offenlegung von Daten umfasst, wurde ich in die Erstellung einbezogen.

16. Tätigkeitsbericht für den öffentlichen Bereich (04/2011–03/2013):
↗ sdb.de/tb16oeb

Tätigkeitsbericht Datenschutz 2023:
↗ sdb.de/tb2023

Dies ist auch nicht das erste Mal, dass ich mich mit diesem Thema befasst habe. Die Rechtsprechung erweitert den Anwendungsbereich des § 11 SächsVermKatG stetig. Diese Entwicklung ist auch meinen vorhergehenden Beiträgen in den Tätigkeitsberichten für das Jahr 2013 (5.14.1, Seite 68 f.) und 2023 (2.2.28, Seite 111 ff.) zu entnehmen.

§ 11 Abs. 2 Satz 4 SächsVermKatG regelt dabei, unter welchen Bedingungen die unteren Vermessungsbehörden die Eigentümerdaten von Grundstücken an andere natürliche oder juristische Personen – hier die Projektfirmen für die Errichtung von Wind- oder Solarenergieanlagen – offenbaren dürfen. Dies bestimmt sich nach dem „berechtigten Interesse". Eine Auslegung des Begriffs des „berechtigten Interesses" stellt dabei eine fachrechtliche Frage dar und nicht ausschließlich eine datenschutzrechtliche. Dennoch wird in jedem Fall zu berücksichtigen sein, dass es sich bei § 11 Abs. 2 Satz 4 SächsVermKatG um eine Schranke des Rechts auf informationelle Selbstbestimmung handelt, die den Grundsätzen der Bestimmtheit und der Verhältnismäßigkeit sowohl in der Auslegung als auch in der Anwendung in jedem Fall genügen muss.

Dieses berechtigte Interesse der Projektfirmen wird in der Rechtsprechung aufgrund von § 2 des Gesetzes für den Ausbau erneuerbarer Energien (EEG) in verschiedenen aktuellen Entscheidungen bestätigt. In § 2 EEG ist ein sogenannter Vorrang der erneuerbaren Energien gegenüber anderen öffentlichen Interessen verankert. Dementsprechend wurde in verschiedenen Verwaltungsgerichtsentscheidungen das berechtigte Interesse dann angenommen, wenn die Firmen

Windenergieanlagen, Freiflächensolaranlagen oder Energiespeicher planen, projektieren oder betreiben wollen. Dabei habe die Bereitstellung der Daten bereits in einem frühen Planungsstadium zu erfolgen. Die Offenbarung kann auch dann erfolgen, wenn die planerischen Voraussetzungen für die Errichtung der betreffenden Anlage – ausweislich vorhandener Regionalpläne oder Bebauungspläne – derzeit nicht vorliegen, sich das Grundstück aber im Außenbereich im Sinne des § 35 Baugesetzbuch befindet.

Hinsichtlich der datenschutzrechtlichen Verhältnismäßigkeit bleibt darauf hinzuweisen, dass hier eine Abwägung mit grundrechtlich garantierten Rechten von Privatpersonen stattfindet. Aus § 2 EEG folgt daher kein datenschutzrechtlicher Vorrang.

Unbenommen bleibt jedoch die Bedeutung der Nutzung der erneuerbaren Energien, insbesondere im Hinblick auf die energiepolitischen Ziele. Strom ist für die Funktionalität von Wirtschaft und Verwaltung essenziell und der Ausbau der Gewinnung von erneuerbaren Energien sichert die Versorgung der Bevölkerung. Hinzu kommt ein eigenes wirtschaftliches Interesse der betroffenen Eigentümer an der Nutzung des entsprechenden Grundstückes. Sodass im Ergebnis die Interessen des Eigentümers in der Regel einer Datenbereitstellung nicht entgegenstehen.

Diese Auffassung habe ich dem Staatsministerium für Infrastruktur und Landesentwicklung mitgeteilt, woraufhin die Handlungsanleitung gefertigt und verkündet wurde.

Was ist zu tun?

Die unteren Vermessungsbehörden haben in jedem einzelnen Fall eine Prüfung der Voraussetzung des § 11 Abs. 2 Satz 4 SächsVermKatG vorzunehmen. Die Handlungsanweisung stellt nur den Regelfall dar, in besonderen Ausnahmefällen kann eine andere Entscheidung zum „berechtigten Interesse" möglich sein.

Relevante Entscheidungen:

VG Dresden 7 K 87/23 vom 11. Februar 2025
VG Leipzig 4 K 2580/24 vom 1. November 2024
VG Leipzig 4 K 176/23 vom 15. August 2024
BayVGH 13a B 22.1688 vom 9. März 2023

2.2.3 Ablesekarten mit Unterschriften der Verbraucher/innen

↗ Art. 5 Abs. 1 Buchst. c DSGVO

Ein Bürger wandte sich an meine Behörde, weil er zur Ablesung des jährlichen Wasserverbrauches von dem Versorgungsbetrieb eine vorgedruckte Ablesekarte für den Rückversand erhalten hatte. Es war vorgesehen, dass der Verbraucher die angefragten Daten samt der Zählernummer und des Zählerstandes ausfüllt und die bereits freigemachte Postkarte offen zurückschickt. Oft enthalten diese Ablesekarten Zeilen für Namen und Adresse. Manche Unternehmen verlangen jedoch noch deutlich mehr Angaben, zum Beispiel die vollständige Adresse, Unterschrift, Telefonnummern oder E-Mail-Adresse. Solche Angaben sind nicht nur unnötig, sondern auch riskant.
Auch wenn der/die Anschlussnehmer/in selbst die Ablese- bzw. Antwortpostkarte ausfüllt, handelt es sich um eine Datenerhebung, welche im Verantwortungsbereich des Wasserversorgungsanbieters liegt. Dementsprechend haben die Unternehmen auch dafür Sorge zu tragen, dass die Datenerhebung nur im notwendigen Maße und so sicher wie möglich erfolgt. Trotz Postgeheimnis ist das (insbesondere unnötige) offene Versenden von Unterschriften im Zusammenhang mit dem jeweiligen vollständigen Namen, der Adresse und Telefonnummer angesichts der zunehmenden Gefahr von Identitätsdiebstahl als sehr bedenklich zu betrachten und sollte daher unbedingt vermieden werden. Dies habe ich dem hier verantwortlichen Versorgungsunternehmen so mitgeteilt.
Auch die Ausführung des Verantwortlichen, dass es sich bei einer vom Anschlussnehmer selbst ausgefüllten Ablesekarte um eine eigenverantwortliche Datenweitergabe durch den Betroffenen selbst handelt, verfängt keinesfalls. Die Datenerhebung liegt in der Verantwortlichkeit des Versorgungsunternehmens, egal, wer die Ablesekarte ausfüllt. Auch ist es nicht möglich, diese Verantwortlichkeit damit abzugelten, indem man die/den Verbraucher/in darauf verweist, sie/er könne ja andere Übermittlungswege nutzen (zum Beispiel die Karte kuvertieren und eine eigene Briefmarke daraufkleben).

Nach Art. 5 Abs. 1 Buchst. c DSGVO sind im Sinne der Datenminimierung nur die Daten zu erheben und zu verarbeiten, welche „für die Zwecke der Verarbeitung notwendig" sind. Für die Angabe einer Telefonnummer und E-Mail-Adresse besteht regelmäßig keine Notwendigkeit. Es muss aus den Ablesekarten daher deutlich hervorgehen, dass diese Angaben freiwillig erfolgen. Eine gleichzeitige handschriftliche Angabe von Namen und Adresse sowie Unterschrift wird meist ebenfalls nicht notwendig sein. Auch hier ist entweder deutlich auf eine Freiwilligkeit der Angaben zu verweisen oder die unnötige Datenerhebung – zum Beispiel die Unterschrift – wegzulassen.

Was ist zu beachten?
Auf offen zu versendenden Ablesekarten dürfen seitens des Ablese- bzw. Versorgungsbetriebes keine unnötigen Angaben, insbesondere Unterschriften, abverlangt werden.

Daraufhin hat das Versorgungsunternehmen die vorgedruckten Karten angepasst. Eine Unterschriftenzeile ist nicht vorgesehen, die Angabe der Telefonnummer soll ausdrücklich nur freiwillig erfolgen.
Mit diesem Ergebnis konnte ich mich einverstanden zeigen und den Vorgang abschließen.

2.2.4 Zulässigkeit des Anschreibens von Rechtsanwältinnen bzw. Rechtsanwälten an Kapitalanleger/innen

↗ Art. 6 Abs. 1 Buchst. b und f DSGVO

Auch wenn die Zeiten vorbei sind, in denen Kapitalanleger/innen aufgrund des Massenvertriebs von Schrottimmobilien und anderen problematischen Kapitalanlagen häufig von Anlegeranwälten und –anwältinnen zur Information und auch Mandantengewinnung angeschrieben werden, erheben betroffene Personen immer wieder wegen sporadisch noch versendeter Anschreiben von Rechtsanwälten und Rechtsanwältinnen Datenschutzbeschwerde bei meiner Behörde. So auch im letzten Berichtszeitraum.
Zivilrechtlich sind Werbeschreiben von Rechtsanwälten und Rechtsanwältinnen gemäß § 43 b Bundesrechtsanwaltsordnung (BRAO) zulässig, wenn sie in Form und Inhalt sachlich unterrichten und nicht auf Erteilung eines Auftrags im Einzelfall gerichtet sind. Die Rechtsanwaltsschreiben in den bei

meiner Behörde eingereichten Fällen waren sachlich gefasst und informierten Beschwerdeführer/innen als Anleger/innen über relevante Umstände des Fonds. Am Ende schrieb der Anwalt, dass er für Anleger bzw. Anlegerinnen tätig werden könnte, und hatte eine Vollmacht beigefügt. Entsprechendes betrachte ich als vertretbar.

Ob das Rechtsanwaltsschreiben den Vorgaben des § 43 b BRAO genügt, ist eine standesrechtliche Frage, für die meine Behörde nicht zuständig ist. Die Beschwerdeführer wurden von mir für eine Überprüfung an die zuständige Rechtsanwaltskammer verwiesen.

Datenschutzrechtlich sind erste Werbeanschreiben von Rechtsanwältinnen bzw. Rechtsanwälten gemäß Art. 21 Abs. 2 DSGVO zunächst zulässig, die Betroffenen können aber nach dieser Norm Widerspruch gegen weitere Schreiben einlegen. Im Übrigen ist auf das Löschungsrecht gemäß Art. 17 DSGVO zu verweisen.

Meistens sind Anwälte und Anwältinnen ausschließlich für Anleger und Anlegerinnen von Kapitalanlagen tätig und nicht für die Anbieterseite oder die Fondsgesellschaften. Diese Anwälte und Anwältinnen erhalten daher die Namen und Adressen der betroffenen anderen Anleger/innen zum Beispiel einer Fondsgesellschaft als anwaltliche Vertreter/innen eines Gesellschafters bzw. einer Gesellschafterin, der die Namen seiner Mitgesellschafter/innen dieses Fonds erfahren wollte, von der Fondsgesellschaft.

Nach der bisher geltenden Rechtsprechung des Bundesgerichtshofs (BGH) zur Weitergabe der Daten durch die Fondsgesellschaft hat ein/e Gesellschafter/in das Recht, die Namen und Anschriften der Mitgesellschafter/innen zu erfahren, auch im Rahmen von Treuhandmodellen (vgl. zum Beispiel die Entscheidung des BGH vom 19. November 2019, II ZR 263/18). Bei Treuhandmodellen sind die Anleger/innen nicht selbst Gesellschafter/innen, sondern diese Anteile werden über Treuhandgesellschaften mittelbar gehalten.

Diese Weitergabe von personenbezogenen Daten der anderen Mitgesellschafter/innen durch die Fondsgesellschaft an anfragende Gesellschafter/innen an deren beauftragte

Rechtsanwälte und Rechtsanwältinnen verstoßen nach der bisherigen Rechtsprechung des BGH auch nicht gegen die Art. 5 und 6 DSGVO, vgl. BGH a. a. O. Rn. 26 ff.
So führt der BGH in Rn. 30 aus: „Vielmehr erlaubt Art. 6 Abs. 1b DS-GVO die Verarbeitung der Daten zur Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist. Dazu gehört auch die Mitgliedschaft in einer Gesellschaft (Schantz in Simitis/ Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 6 DS-GVO Rn. 16; Buchner/Petri in Kühling/Buchner, DS-GVO, BDSG, 2. Aufl., Art. 6 DS-GVO Art. 16 Rn. 30)."
Dies beurteilt nunmehr der Europäische Gerichtshof (EuGH) anders, vgl. Urteil des EuGH vom 12. September 2024, C-1722 und C-18/22, zumindest dann, wenn die betreffenden Beteiligungs- und Treuhandverträge, auf deren Grundlage mittelbare Beteiligungen an den betreffenden Gesellschaften erworben wurden, es ausdrücklich verbieten, die Daten betreffend die mittelbaren Anleger/innen anderen Anteilseignern bzw. Anteilseignerinnen mitzuteilen (Rn. 45).
Bezogen auf die mögliche Rechtsgrundlage des Art. 6 Abs. 1 Buchst. b DSGVO führt der EuGH in Rn. 46 f. weiter aus:

> „Das wesentliche Merkmal des Erwerbs einer mittelbaren Beteiligung an einer Publikumsfondsgesellschaft über eine Treuhandgesellschaft besteht gerade in der Anonymität der Gesellschafter, auch im Verhältnis der Gesellschaft untereinander. [...] Deshalb ist die Weitergabe von Gesellschafterdaten nicht als im Sinne von Art. 6 Abs. 1 Buchst. b DSGVO für die Erfüllung eines Vertrages [...] erforderlich anzusehen."

Bezogen auf die mögliche Rechtsgrundlage des Art. 6 Buchst. f DSGVO und dass es letztlich Sache des vorlegenden nationalen Gerichts ist, zu beurteilen, ob die drei Voraussetzungen der Norm vorliegen, gibt der EuGH jedoch sachdienliche Hinweise für eine Prüfung (Rn. 55).
Das Interesse eines Gesellschafters bzw. einer Gesellschafterin, personenbezogene Daten über andere mittelbare Gesellschafter/innen dieser Gesellschaft zu erhalten, um mit ihnen

über den Abkauf seiner bzw. ihrer Gesellschaftsanteile zu verhandeln oder um sich mit ihnen zur gemeinsamen Willensbildung im Rahmen von Gesellschafterbeschlüssen abzustimmen (vgl. Rn. 56), kann grundsätzlich ein berechtigtes Interesse an der Offenlegung personenbezogener Daten im Sinne dieser Norm darstellen, Rn. 57.

Hinsichtlich der zweiten Stufe der Prüfung, der Erforderlichkeit dieser Verarbeitung zur Verwirklichung des betreffenden Interesses und insbesondere das Vorliegen von Mitteln, die ebenso geeignet sind und weniger stark in die Grundrechte der betroffenen Person eingreifen, führt der EuGH aus, dass es möglich wäre, diesen Fonds oder diese Gesellschaft unmittelbar aufzufordern, seine bzw. ihre Anfrage an die betreffenden Gesellschafter/innen weiterzuleiten. Eine solche Lösung könnte auch in dem Fall angewandt werden, in dem der/die anfragende Gesellschafter/in mit einem anderen Gesellschafter oder einer Gesellschafterin Verhandlungen über den Kauf von dessen bzw. deren Anteilen aufnehmen oder sich mit ihm bzw. ihr zur gemeinsamen Willensbildung im Rahmen von Gesellschafterbeschlüssen abstimmen möchte, Rn. 59.

Abzuwarten bleibt, ob und gegebenenfalls wie der BGH im Hinblick auf dieses Urteil des EuGH seine Rechtsprechung ändert. Eine Datenschutzbeschwerde, gestützt auf die möglicherweise unberechtigte Weitergabe von personenbezogenen Daten von Mitgesellschaftern bzw. Mitgesellschafterinnen an andere Gesellschafter/innen, wäre an die Aufsichtsbehörde in dem Bundesland zu richten, in dem die Fondsgesellschaft ihren Sitz hat.

Aufgrund der bisher geltenden Rechtslage waren entsprechende ältere Beschwerden betroffener Personen abzuweisen.

Was ist zu beachten?

Informationsanschreiben von Rechtsanwälten/Rechtsanwältinnen an Kapitalanleger/innen – auch bei Treuhandbeteiligungen – sind nach der bisherigen Rechtsprechung des BGH datenschutzrechtlich zulässig. Der EuGH sieht das in einem aktuellen Urteil teilweise anders. Betroffene Personen können aber nach Art. 21 Abs. 2 DSGVO Widerspruch gegen weitere Schreiben einlegen.

2.2.5 Video-Livebilder an Tiefgaragenausfahrt zur Gefahrenreduzierung

↗ Art. 2 Abs. 1, Art. 4 Nr. 2, Art. 6 Abs. 1 Buchst. f, Art. 13 DSGVO

Eine Anwohnerin bemerkte eines Tages zwei Videokameras an einem Neubau einer Wohnanlage, die sie regelmäßig passieren musste. Diese waren links und rechts einer Tiefgarageneinfahrt angebracht. Die sich kreuzenden Sichtachsen der beiden Kameras waren auf den entlang der Hausfront gelegenen Gehweg gerichtet. Die Anwohnerin berichtete von einem Monitor neben dem Tiefgarageneingang. Anhand der dort dargestellten Bilder kam sie zu dem Schluss, dass ein Passieren des Gebäudes nicht möglich war, ohne aufgenommen zu werden. Dies nahm sie zum Anlass, bei meiner Behörde eine Datenschutzbeschwerde einzulegen.

Tatsächlich ergaben meine Nachforschungen, dass der Gebäudeeigentümer für die ausfahrenden Fahrzeugnutzer/innen vor der Ausfahrt zwei Monitore hatte anbringen lassen. Diese stellten ein Echtzeitbild der Verkehrssituation vor der Ausfahrt dar, wobei der Überwachungsbereich über die öffentliche Straße bis zu den gegenüberliegenden Gebäuden und auch auf die dortigen Grundstücke reichte. Über die Kamerabilder konnten Fußgänger/innen oder den Fußweg auch regelwidrig nutzende Radfahrer/innen, die sich der Ausfahrtrampe auf Kollisionskurs näherten, noch vor deren Eintritt in dem verengten Blickwinkel am Rampenende seitens ausfahrender Autofahrer/innen erkannt und dadurch entsprechende Gefahrenlagen abgewendet werden. Eine Speicherung der Kamerabilder wurde nach Angaben des Eigentümers nicht vorgenommen. Auf die Videobeobachtung hinweisende Schilder waren allerdings nicht angebracht.

Ich kam bei meiner Prüfung zu der Einschätzung, dass eine bloße Darstellung der Livebilder des Verkehrs, beschränkt auf den Gehweg, datenschutzrechtlich noch zulässig ist. Nicht zu rechtfertigen war jedoch eine sich auf die Fahrbahn und dahinterliegende Bereiche erstreckende Videoüberwachung. Obgleich vorliegend nur Livebilder der Kameras dargestellt wurden, handelt es sich gleichwohl um eine Verarbeitung

personenbezogener Daten. Eine Videoüberwachung kann in zwei Ausprägungen erfolgen, in Form einer Liveübertragung (Videobeobachtung, Monitoring) als auch einer Videoaufzeichnung (Fixierung von Videodaten auf einem Datenträger). Begrifflich stellt bereits eine Livebeobachtung eine Erhebung personenbezogener Daten dar, vgl. Art. 4 Nr. 2 DSGVO. Damit vollzog sich die rechtliche Wertung nach den Vorschriften der Datenschutz-Grundverordnung (Art. 2 Abs. 1 DSGVO). Grundlage für die datenschutzrechtliche Beurteilung konnte nur die Interessenabwägung in Art. 6 Abs. 1 Buchst. f DSGVO sein. Danach ist die Überwachung rechtmäßig, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

Die Monitore haben den Zweck, die ausfahrenden Personen quasi durch zwei „zusätzliche Augen" zu unterstützen, um so Unfälle und letztlich eine Schädigung der Fußwegnutzer/innen im Bereich der Tiefgaragenausfahrt zu vermeiden, was als berechtigtes Interesse anzuerkennen ist. Eine wirkliche Alternative zur Videobeobachtung war nicht erkennbar, zumal die sichtbare Darstellung sich nähernder Fußgänger/innen oder sonstiger Gehwegnutzer/innen geeignet ist, das reale und bei jeder Ausfahrt bestehende Unfallrisiko signifikant zu reduzieren. Auch wenn eine von privaten Stellen ausgehende Videoüberwachung im Allgemeinen an der Grenze des eigenen Grundstücks zu enden hat, ist vorliegend gegen eine Überwachung jedenfalls des Gehwegs entlang der Gebäudefront nichts einzuwenden. Auf diese Weise können ausfahrende Fahrzeugnutzer/innen erkennen, ob und welche Verkehrsteilnehmer/innen (Fußgänger/in oder Radfahrer/in) sich der Ausfahrt nähern.

Was jedoch die darüber hinausgehende Videoüberwachung der Fahrbahn sowie der gegenüberliegenden Grundstücke anbelangt, konnte ich keinen räumlichen Zusammenhang mit den Überwachungszwecken herstellen. Dementsprechend war der Kamerabetreiber gehalten, mittels physischer oder

technischer Mittel nach seiner Wahl den Erfassungsbereich so einzuschränken, dass nur der Gehweg unmittelbar vor der Gebäudefront sichtbar ist. Denkbar ist hier grundsätzlich das Anbringen einer (optischen) Blende oder das Verpixeln nicht relevanter Bereiche. Auch eine entsprechende Änderung der Kameraausrichtung kommt natürlich infrage.

Letztlich sah ich auch die Belange der betroffenen Personen, mithin der Passanten und Passantinnen, nicht als derart stark beeinträchtigt, dass diese einer Livebeobachtung entgegengestanden hätten. In den Aufnahmebereich eintretende Personen werden nur beim Ausfahrvorgang von den aus der Tiefgarage ausfahrenden Personen wahrgenommen, bevor sie kurze Zeit später auch physisch für diese sichtbar werden. Die Verarbeitung besteht nur in der Darstellung von Livebildern und nicht in der ungleich eingriffsintensiveren Speicherung. Letztere wäre auch im Hinblick auf den Verarbeitungszweck in keiner Weise zu rechtfertigen. Die Passanten und Passantinnen sind einzig für die ausfahrenden Personen kurz vor dem Verlassen der Tiefgarage sichtbar. Die Eingriffstiefe der Verarbeitung in das Persönlichkeitsrecht der Passanten und Passantinnen und anderer Gehwegnutzer/innen ist daher als geringfügig einzustufen. Mit einer Identifizierung oder anderweitigen Nutzung müssen die Nutzer/innen des Gehwegs zudem nicht rechnen. Hinzu kommt, dass die reine Videobeobachtung auch der Sicherheit der Passanten und Passantinnen dient und es erkennbar nicht darum geht, Passanten und Passantinnen beim Aufenthalt im öffentlichen Verkehrsraum zu überwachen.

Im Ergebnis begegnete die rein auf die unmittelbar im Bereich der Tiefgaragenausfahrt befindlichen Gehwegbereiche beschränkte Videobeobachtung (Livebild) keinen datenschutzrechtlichen Bedenken. Neben der (überschießenden) Erfassung der Straßenfahrbahn sowie nachbarlicher Grundstücke bemängelte ich auch die fehlenden Informationen nach Art. 13 DSGVO. Ich riet dem Eigentümer diesbezüglich, an jeder Seite der Tiefgarageneinfahrt in einiger Entfernung zu den Kameras vorzugsweise das von den Aufsichtsbehörden empfohlene „vollständige Informationsblatt" anzubringen.

Was ist zu tun?

Bei direkt an den Gehweg grenzenden Tiefgaragenausfahrten kann ein Video-Livebild für die Ausfahrenden den Ausfahrtvorgang erleichtern und außerdem die Sicherheit von Passanten entscheidend verbessern. Eine entsprechende Videobeobachtung kann dann im Einzelfall datenschutzrechtlich statthaft sein. In diesem Fall sind entsprechende schriftliche Hinweise (Hinweisschilder) anzubringen.

2.2.6 Dauerüberwachung in einem personallosen Fitnessstudio

↗ Art. 6 Abs. 1 Buchst. a, b, f DSGVO, Art. 13 DSGVO

Wie stark allein die Existenz von Videokameras das subjektive Empfinden der überwachten Personen stört, zeigte sich einmal mehr an einer anonymen Eingabe, die meine Behörde erreichte. Dem/Der Hinweisgeber/in waren beim regelmäßigen Training in seinem/ihrem Fitnessstudio mehrere Videokameras aufgefallen, weshalb er/sie sich zu einem Hinweis bei meiner Behörde veranlasst sah. Er/Sie drückte darin unmissverständlich sein/ihr Unwohlsein allein durch die bloße Existenz der Videokameras aus und sah auch die Gefahr, dass damit sensible Bereiche gefilmt werden. Schließlich kam in ihm/ihr die Frage auf, was mit dem Videomaterial denn überhaupt passiert.

Ich nahm dies zum Anlass für eine eingehende Überprüfung. Tatsächlich ergab diese, dass nicht nur der Eingangsbereich und der Flur mit Spinden im Kamerafokus lagen, sondern auch die Trainingsfläche mit mehreren Videokameras überwacht wurde. Nur ein Nebenraum, in dem sich nach meiner Kenntnis lediglich einige Matten befanden, war überwachungsfrei. Es zeigte sich weiter, dass es sich um ein personallos betriebenes Fitnessstudio handelte. Der Betreiber machte geltend, dass die Videoüberwachung dem Schutz von Personen und Sachwerten diene und auch der Gefahrenabwehr sowie der Dokumentation schwerwiegender Vorfälle. Weiter meinte er, damit das Sicherheitsgefühl der Mitglieder zu erhöhen, was zumindest bei dem/der anonymen Hinweisgeber/in den gegenteiligen Effekt zeitigte. Er sah speziell in einem personallosen Fitnessstudio ein erhöhtes Sicherheitsrisiko. Der Nutzen der Kameras sei, dass sie bei gesundheitlichen Notsituationen (zum Beispiel medizinischen Zwischenfällen) zur schnelleren Alarmauslösung beitragen könnten. Schließlich könnten ohne die Videoüberwachung eigentumsbezogene Straftaten nicht unmittelbar bemerkt oder aufgeklärt werden.

Bei genauer rechtlicher Betrachtung kam ich zu dem Ergebnis, dass sich die Videoüberwachung der Trainingsflächen

und Flurbereiche unter Berücksichtigung der vorgebrachten Argumente datenschutzrechtlich nicht rechtfertigen lässt.
Zwar hatte der Betreiber an der Eingangstüre ein kleines Hinweisschild des Kameraherstellers angebracht. Ungeachtet dessen, dass dieses nicht den Anforderungen des Art. 13 DSGVO entsprach, stellt das bloße Passieren eines solchen Hinweises keine (konkludente) Einwilligung in die Videoüberwachung dar, Art. 6 Abs. 1 Buchst. a DSGVO.

Reichweite der Sorgfaltspflichten

Die Videoüberwachung ließ sich auch nicht mit der Erfüllung des Mitgliedschaftsvertrags in Zusammenhang bringen Art. 6 Abs. 1 Buchst. b DSGVO. Denn die Schutzpflichten des Betreibers zielen in erster Linie auf die Instandhaltung der vorhandenen Fitnessgeräte sowie die Bereitstellung von Spinden. Eine nahezu lückenlose Videoüberwachung speziell der Trainingsflächen zum Schutz der Gesundheit sowie des Eigentums der Nutzer/innen rechnet allerdings nicht hierzu, muss der Betreiber doch nicht für alle denkbaren Möglichkeiten eines Schadenseintritts vorsorgen. Der vertraglichen Sorgfaltspflicht ist bereits dann Genüge getan, wenn ein Sicherheitsgrad erreicht ist, wie ihn die Mitglieder vernünftigerweise erwarten können. In erster Linie bezieht sich diese auf die Instandhaltung der Fitnessgeräte und die regelmäßige Überprüfung der Räumlichkeiten in einem personallosen Fitnessstudio (Beschädigungen, Vandalismus, Reinigungsarbeiten etc.).
Zu berücksichtigen ist auch, dass den Nutzern und Nutzerinnen eines personallos betriebenen Fitnessstudios bekannt und bewusst ist, dass beim Training ein potenziell höheres Risiko einer Verletzung besteht und in diesem Fall kein/e Betreuer/in vor Ort zu Hilfe eilen kann. Der Aspekt, dass Videokameras das subjektive Sicherheitsempfinden erhöhen können, steht bereits nicht im Kontext mit den den/die Betreiber/in treffenden Sorgfaltspflichten. Auch sonst taugt er nicht dazu, die Notwendigkeit einer Videoüberwachung zu begründen, zumal subjektive Wertungen höchst unterschiedlich ausfallen können.

Keine Rechtfertigung mit berechtigten Interessen

Damit blieb als Rechtsgrund einzig die Interessenabwägung, Art. 6 Abs. 1 Buchst. f DSGVO. Für eine Zulässigkeit fehlte es allerdings bereits an einem berechtigten Interesse. Ein Interesse ist dann berechtigt, wenn es rechtmäßig und hinreichend klar formuliert ist, ferner darf es nicht rein spekulativ sein. Im vorliegenden Fall konnte der Betreiber lediglich einen Fall der Sachbeschädigung sowie des Verlusts eines Wertgegenstands eines Mitglieds angeben. Nähere Angaben dazu bekam ich nicht; der Betreiber beließ es bei bloßen Behauptungen. Daher konnte ich keine Anzeichen für eine konkrete Gefährdungslage erkennen. Demzufolge hatte ich davon auszugehen, dass die Interessenlage rein spekulativ war.

Er konnte mir auch nicht schlüssig aufzeigen, wie sich etwa medizinische Notfälle mithilfe von Kameras zeitnah feststellen ließen. Dies wäre allenfalls dann möglich, wenn ständig eine Person die Livebilder der Videokameras betrachtet, was in der Realität aber nicht der Fall war. Der Betreiber hatte zudem übersehen, dass sich im Regelfall, mit Ausnahme der Randzeiten, mehrere Personen im Fitnessstudio aufhalten, die im Bedarfsfall eingreifen und Hilfe holen können. Denkbar und empfehlenswert wäre es auch, Notknöpfe oder ein Notfalltelefon anzubringen, um im Bedarfsfall schnell medizinische Hilfe holen zu können. Auch wenn es dem grundsätzlichen Konzept eines personallosen Fitnessstudios zuwiderläuft, kommt zumindest in den Randzeiten auch eine Beaufsichtigung mittels Personal infrage.

Was die Überwachung der Spindbereiche (Umkleiden) angeht, ließ sich dem entgegenhalten, dass letztlich jedes Mitglied es selbst in der Hand hat, für den Schutz werthaltiger Gegenstände (wie zum Beispiel Smartphones) zu sorgen, indem diese immer mitgeführt werden. Daneben könnte der/die Betreiber/in auch separate Wertschließfächer bereitstellen.

Betrachtet man die Trainingsgeräte in einem Fitnessstudio, so ist lediglich bei Kleingeräten wie Hantelscheiben oder Kurzhandeln ein Diebstahl denkbar. Von Großgeräten oder fest verbauten Geräten lassen sich nicht ohne Weiteres einzelne Teile lösen und mitnehmen. Zudem gibt es alternative

Möglichkeiten wie Diebstahlsicherungen an einzelnen Fitnessgeräten oder etwa stichpunktartige Taschenkontrollen der Trainierenden. Nicht zu vergessen ist, dass zumindest in Stoßzeiten sowie beim Aufenthalt mehrerer Mitglieder eine gegenseitige soziale Kontrolle erfolgt, die eine verhaltenslenkende und letztlich abschreckende Wirkung auf potenzielle Diebe hat.

In jedem Fall wäre die Zulässigkeit der Videoüberwachung der Trainings- und Flurbereiche an den überwiegenden Interessen der Trainierenden gescheitert, hatten diese doch wegen der nahezu flächendeckenden Überwachung dieser Bereiche keine Ausweichmöglichkeit. Schwerer wiegt jedoch der Umstand, dass der Aufenthalt in einem Fitnessstudio zum Freizeitbereich zählt. Mitglieder suchen ein Fitnessstudio in erster Linie auf, um sich dort fit und gesund zu halten oder ihrem Hobby nachzugehen. Mitglieder pflegen den sozialen Austausch mit Gleichgesinnten, mit denen auch Freundschaften oder Trainingsgemeinschaften entstehen können, oder kommunizieren miteinander. Der Aufenthalt dort hat mithin auch eine soziale Komponente. Im Freizeitbereich überwiegen allerdings generell die Interessen der betroffenen Personen. Nicht zu vergessen ist außerdem, dass der/die Betreiber/in sowohl über die Möglichkeit der Sichtung der Livebilder als auch nachträglich mit Blick auf die Aufnahmen Mitglieder bei unvorteilhaften und nicht exakt ausgeführten Übungen sehen kann. Die permanente Videoüberwachung während der gesamten Öffnungszeiten auf dem Großteil der Trainingsflächen bedeutete schon aufgrund der Alternativlosigkeit der Trainierenden, die der Überwachung weder zeitlich noch räumlich ausweichen konnten, einen gravierenden Eingriff in das Grundrecht auf informationelle Selbstbestimmung. Das Interesse der Trainierenden, im Fitnessstudio überwachungsfrei trainieren zu können, überwiegt die Betreiberinteressen sowie auch einen möglichen Schutz vor Gefahren, die schlicht dem allgemeinen Lebensrisiko zuzurechnen sind.

Der/Die Betreiber/in zeigte sich einsichtig, und so konnte ich diese/n dazu bringen, die Videoüberwachung der Trainings- und Flurbereiche während der Betriebszeiten einzu-

stellen, ohne dass es der Ergreifung von Abhilfemaßnahmen bedurfte. Lediglich gegen die Videoüberwachung des Eingangsbereiches hatte ich keine rechtlichen Bedenken, da diese nicht zum dauerhaften Aufenthalt bestimmt sind. Ich konnte ebenfalls erreichen, dass die Hinweisbeschilderung mit Schildern gemäß den Vorgaben des Art. 13 DSGVO ergänzt wurde.

Fazit

Der Betrieb eines Fitnessstudios stellt grundsätzlich eine Gefahrenquelle dar, die besondere Anforderungen an ein personallos betriebenes Fitnessstudio stellt. Der/Die Betreiber/in unterliegt generell den sich aus dem Mitgliedschaftsvertrag ergebenden vertraglichen Schutzpflichten. Diese verpflichten ihn/sie allgemein dazu, sich bei der Vertragsabwicklung so zu verhalten, dass Körper, Leben, Eigentum und sonstige Rechtsgüter der Mitglieder nicht verletzt werden. Daneben trägt er/sie auch die gesetzliche Verkehrssicherungspflicht. Er/Sie hat also im Rahmen des Zumutbaren alles Notwendige und Erforderliche zu veranlassen, um die Mitglieder vor Schäden zu bewahren. Diese Pflichten bestehen aber nur in dem Maße, wie ein umsichtiger und vernünftiger Mensch notwendige und zumutbare Vorkehrungen treffen würde.
In einem Fitnessstudio zählt hierzu neben anderen die regelmäßige Kontrolle der Räumlichkeiten und Fitnessgeräte, nicht zuletzt zur eigenen Absicherung und der Minimierung von Verletzungsgefahren bei deren Benutzung. Der/Die Betreiber/in sollte aber aus eigenem Interesse den Grad seiner/ihrer Verantwortlichkeit nicht überspannen und sich etwa auch für die Aufklärung von Diebstählen unter den Mitgliedern in der Pflicht sehen. Auf der anderen Seite sollten sich Sportbegeisterte darüber im Klaren sein, dass der Aufenthalt in einem personallosen Fitnessstudio dem allgemeinen Lebensrisiko unterliegt und es bei der Nutzung der Fitnessgeräte zu Unfällen kommen kann. Es ist jedem Mitglied auch klar, dass in diesem Fall kein Personal zur Verfügung steht, das unmittelbar eingreifen kann.

Was ist zu beachten?
Der Betrieb eines personallosen Fitnessstudios rechtfertigt keine Videoüberwachung von Trainingsflächen. Hieran ändert auch die Gefahr möglicher medizinischer Notfälle nichts. Bloße Videoaufnahmen sind ohnehin nicht geeignet, diese zu erkennen. Dem verbleibenden Restrisiko hat der/die Betreiber/in im Rahmen der Sorgfalts- und Verkehrssicherungspflichten anderweitig zu begegnen.

2.2.7 Schutz von Warenautomaten mit Videokameras

↗ Art. 6 Abs. 1 Buchst. f DSGVO, Art. 13 DSGVO

Immer häufiger sind an belebten Orten im Freien Warenautomaten anzutreffen, deren Sortiment von Snacks und Getränken bis zu Speiseeis reicht. Im Wege einer Beratungsanfrage trat ein Betreiber zwei solcher Snack- und Getränkeautomaten, die er an einem regionalen Bahnhof aufgestellt hat, an mich heran. Diese befinden sich auf einem Grünstreifen entlang eines gut frequentierten Wegs in der Nähe des Bahnhofsparkplatzes. Er berichtete mir von Vandalismus an den Automaten, durch den ein erheblicher Sachschaden angerichtet worden war. Unbekannte hätten nicht nur versucht, die Scheiben der Automaten mit einem Gullideckel einzuschlagen, sondern hätten sich auch am Blech hinter dem Automaten, wo der Kompressor untergebracht sei, zu schaffen gemacht.
Zusätzlich zu bereits eingebauten Sicherheitssensoren (Türkontakt- und Vibrationssensoren) wollte er die beiden Automaten mittels einer Videokamera sichern. Dabei war beabsichtigt, nur die unmittelbar an die Automaten herantretenden Personen in einem Abstand von etwa einem Meter vor dem Automaten aufzuzeichnen. Zusätzlich würden gut sichtbare Hinweisschilder angebracht. Der Grundeigentümer der Stellflächen hatte sich damit bereits einverstanden erklärt.

Wertung

Ich teilte dem Betreiber mit, dass ich gegen eine Videoüberwachung des Nahbereichs vor den Warenautomaten keine grundsätzlichen Bedenken hätte. Er könne sich dabei auf die Interessenabwägung als Rechtsgrund stützen, Art. 6 Abs. 1 Buchst. f DSGVO. Danach ist eine Verarbeitung zulässig, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen.

Ein sich aus dem Eigentumsschutz und der mit der Videoüberwachung verbundenen Abschreckung potenzieller Straftäter/innen ergebendes berechtigtes Interesse war nach meiner Überzeugung gegeben. Durch den belegten Vorfall mit hohem Sachschaden war von einer konkreten Gefährdungslage auszugehen.
Mit der Beschränkung auf den unmittelbaren Nahbereich sah ich auch das mit dem Grundsatz der Datenminimierung in Zusammenhang stehende Erforderlichkeitsgebot ausreichend beachtet. Zur wirksamen Sicherung der Warenautomaten war die Erfassung einer Fläche von zwei Metern Breite und einem Meter Tiefe geplant. Dies war räumlich zum Schutz der Warenautomaten notwendig, aber auch ausreichend. Der Betreiber veranschaulichte mir den geplanten Überwachungsbereich mittels mehrerer Fotos, auf denen er mit Zollstöcken die Flächen gut sichtbar markiert hatte. Durch Ausblendung aller jenseits davon liegenden Bereiche ist letztlich sichergestellt, dass den Automaten in größerem Abstand passierende Personen von der Erfassung ausgenommen sind. Die Interessenabwägung fällt auch zugunsten des Betreibers aus. Er erfasst nur Personen, die sich dem Warenautomaten bewusst nähern und nicht etwa zufällig dort vorbeilaufende Passanten und Passantinnen. Die Intensität der Videoüberwachung und damit die Eingriffstiefe in das Recht auf informationelle Selbstbestimmung ist letzten Endes als gering einzustufen.
Da mir der Betreiber auch vorneweg signalisierte, entsprechende Hinweisschilder anzubringen, war davon auszugehen, dass er die gesetzlichen Informationspflichten des Art. 13 DSGVO einhält.

Fazit

In der heutigen Zeit sind auch Warenautomaten bedauerlicherweise immer wieder Ziel roher Gewalt, obgleich auch diese immer öfter allein mit Kartenzahlungsbetrieb eingerichtet sind und damit zumindest ein Anreiz, schnell an Bargeld zu kommen, kaum bestehen sollte. Beabsichtigt ein Betreiber bzw. eine Betreiberin seinen bzw. ihren Warenautomaten zu

Was ist zu tun?
Betreiber/innen von Warenautomaten können grundsätzlich bei entsprechender Erforderlichkeit, nachgewiesenen Schäden bzw. Vandalismus, Sachbeschädigung, den unmittelbaren Nahbereich vor einem Automaten in angemessenem Umfang überwachen. Die Zulässigkeit einer Videoüberwachung richtet sich nach den örtlichen Verhältnissen.

überwachen, kommt es auf die konkreten Verhältnisse im jeweiligen Einzelfall an. Empfehlenswert ist es, den Warenautomaten möglichst nicht auf dem Gehweg zu platzieren, sondern vorzugsweise angrenzend daran auf einer privaten Fläche wie etwa einem Grünstreifen. Steht der Warenautomat an einem belebten Ort, ist die Gefahr einer Beschädigung grundsätzlich geringer einzustufen als im Vergleich zu einem abgelegenen weniger frequentierten Standort. Zu berücksichtigen ist auch, wie groß der überwachte Bereich ist und ob bloße Passanten und Passantinnen eine Zone haben, in der sie unbeobachtet vorbeigehen können.

2.2.8 Extremer Fall der Videoüberwachung in einer Flüchtlingsunterkunft

↗ Art. 6 Abs. 1 Buchst. f DSGVO

Einen außergewöhnlichen Fall von Überwachung mittels Videotechnik stellte ich in einer Flüchtlingsunterkunft fest. Bekannt wurde mir dieser über die Beschwerde eines dort untergebrachten Flüchtlings. Dieser berichtete mir von mehreren von der Decke hängenden Rundum-Videokameras. Nachdem er mir hierzu einige Bilder vorgelegt hatte, die sein Vorbringen zunächst bestätigten, konfrontierte ich den Eigentümer damit. Ich staunte nicht schlecht, als dieser freimütig eine Anzahl von 37 Videokameras innerhalb der Flüchtlingsunterkunft einräumte. Auf dem mir vorgelegten Gebäudeplan waren schließlich noch weitere 35 Außenkameras zu erkennen, eine Kamera war noch projektiert. Dies veranlasste mich dazu, mir kurzfristig vor Ort selbst ein Bild von der Überwachungssituation zu machen.

Räumlichkeiten und Nutzung

Bei dem zuvor schriftlich gegenüber dem Eigentümer angekündigten Kontrollbesuch stellte sich heraus, dass die Flüchtlingsunterkunft für mehrere hundert Personen ausgelegt war.
Bereits bei meiner Ankunft außerhalb des Geländes waren mehrere Außenkameras sichtbar. Im Gebäudeinneren fielen

mir sofort mehrere der zuvor beschriebenen von der Decke herabhängenden 360°-Kameras auf. Ich konnte nur zu gut nachvollziehen, wie sich ein Gefühl der permanenten Überwachung aufgrund der schieren Anzahl der weithin sichtbaren Kameras insbesondere für die dortigen Bewohner/innen ergeben musste. Die Mitarbeitenden des privaten Sicherheitsdienstes, die sich am Empfangstresen sowie meistens im Eingangsbereich (Foyer) der Flüchtlingsunterkunft aufhielten, schienen sich hingegen kaum an den Kameras zu stören.

Die Anlage bestand aus einer großen ehemaligen Fabrikhalle sowie einem Außengelände. In der Halle befanden sich die durch provisorische Wände abgetrennten nach oben offenen Wohnbereiche (Kabinen) der Bewohner/innen. Weiter gab es dort einen Speisesaal mit Küche, einen Schulungs- und Freizeitraum, Arbeitsräume für die Bewohner/innen (wie Werkstatt, Friseur), Sanitärräume, einen Gebetsraum sowie Räume für den Dienstleister, der die Einrichtung betreibt und die soziale Betreuung der Flüchtlinge übernommen hat. Am Zugang zu dem Gelände kontrollierte ein privater Sicherheitsdienst die ein- und ausgehenden Personen.

Der Eigentümer der Immobilie, der die Videokameras angebracht hatte, gab mir gegenüber zur Auskunft, dass diese permanent aktiv seien. Nur in den Schulungsräumen würden die Kameras während der dortigen Schulungen deaktiviert. Es stellte sich jedoch heraus, dass nicht alle Videokameras tatsächlich in Betrieb waren. Bei einzelnen Videokameras waren die dort sichtbaren Wohnbereiche der untergebrachten Flüchtlinge geschwärzt. Die Kamerabilder wurden nur gespeichert, eine Livesichtung fand aufgrund der großen Datenmenge nicht statt.

Zwecke und Hintergründe für die Videoüberwachung

Auf die Frage nach den Beweggründen für die Anschaffung und Inbetriebnahme der Videoüberwachung bezog sich der Eigentümer auf zwei Vorfälle in anderen Gemeinschaftsunterkünften in Deutschland. Wichtig sei ihm daher, durch die Videoüberwachung aus Gründen der Sachverhaltsauf-

klärung alle Laufwege der Bewohnerinnen und Bewohner zu erfassen.
Der Eigentümer begründete die Videoüberwachung mit dem ständigen Wechsel der dort untergebrachten Personen. Er sah aufgrund der Vielzahl der die Einrichtung betretenden Personen eine vermeintliche besondere Gefährdungslage. Die Videoüberwachung habe den vorbeugenden Schutz der Einrichtungsgegenstände sowie der untergebrachten und dort tätigen Personen zum Ziel. Bereits mehrfach habe die Polizei zur Verfolgung von Straftaten zwischen den Bewohnerinnen und Bewohnern wegen Videoaufnahmen angefragt, die jeweils an diese herausgegeben worden seien. Der Zweck der Videoüberwachung liege in der Prävention und Abschreckung. Der Eigentümer ging davon aus, dass die Bewohnerinnen und Bewohner ihr Verhalten anpassen würden, wenn sie von einer (permanenten) Videoüberwachung ausgehen. Er ergänzte, dass es hin und wieder Auseinandersetzungen gebe und auch Gegenstände der Flüchtlinge entwendet würden, was daran liege, dass die Wohnräume nicht abschließbar seien.

Rechtliche Wertung

Bei keiner der von mir festgestellten Videokameras sah ich die Voraussetzungen für einen zulässigen Kamerabetrieb gegeben. Diese konnte sich einzig aus der Vorschrift des Art. 6 Abs. 1 Buchst. f DSGVO ergeben, wonach sich eine Verarbeitung personenbezogener Daten auf die Wahrung berechtigter Interessen stützen lässt, wenn diese hierzu erforderlich ist und die Interessen der betroffenen Personen das Verantwortlicheninteresse nicht überwiegen.
Es lag schon kein berechtigtes Interesse vor. Hierzu muss ein tatsächliches und gegenwärtiges Interesse vorliegen, ich benötige hierfür also konkrete Tatsachen, die eine (konkrete) Gefahrenlage belegen. Diese kann sich aus entsprechenden Vorfällen in der Vergangenheit oder anderen Ereignissen ergeben, die eine Gefahrenlage objektiv begründen können. Subjektive Befürchtungen genügen diesen Anforderungen nicht.
Zwar schienen die Argumente des Eigentümers nicht völlig aus der Luft gegriffen, jedoch fußten sie auf Vorfällen aus

anderen Gemeinschaftsunterkünften in Deutschland. Bezogen auf den konkreten Fall, taugten sie nur als Ausdruck vager Befürchtungen potenzieller Vorfälle, die es mit der Videoüberwachung zu vermeiden galt. Auch statischen Daten (zum Beispiel die polizeiliche Kriminalitätsstatistik) oder vergleichbare Auswertungen, die gelegentlich angeführt werden, fehlt der Bezug zur konkreten Videoüberwachung. Hinzu kam in dem Fall, dass der Eigentümer explizit den vernünftigen und guten persönlichen Umgang mit den Bewohnerinnen und Bewohnern herausstellte und es in dem halben Jahr des Kamerabetriebs noch keinen Fall von Vandalismus und Schäden an der Einrichtung gegeben hatte. Dies belegte umso mehr, dass sich die Videoüberwachung letzten Endes einzig auf rein hypothetische und spekulative Erwägungen stützte. Anzeichen für das Vorliegen einer konkreten Gefährdungslage konnte ich jedenfalls nicht feststellen.

Die mutmaßlichen polizeilichen Anfragen zur Herausgabe des Videomaterials konnten hieran nichts ändern. Denn private Stellen sind nicht dazu berufen, Hilfstätigkeiten für die staatlichen Ermittlungsbehörden zu erbringen, zumal die Ermittlung und Untersuchung von Straftaten eine rein hoheitliche Aufgabe ist. Es ist zwar durchaus nachvollziehbar, dass vor dem Hintergrund des beengten Zusammenlebens von Menschen mit teils traumatisch oder psychisch belastenden Fluchterfahrungen und angesichts unterschiedlicher Religionszugehörigkeiten Spannungen entstehen, Auseinandersetzungen auftreten können und es auch zu Straftaten wie Körperverletzungen oder Diebstahl kommen kann. Eine Videoüberwachung mit dem Zweck, die Aufklärung von Straftaten unter den Bewohnerinnen und Bewohnern zu fördern, liegt jedoch erkennbar nicht in der Sphäre des Eigentümers. Ein berechtigtes Verantwortlicheninteresse, wie es die Vorschrift des Art. 6 Abs. 1 Buchst. f DSGVO verlangt, lässt sich damit also nicht begründen.

Die Videoüberwachung war außerdem zum Eigentumsschutz sowie dem Schutz der Bewohner/innen und dort tätigen Personen nicht geeignet. Der Eigentümer übersah, dass sich Vorfälle bei nachträglicher Sichtung von Videoaufnahmen

bereits ereignet haben. Zu bedenken war außerdem, dass das Vorhandensein von Videokameras bei Affekthandlungen völlig ausgeblendet wird und Menschen in psychischen Ausnahmesituationen nicht rational handeln. Ferner fand bereits eine routinemäßige Eingangskontrolle des privaten Sicherheitsdienstes statt, der auch regelmäßig Kontrollgänge auf dem Gelände durchführte. Objektiv betrachtet sind diese ohnehin weitaus effektiver als eine Videoüberwachung, denn nur in dem Moment, in dem Vorkommnisse wahrgenommen werden, besteht die reale Möglichkeit eines unmittelbaren Eingreifens.

Schließlich hätten auch die Betroffeneninteressen überwogen. Insbesondere die „Wohnraumnähe" der Videoüberwachung war aus Sicht der Bewohnerinnen und Bewohner unzumutbar und in besonderem Maße belastend. Mit Ausnahme des Gebetsraums, der Sanitärräume sowie der Wohnbereiche (Kabinen) – waren die untergebrachten Personen ständig unter Beobachtung und auf Schritt und Tritt im Fokus der Kameras. Jede Bewegung beim Verlassen der Wohnbereiche konnte beobachtet und nachverfolgt werden. Die Überwachung des Speiseraums, der Arbeitsplätze sowie der Aufenthalts- und Gemeinschaftsräume (Freizeiteinrichtungen) war ohnehin a priori unzulässig.

Datenschutz-Folgenabschätzung

In dem Fall einer derart massiven Videoüberwachung hätte der Eigentümer anhand des räumlichen Umfangs der überwachten Bereiche sowie der Vielzahl der Videokameras zuvor eine Datenschutz-Folgenabschätzung vornehmen müssen. Man konnte mit Fug und Recht von einer umfangreichen und systematischen umfangreichen Überwachung sprechen. Darin hätten auch die Risiken für die von der Überwachung betroffenen Personen – in erster Linie die dortigen Bewohner/innen sowie die Mitarbeiter/innen der Betreiberfirma – entsprechende Beachtung finden müssen. Die Pflicht, eine Datenschutz-Folgenabschätzung vorzunehmen, hat als Konsequenz, dass auch ein Datenschutzbeauftragter zu benennen ist.

Umfang des Grundrechtsschutzes

Im Übrigen kann sich jede natürliche Person auf das Recht auf informationelle Selbstbestimmung berufen. Auch das in Artikel 8 der Grundrechtecharta der Europäischen Union enthaltene Grundrecht auf Datenschutz ist nicht auf EU-Staatsangehörige beschränkt. Danach hat jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten.

Ergebnis

Schließlich konnte ich im direkten Kontakt mit dem Eigentümer erreichen, dass er alle Videokameras außer Betrieb nimmt. Ansonsten hätte ich mich gezwungen gesehen, eine schriftliche Anordnung mitsamt einer Zwangsgeldandrohung zu erlassen. Dies habe ich dem Eigentümer gegenüber auch unmissverständlich so klargemacht. Wie mir der Eigentümer wenige Monate später mitgeteilt hat, sind die Verträge zur Unterbringung von Asylsuchenden ausgelaufen – somit steht das Gebäude, in dem die Flüchtlinge vormals untergebracht war, nunmehr leer.

Was ist zu tun?
Subjektive Einschätzungen reichen nicht aus, um eine Videoüberwachung auf der Grundlage von Art. 6 Abs. 1 Buchst. f DSGVO zu rechtfertigen, auch wenn sie sich auf statistische Daten gründen. Diese belegen lediglich eine abstrakte Gefährdungslage, auf die sich regelmäßig keine zulässige Videoüberwachung stützen lässt.

2.2.9 Telepräsenz-Avatare im Unterricht

↗ Art. 2 GG; Art. 4, 6, 7 DSGVO; § 1 SächsFrTrSchulG; §§ 3, 38b SächsSchulG; § 201 StGB

Eine Schule in freier Trägerschaft hatte den Einsatz eines Telepräsenz-Avatars im Unterricht erwogen, um einem langzeiterkrankten Schüler dennoch die Teilnahme am Unterricht mittels Videoübertragung zu ermöglichen. Das hierfür vorgesehene Bild- und Tonübertragungsgerät, ein Computer mit Monitor, sollte im Unterricht und gegebenenfalls auch in den Pausen zum Einsatz kommen, im Klassenraum platziert werden und das Unterrichts- und Pausengeschehen in Bild und Ton an das Endgerät des Schülers übertragen. Der Schüler habe die Möglichkeit der Fernsteuerung der Kamera und deren Blickrichtung und könne sich optisch und akustisch bemerkbar machen, wenn er etwas zum Unterricht oder zur Pausenunterhaltung beitragen möchte. Eine Bildübertragung vom schulabwesenden Schüler in den Klassenraum erfolge

nicht. Zur Zulässigkeit des Einsatzes eines solchen Verfahrens habe ich mich wie folgt positioniert:

1. Verarbeitung personenbezogener Daten der Schüler/innen

a) Grundsätzlich kommt zunächst Art. 6 Abs. 1 Buchst. e DSGVO als Rechtsgrundlage in Betracht, denn der Einsatz des Verfahrens und des Avatars dient der Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe, namentlich der Mitwirkung der freien Schule bei der Erfüllung der öffentlichen Bildungsaufgaben (§ 1 Sächsisches Gesetzes über Schulen in freier Trägerschaft [SächsFrTrSchulG]). Gleichwohl fehlt es vorliegend schon an der Erforderlichkeit des Einsatzes eines Telepräsenz-Avatars für die diesbezügliche Aufgabenwahrnehmung. Grundsätzlich sind für die Erfüllung des Bildungsauftrags der Verfassung des Freistaats Sachsen vielfältige Möglichkeiten gegeben, wobei dem Präsenzunterricht natürlich der Vorrang gebührt. Aber auch in dem zu betrachtenden Fall eines langzeiterkrankten Schülers bestehen – soweit das angesichts der Art und Dauer der Erkrankung des betreffenden Schülers überhaupt möglich und angezeigt ist – eine ganze Reihe von alternativen Möglichkeiten der Teilhabe am Unterrichtsgeschehen, zuallererst selbstredend E-Learning-Plattformen wie etwa Lernsax. Davon abgesehen bedürfte es bei der Inanspruchnahme der Vorschrift des Art. 6 Abs. 1 Buchst. e DSGVO zusätzlich einer Rechtsgrundlage im (Schul-) Recht des Freistaats Sachsen
(Art. 6 Abs. 3 Satz 1 Buchst. b DSGVO). Eine solche, insbesondere auch den Anforderungen des Art. 6 Abs. 3 Sätze 2 und 3 DSGVO genügende Rechtsgrundlage ist aber nicht ersichtlich.
Insbesondere die Bezugnahme auf die das Thema E-Learning betreffende Vorschrift des § 38b Sächsisches Schulgesetz (SächsSchulG) geht an dieser Stelle fehl, weil es für die Anwendbarkeit des Sächsischen Schulgesetzes auch auf Schulen in freier Trägerschaft einer ausdrück-

lichen gesetzlichen Bestimmung bedarf (§ 3 Abs. 1 Satz 3 SächsSchulG). Daran fehlt es vorliegend; weder im Sächsischen Schulgesetz noch im Sächsischen Gesetz über Schulen in freier Trägerschaft findet sich eine Regelung, dass § 38b SächsSchulG auch für Schulen in freier Trägerschaft anwendbar sein soll.
Aber auch unabhängig davon bietet § 38b SächsSchulG, der im Übrigen eines im Vorfeld des Einsatzes eines Telepräsenz-Avatars von der Schulkonferenz beschlossenen pädagogischen Konzeptes bedarf (§ 38b Satz 1 SächsSchulG), keine ausreichende Rechtsgrundlage für den Einsatz eines Telepräsenz-Avatars, denn er sagt lediglich aus, dass Schülerinnen und Schüler, insbesondere auch längerfristig erkrankte, zeitweilig auch über E-Learning unterrichtet werden können. Insoweit ist in dieser Vorschrift nur eine grundsätzliche Erlaubnis zur Nutzung solcher Lernformen für die Schulen zu sehen, stellt jedoch keine ausreichend bestimmte und konkrete Rechtsgrundlage für die Verarbeitung personenbezogener Daten mittels eines Telepräsenz-Avatars dar. Ich verweise insoweit neben Art. 6 Abs. 3 Sätze 2 und 3 DSGVO insbesondere auch auf die Rechtsprechung des Bundesverfassungsgerichts (Urteil vom 15. Dezember 1983 – 1 BvR 209/83, juris), wonach Eingriffe in das Recht auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 Grundgesetz einer (verfassungsmäßigen) gesetzlichen Grundlage bedürfen, aus der sich die Voraussetzungen und der Umfang der Beschränkungen klar und für den Bürger erkennbar ergeben und die damit dem rechtsstaatlichen Gebot der Normenklarheit entspricht. § 38b SächsSchulG enthält aber weder Vorgaben hinsichtlich des Umfangs oder des Zwecks der Verarbeitung personenbezogener Daten noch die ausdrückliche Befugnis, personenbezogene Daten dazu verarbeiten zu dürfen. Auch fehlen Vorgaben für organisatorische und verfahrensrechtliche Vorkehrungen.
Im Ergebnis der Überlegungen kann der Einsatz eines Telepräsenz-Avatars also nicht auf Art. 6 Abs. 1 Buchst. e

DSGVO in Verbindung mit § 38b SächsSchulG gestützt werden.

b) Für Schulen in freier Trägerschaft – als nichtöffentliche Stellen – kommt als Rechtsgrundlage noch eine Interessenabwägung gemäß Art. 6 Abs. 1 Buchst. f DSGVO in Betracht.

Es kann dahinstehen, ob man vorliegend das berechtigte Interesse der Schule, also die Erfüllung des Bildungsauftrages, oder das berechtigte Interesse des Schülers, mithin die Teilhabe am Schulunterricht trotz Erkrankung, in der Interessenabwägung aufgreift. In beiden Fällen ist schon die Erforderlichkeit des Einsatzes eines Telepräsenz-Avatars fraglich, denn natürlich gibt es alternative mildere Mittel, die weniger oder gar nicht in die Rechte der betroffenen Mitschüler und Mitschülerinnen sowie Lehrkräfte eingreifen. Das kann die in der freien Schule genutzte E-Learning-Plattform sein, in Betracht kommen aber auch Erklärvideos, Konsultationen über Telefon, Kommunikation über E-Mail und andere Varianten der Einbeziehung erkrankter Schüler/innen in den Unterrichtsablauf. Gleichwohl ist einzuräumen, dass diese milderen Alternativen natürlich nicht absolut gleichwertig sind, insbesondere was die „synchrone und sozial-interaktive" Teilhabe am Präsenzunterricht der Mitschüler/innen betrifft.

Ob mithin von einer Erforderlichkeit im Sinne des Art. 6 Abs. 1 Buchst. f DSGVO ausgegangen werden kann, ist aber eben auch nicht allein entscheidend, denn in die sich anschließende Interessenabwägung sind ja auch die betroffenen Personen zu berücksichtigen und dabei fällt die Abwägung klar zugunsten der in der Klasse befindlichen Datenschutzrechte der Mitschüler und Mitschülerinnen aus. Diese können nicht abschätzen, wer alles aus der Ferne das Unterrichtsgeschehen mitverfolgt – naheliegend ist, dass natürlich auch die Eltern oder andere Familienangehörige ein Interesse haben, mitzuerleben, wie ihr erkranktes Kind von zu Hause aus am Unterricht teilnimmt, welche Herausforderungen sich dabei stellen

und ob es benachteiligt und wie es bewertet wird – und gegebenenfalls auch (unzulässigerweise) aufzeichnet. Diese Öffnung des üblicherweise in einer geschlossenen, definierten Umgebung (Unterrichtsraum/Schulklasse) stattfindenden Unterrichts nach außen, mindestens in die Familie des erkrankten Schülers hinein, birgt ohne Zweifel eine Reihe von Risiken und führt wegen des Überwachungsdruckes auch zu Verhaltensänderungen und Verhaltensanpassungen bei den Schülern und Schülerinnen ähnlich wie bei Hospitationen. Art. 6 Abs. 1 Buchst. f DSGVO stellt Kinder insoweit aber unter einen besonderen Schutz, das heißt, deren Interessen ist bei der Abwägung schon von Gesetzes wegen ein besonderes Gewicht verliehen.

Vor diesem Hintergrund geht die Interessenabwägung also zugunsten der betroffenen Mitschüler/innen aus; auch auf Art. 6 Abs. 1 Buchst. f DSGVO kann die mit dem Betrieb eines Telepräsenz-Avatars verbundene Verarbeitung von Schülerdaten nicht gestützt werden.

c) Im Ergebnis verbleiben als tragfähige Rechtsgrundlage derzeit nur Einwilligungen nach Art. 7 DSGVO, auch wenn in Bezug auf die Freiwilligkeit durchaus Bedenken ins Feld geführt werden könnten. Denn es ist nicht ohne Weiteres von der Hand zu weisen, dass vorliegend und in vergleichbaren Fallgestaltungen auch ein gewisser sozialer Druck zur Erteilung der Einwilligung bestehen wird. Schließlich möchte kein/e Schüler/in und auch kein Elternteil als derjenige dastehen, der einem erkrankten Schüler die Teilhabe am Live-Unterricht durch Verweigerung der Einwilligung letztendlich verwehrt. Genau dies stellt das Problem der Einwilligungslösung dar: Es reicht schon, dass lediglich ein/e Schüler/in keine Einwilligung erteilt, um das gesamte Vorhaben zu stoppen. Gleichwohl ist dies zurzeit wohl die einzige kurzfristig umsetzbare Lösung (vergleiche dazu aber auch nachfolgend Buchst. d), die so übrigens auch von Herstellern der Telepräsenz-Avatare und auch von

anderen Datenschutzaufsichtsbehörden (Der Landesbeauftragte für Datenschutz und Informationsfreiheit der Freien Hansestadt Bremen: 7. Jahresbericht nach der Datenschutz-Grundverordnung, 9.3; Unabhängiges Datenschutzzentrum Saarland: 33. Tätigkeitsbericht 2024, 7.1) vertreten wird.

d) Anders als Schulen in öffentlicher Trägerschaft haben freie Schulen darüber hinaus die Möglichkeit, den Einsatz von Telepräsenz-Avataren (langfristig) über entsprechende Regelungen in den Schulverträgen und damit über Art. 6 Abs. 1 Buchst. b DSGVO abzusichern. Dazu bedürfte es aber klarer Festlegungen, unter welchen Voraussetzungen, für welche Zeiträume und unter welchen Rahmenbedingungen der Einsatz eines entsprechenden Verfahrens mit Avatar infrage kommen kann. Es liegt auf der Hand, dass dies nur eine Lösung für die Zukunft sein kann.

e) Soweit sich der Einsatz von Avataren auch auf Zeiten außerhalb der Unterrichtsstunden, mithin die Pausen, erstrecken soll, sehe ich dafür keine Möglichkeit. Die soziale Teilhabe in den Pausen ist vom Bildungsauftrag der Schulen nicht umfasst und würde zu unakzeptablen Beeinträchtigungen des Persönlichkeitsrechts der Mitschüler/innen führen. Allzu leicht würde im Pausentrubel die über den Avatar bestehende mittelbare Präsenz des tatsächlich nicht anwesenden Schülers in Vergessenheit geraten bzw. übersehen, sodass dieser Schüler regelmäßig Informationen und Handlungen (unbemerkt) zur Kenntnis nehmen könnte, die so für ihn nicht bestimmt sind. Dabei ist auch zu berücksichtigen, dass sich der Erfassungsbereich des Avatars in den Pausen durchaus auch auf Personen außerhalb des Klassenverbandes und damit auf Personen, die keine Einwilligung erteilt oder noch nicht einmal Kenntnis vom Betrieb des Avatars haben, erweitern kann und auch wird. Auch vertrauliche, nicht für Dritte bestimmte Gesprächsinhalte, die regelmäßig außerhalb des Unterrichts stattfinden, könnten

auf diese Weise übermittelt werden und damit einen strafrechtlich relevanten Bereich (§ 201 Strafgesetzbuch) berühren.
Tatsächlich ist davon auszugehen, dass Kinder und Jugendliche über verschiedene (private) Kommunikationsmöglichkeiten verfügen und diese untereinander auch – auch und gerade in Krankheitszeiten – bezeichnenderweise häufig sogar zu extensiv – nutzen; einer diesbezüglichen Unterstützung durch die Schule (in den Pausenzeiten) bedarf es dazu nicht.

2. Verarbeitung personenbezogener Daten der Lehrkräfte

a) Der Betrieb eines Telepräsenz-Avatars berührt nicht nur die Persönlichkeitsrechte der Schüler/innen, sondern auch und vor allem des Lehrpersonals.
Die unter Nummer 1 Buchstabe a und b erfolgten Ausführungen gelten daher sinngemäß auch für Lehrkräfte.
Mithin kommen auch hier weder Art. 6 Abs. 1 Buchst. e noch Buchst. f DSGVO als Rechtgrundlage in Betracht.

b) Ein wesentlicher Unterschied besteht jedoch in Bezug auf die Einwilligung, für deren Anwendung im Beschäftigungsverhältnis sehr enge Grenzen gezogen sind.
Die Anforderungen an eine wirksame Einwilligung sind in Art. 4 Nr. 11 und Art. 7 DSGVO festgelegt. Nach Art. 4 Nr. 11 DSGVO ist eine „Einwilligung" der betroffenen Person jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.
Besonderes Augenmerk ist nach der Datenschutz-Grundverordnung auf die Freiwilligkeit einer Einwilligung zu richten. Es kann nur dann davon ausgegangen

werden, dass eine betroffene Person ihre Einwilligung freiwillig gegeben hat, wenn sie eine echte und freie Wahl hat, also in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden (Erwägungsgrund 42 zur DSGVO, Satz 5). Eine Einwilligung liefert regelmäßig immer dann keine gültige Rechtsgrundlage, wenn zwischen der betroffenen Person und dem Verantwortlichen – wie das im Arbeitsverhältnis der Fall ist – ein klares Ungleichgewicht besteht und es deshalb unwahrscheinlich ist, dass die Einwilligung freiwillig gegeben wurde (Erwägungsgrund 43 zur DSGVO, Satz 1).

Im Beschäftigungsverhältnis kommt eine wirksame Einwilligung aufgrund des Über-/Unterordnungsverhältnisses also regelmäßig nicht in Betracht (vgl. dazu auch § 21 des Referentenentwurfs zum Beschäftigtendatengesetz – BeschDG – vom 8. Oktober 2024). So entfällt die Freiwilligkeit immer dann, wenn sich die betroffenen Personen im Beschäftigungsverhältnis beeinflusst, gedrängt, bestimmt oder gezwungen sehen, ohne dass es einer Zwangsausübung bedarf.

Nur ausnahmsweise können Beschäftigte in die Verarbeitung ihrer personenbezogenen Daten durch ihre Arbeitgeber einwilligen. Dabei handelt es sich ausschließlich um sogenannte arbeitnehmernützige Verarbeitungen, also beispielsweise wenn der Beschäftigte einen rechtlichen oder wirtschaftlichen Vorteil erhält. Dies ist vorliegend nicht der Fall; tatsächlich unterliegt die Lehrkraft durch den Avatar stattdessen sogar einem erhöhten Überwachungsdruck. Das Kriterium „Freiwilligkeit" ist also zweifelsfrei nicht erfüllt.

Einwilligungen, die nicht zweifelsfrei freiwillig erteilt worden sind, sind unwirksam und können nicht als Rechtsgrundlage für eine Datenverarbeitung herangezogen werden.

Im Ergebnis scheidet also Art. 6 Abs. 1 Buchst. a DSGVO als Rechtsgrundlage für die Verarbeitung personenbezogener Daten der Lehrkräfte aus.

c) Nach meiner Auffassung können die Arbeitgeber nichtöffentlicher Stellen die Datenverarbeitungen in Beschäftigungskontext jedoch auf Art. 6 Abs. 1 Buchst. b DSGVO (zur Erfüllung des Arbeitsvertrages) stützen. Dies gilt auch für die Anweisung des Arbeitgebers, den Unterricht gegebenenfalls unter zusätzlichem Einsatz eines Telepräsenz-Avatars durchzuführen.

Unter die Erfüllung des Arbeitsvertrages im Sinne des Art. 6 Abs. 1 Buchst. b DSGVO fallen sämtliche Datenverarbeitungen, die unmittelbar mit der Durchführung des Arbeitsvertrages zusammenhängen und dafür erforderlich sind, demnach also auch Datenverarbeitungen, die es den Beschäftigten ermöglichen, ihre vertraglich geschuldete Tätigkeit zu erbringen, ebenso das Weisungsrecht des Arbeitgebers.

Die arbeitsvertraglich geschuldete Verpflichtung besteht vorliegend in der Unterrichtung von Schülern und Schülerinnen. Der konkrete Inhalt der zu erbringenden Arbeitsleistungen ergibt sich grundsätzlich aus dem Arbeitsvertrag. Entsprechend dieser Regelungen bestimmt sich der Umfang des Direktionsrechts des Arbeitgebers. Ob die Erbringung der Tätigkeit des Schulunterrichts auch mittels Telepräsenz-Avatars laut Arbeitsvertrag geschuldet ist oder vom Arbeitgeber im Rahmen des Direktionsrechtes angeordnet werden kann, es einer Änderungskündigung oder einer einvernehmlichen Änderung des Arbeitsvertrages durch die Arbeitsvertragsparteien bedarf, ist aber eine zivil- bzw. arbeitsrechtliche Vorfrage, die von mir nicht entschieden werden kann.

Soweit die Unterrichtung auch mittels Videoübertragung bzw. mit Telepräsenz-Avatar arbeitsvertraglich geschuldet bzw. vom Direktionsrecht umfasst wäre, könnte damit Art. 6 Abs. 1 Buchst. b DSGVO als Rechtsgrundlage herangezogen werden. Im Zuge der diesbezüglichen Erforderlichkeitsprüfung wären auch die Grundrechte der Lehrkräfte zu berücksichtigen.

Was ist zu tun?
Der Einsatz von Videoübertragungstechnik bzw. Telepräsenz-Avataren zur Unterrichtsteilhabe kann sich nur auf den Unterricht selbst beziehen, ist jedoch nicht in den Pausen statthaft. Für die Verarbeitungen der Daten von Mitschülern und Mitschülerinnen kommen dabei kurzfristig nur Einwilligungen in Betracht, darüber hinaus kann in Schulen in freier Trägerschaft erwogen werden, diese Verarbeitungen zukünftig in den Schulverträgen zu verankern. Bei Lehrkräften könnte die Verarbeitung auf arbeitsvertragliche Regelungen und dann das Direktionsrecht des Arbeitgebers gestützt werden.

Im Übrigen schließe ich nicht aus, dass der Gesetzgeber den hier vorliegenden Regelungsbedarf erkennt und noch eine gesetzliche, für alle Schulträger gleichermaßen anwendbare normenklare Regelung schafft, die Umfang, Tiefe und Ausmaß einer entsprechenden personenbezogenen Datenverarbeitung bestimmt und die Einwilligungen oder vertragliche Lösungen für den Einsatz von Videoübermittlungstechnik und Telepräsenz-Avataren entbehrlich macht.

2.2.10 Offene Bekanntgabe von Noten im Klassenverbund

↗ Art. 4 DSGVO, § 3 SächsDSDG, § 63a SächsSchulG, Teil II. 3. Buchst. b) Sächs. VwV Schuldatenschutz

Während des Berichtszeitraumes erreichten mich verschiedene Anfragen und Beschwerden von Schülerinnen und Schülern oder deren Eltern. Gerügt wurde jeweils, dass durch die Lehrperson die Noten einzelner oder aller Lernenden einer Klasse (oder eines Kurses) laut dargestellt wurden. Dabei seien die Noten einzelnen Individuen direkt zuzuordnen gewesen. Hierin wurde eine unberechtigte Offenlegung dieser personenbezogenen Daten gesehen.
Grundsätzlich ist festzuhalten, dass es sich bei Noten – also der Bewertung einer Leistung – um personenbezogene Daten handelt und die anderen Schülerinnen und Schüler der Klasse in diesem Zusammenhang „Dritte" im Sinne von Art. 4 DSGVO sind. Eine Offenlegung dieser Daten darf daher nur aufgrund einer Rechtsgrundlage erfolgen.
Diese Rechtsgrundlage liefert § 63a Sächsisches Schulgesetz. In diesem sind die Grundlagen des Schuldatenschutzes normiert. Unter anderem enthält er auch die Ermächtigungsvorschrift für das Sächsische Staatsministerium für Kultus, die Details des Datenschutzes in Schulen mittels einer Verwaltungsvorschrift genauer zu regeln. Von dieser Ermächtigung wurde Gebrauch gemacht und die Verwaltungsvorschrift Schuldatenschutz verkündet (Sächs. VwV Schuldatenschutz vom 11. Juli 2018 [MBl. SMK S. 282], zuletzt enthalten in der Verwaltungsvorschrift vom 9. Dezem-

ber 2025 [SächsABl. SDr. S. S 255]). Diese regelt nicht nur Voraussetzungen des Datenschutzes, sondern liefert auch abgestimmte Formblätter.

In Teil II. 3. der Sächs. VwV Schuldatenschutz ist die Verarbeitung von Schülerdaten geregelt. Unter Buchst. b folgt ausdrücklich die Möglichkeit, dass Noten in der Klasse oder im Kurs nach Ermessen der Lehrerin bzw. des Lehrers offengelegt werden dürfen. Es kommt daher auf eine Ermessensentscheidung der Lehrperson an. Eine Ermessensentscheidung ist eine Einzelfallentscheidung, bei der die verschiedenen Interessen gegeneinander abgewogen werden müssen. So ist in diesem Spannungsverhältnis das Interesse an der bestmöglichen Bildung auf der einen und auf der anderen Seite das Selbstbestimmungsrecht der Schüler/innen zu betrachten.

Dabei kann das Offenbaren der Noten pädagogisch wertvoll sein. Es ermöglicht der Lehrkraft die Erläuterung typischer oder besonderer Stärken und Schwächen an konkreten Beispielen und erleichtert die Einschätzung eigener Leistungen. Außerdem dient es der Transparenz und bietet den Schülerinnen und Schülern die Gewähr, dass die Notengebung dem Grundsatz der Chancengleichheit folgt.

Gleichsam birgt es die Gefahr, dass sich Schüler/innen herabgewürdigt sehen oder die Noten Grundlage für Spott und Hänseleien bilden. Darüber hinaus handelt es sich bei den Noten um personenbezogene Daten, welche grundsätzlich schützenswert sind.

Dabei ist ebenfalls zu beachten, dass die oben genannten pädagogischen Ziele durch andere Maßnahmen auch erreicht werden können, zum Beispiel: einem anonymisierten Notenspiegel, offene Diskussionszeiten, in denen die Schüler/innen untereinander austauschen können, gegenüber wem sie die Noten offenbaren möchten oder das Einholen der Einwilligung in die Offenlegung.

Unter keinen Umständen darf die Lehrkraft die Notenverkündung nutzen, um Schüler/innen herabzuwürdigen. Soweit der Lehrkraft bekannt ist, dass Hänseleien aufgrund der Noten stattfinden und damit ein unfreundliches Klima

Was ist zu tun?
Lehrer/innen müssen bei jeder Notenverkündung eine Ermessensentscheidung treffen, ob die Offenbarung der Noten gegenüber allen anwesenden Schülerinnen und Schülern pädagogisch am wertvollsten ist. Nur dann ist die Offenbarung rechtmäßig.

in der Gemeinschaft der Klasse geschaffen oder weiter verstärkt wird, ist eine offene Bekanntgabe ebenfalls nach den oben genannten Gesichtspunkten ausgeschlossen. Nur wenn sich im Rahmen der Ermessensentscheidung zu der jeweiligen Notenverkündung ergibt, dass die Offenbarung an alle anwesenden Schüler/innen pädagogisch am wertvollsten ist, kann dies auch erfolgen.

2.2.11 Onlineanhörung im Bußgeldverfahren

↗ § 46 Abs. 1 OWiG in Verbindung mit § 136 Abs. 1 Satz 2 StPO

Im Rahmen der Petitionsbearbeitung habe ich mich auch mit der Frage der datenschutzrechtlichen Rechtmäßigkeit von Onlineanhörungen im Bußgeldverfahren beschäftigt. Dabei habe ich eine Bußgeldbehörde gebeten, mir eine entsprechende Testkennung und ein Passwort – jeweils als Betroffener und als Zeuge – zu übersenden.
Bei der Prüfung der Onlineanhörung stellte ich datenschutzrechtliche Mängel fest. Da es sich bei dieser Anwendung um ein Tool handelt, welches die vertreibende Firma mehreren sächsischen Bußgeldstellen bereitstellt und der Verdacht nahelag, dass die Mängel auch bei der Verwendung durch andere Nutzer/innen auftreten, habe ich zudem die Onlineanhörung einer sächsischen Großstadt in Ordnungswidrigkeitenverfahren geprüft und ebenfalls datenschutzrechtliche Verstöße festgestellt.
Im Bußgeldverfahren ist dem/der Betroffenen gemäß § 55 Abs. 1 Gesetz über Ordnungswidrigkeiten (OWiG) in Verbindung mit § 163a Abs. 1 Strafprozessordnung (StPO) die Gelegenheit zu gewähren, sich zum Vorwurf zu äußern. Über die Form der Anhörung entscheidet die Verwaltungsbehörde nach pflichtgemäßem Ermessen. Dazu stehen ihr drei Möglichkeiten zur Auswahl: persönliche Anhörung in mündlicher Form, elektronische oder schriftliche Anhörung durch Versendung eines Anhörungsdokuments und Ladung zur förmlichen Vernehmung in das Dienstgebäude. Die schriftliche und elektronische Anhörung ist insbesondere für Massenverfahren, zum

Beispiel bei Verkehrsordnungswidrigkeiten, geeignet und wird meines Wissens von allen sächsischen Bußgeldstellen verwendet. Grundsätzlich muss jedoch eine Onlineanhörung – als lediglich weitere Möglichkeit für den Betroffenen, seinen Anspruch auf rechtliches Gehör wahrzunehmen – zwingend inhaltsgleich zum schriftlichen Verfahren ausgestaltet sein und die gesetzlichen Vorgaben erfüllen.

In den von mir geprüften Onlineanhörungen eines Betroffenen wurde dieser mittels Pflichtfeld (im Formular mit einem „*" gekennzeichnet) gezwungen, Angaben zur Sache – „Haben Sie das Tatfahrzeug geführt?" – zu machen. Dies widerspricht § 46 Abs. 1 OWiG in Verbindung mit § 136 Abs. 1 Satz 2 StPO und ist rechtswidrig. Dem/Der Betroffenen steht es nach dem Gesetz frei, sich zu der Beschuldigung zu äußern oder nicht zur Sache auszusagen. Ich habe die betroffenen Bußgeldbehörden angewiesen, diese Einstellung mit sofortiger Wirkung abzuändern.

Auch die geprüften Onlineanhörungen von Zeuginnen bzw. Zeugen entsprachen nicht dem schriftlichen Anhörungsbogen und damit auch nicht den gesetzlichen Vorgaben. Schriftlich gab es zwei Reaktionsmöglichkeiten: Angaben zum/zur Fahrzeugführer/in oder die Inanspruchnahme des Zeugnisverweigerungsrechts (ZVR) gemäß § 46 Abs. 1 OWiG in Verbindung mit §§ 52 ff. StPO mit dem Unterbleiben einer Angabe. Online hingegen musste die Zeugin bzw. der Zeuge (Pflichtfeld) angeben, ob ihm der/die Fahrzeugführer/in bekannt ist („ja/nein"). Die Möglichkeit von einem eventuell einschlägigen ZVR Gebrauch zu machen, lag nicht vor bzw. ergab sich erst, wenn die Zeugin bzw. der Zeuge bereits eine Aussage zur/zum Fahrzeugführenden machte („ja"). Hierin liegt ein klarer Verstoß gegen die gesetzlichen Bestimmungen über das ZVR. Deshalb müssen bei der Onlineabfrage, ob der Zeugin bzw. dem Zeugen die bzw. der Fahrzeugführende bekannt ist, die Eingabemöglichkeiten „ja" und „nein" um eine weitere Variante – „Ich mache von meinem Zeugnisverweigerungsrecht Gebrauch" – ergänzt werden.

Zudem wurde bei einer Onlineanhörung nach der Angabe, vom ZVR Gebrauch zu machen, der Verwandtschaftsgrad erfragt.

Dies stellte eine weitere Diskrepanz zum schriftlichen Fragebogen dar. Zwar war diese Abfrage nicht als Pflichtfeld ausgestaltet, gleichwohl sollte sie aus Gründen der Datensparsamkeit vermieden werden, da für das ZVR der Grad der Verwandtschaft unerheblich ist (BeckOK StPO, 56. Auflage, § 52 Rn. 8).

Die von meiner Prüfung direkt betroffenen Bußgeldbehörden haben bis zum Redaktionsschluss meine Hinweise größtenteils umgesetzt. Da, wie bereits erwähnt, die das Tool anbietende Firma für eine Vielzahl von sächsischen Bußgeldbehörden tätig ist, wandte ich mich zusätzlich an das Sächsische Staatsministerium des Innern (SMI) als Aufsichtsbehörde und bat darum, alle sächsischen Bußgeldbehörden auf die datenschutzrechtlichen Probleme hinzuweisen und mir die entsprechende Umsetzung zu bestätigen. Das SMI teilte mit, dass die Landesdirektion Sachsen (LDS) um Prüfung des Sachverhaltes gebeten wurde. Die LDS hat daraufhin die sächsischen Kommunen, welche gemäß Ordnungswidrigkeiten-Zuständigkeitsverordnung (OWi-ZustV) für die Verfolgung und Ahndung von Verkehrsordnungswidrigkeiten zuständig sind, um zeitnahe Überprüfung der eigenen Verfahrensweise und, soweit erforderlich, um Überarbeitung nach unseren Maßgaben sowie um Rückmeldung zur Umsetzung aufgefordert.

Was ist zu tun?
Eine Onlineanhörung – als lediglich weitere Möglichkeit für die betroffenen Personen, ihren Anspruch auf rechtliches Gehör wahrzunehmen – muss zwingend die gesetzlichen Vorgaben umsetzen und insofern inhaltsgleich zum korrekten schriftlichen Verfahren ausgestaltet sein.

2.2.12 Fahrerermittlung im Bußgeldverfahren durch Recherche in sozialen Medien

↗ § 46 Abs. 1 und 2 OWiG in Verbindung mit § 161 Abs. 1 StPO

Im Berichtszeitraum wandte sich ein besorgter Petent und Fahrzeughalter mit dem Vortrag an mich, dass eine sächsische Bußgeldbehörde im Rahmen der Fahrerermittlung in einem Verkehrsordnungswidrigkeitenverfahren unberechtigt auf sein Facebook-Konto zugegriffen habe. Die Behörde hätte die Fahrerin seines Pkw über die sozialen Medien ermittelt. Der Petent sei ausschließlich über Facebook in den sozialen Medien vertreten. Dieser Account sei allerdings auf „privat" eingestellt, sodass Außenstehende keinen Zugriff hätten.

Die von mir um Stellungnahme gebetene Bußgeldbehörde bestätigte den Sachverhalt dahingehend, dass dem Petenten als Fahrzeughalter ein Zeugenfragebogen übersandt worden sei, in welchem er darauf hingewiesen worden sei, dass er durch Angaben zur Fahrzeugführerin weitere Ermittlungen vermeiden könne. Mangels Rückmeldung des Petenten habe die zuständige Sachbearbeiterin ein Fahrerermittlungsersuchen an den internen Ermittlungsdienst des zuständigen Landratsamtes verfügt, durch welchen die später Betroffene im Verkehrsordnungswidrigkeitenverfahren als verantwortliche Fahrzeugführerin ermittelt und deren Angaben der Bußgeldstelle entsprechend übermittelt worden seien. Der Ermittlungsdienst gab an, man habe unter Zuhilfenahme sozialer Medien ermittelt. Bei „Google" habe der Bearbeiter den Namen des Petenten eingegeben, woraufhin ein vorhandener Account bei Facebook angezeigt worden sei. Jedem zugänglich seien dort Fotos des Petenten und sogenannte Likes zu Bildern eingestellt. Über diese Likes sei der Bearbeiter an ein für jeden Nutzer zugängliches Facebook-Profil gelangt, in dem Fotos sichtbar gewesen seien, die mit den vorhandenen Fotos der Bußgeldstelle abgeglichen worden seien, wodurch die Fahrzeugführerin habe ermittelt werden können.

Aus datenschutzrechtlicher Sicht ist das Vorgehen des Ermittlungsdienstes sowie der Bußbehörde nicht zu beanstanden. Die Bußgeldstelle sandte dem Petenten nach einem negativen Plausibilitätsabgleich – der Abgleich des bei dem Verstoß gefertigten Lichtbildes mit den Angaben aus der Halterabfrage ergab, dass er offenkundig nicht als Fahrzeugführer zum Tatzeitpunkt in Betracht kam – vorschriftsmäßig einen Zeugenfragebogen zu mit dem Hinweis, dass weitere Ermittlungshandlungen zulässig sind.

Sofern der Halter nicht reagiert, keine Angaben zu der Person des Fahrers macht oder von seinem Zeugnisverweigerungsrecht oder Auskunftsverweigerungsrecht gemäß §§ 52 bis 55 Strafprozessordnung (StPO) Gebrauch macht und die gegebenenfalls bestehende Möglichkeit, im Verwarnungsgeldverfahren das Verwarnungsgeld zu zahlen, ungenutzt verstrichen ist, können weitere Ermittlungen zur Person des

Fahrzeugführers stattfinden. Hierbei ist den Behörden eine Kenntnisnahme öffentlich zugänglicher Informationen – auch aus sozialen Netzwerken – grundsätzlich nicht verwehrt. Soweit die Behörden nicht, gegebenenfalls unter Verwendung einer falschen Identität, in abgeschlossenen Chatgruppen agieren oder sonstige Schutzvorkehrungen überwinden, ist eine Recherche auf jedermann zugänglichen Websites oder in sozialen Medien auf Grundlage der allgemeinen Ermittlungsbefugnis zulässig. Auch, wenn im vorliegenden Fall das Facebook-Konto des Petenten auf „Privat" gestellt war, waren noch immer Fotos des Petenten und die jeweils dazugehörigen „Likes" für jeden sichtbar. Laut des Ermittlungsdienstes konnte anhand dieser Informationen die Fahrzeugführerin ermittelt werden. Dieser geringfügige Eingriff in das Recht des Petenten auf informationelle Selbstbestimmung war gemäß § 46 Abs. 1 und 2 Gesetz über Ordnungswidrigkeiten (OWiG) in Verbindung mit § 161 Abs. 1 StPO zulässig. Danach ist die für das Bußgeldverfahren zuständige Verwaltungsbehörde zur Erforschung des Sachverhalts befugt, Ermittlungen jeder Art vorzunehmen, soweit nicht andere gesetzliche Vorschriften ihre Befugnisse besonders regeln. Letzteres war vorliegend nicht der Fall.

Was ist zu tun?
Für die Ermittlung einer Fahrzeugführerin oder eines Fahrzeugführers im Rahmen eines Bußgeldverfahrens darf die Behörde auf Grundlage der allgemeinen Ermittlungsbefugnis auf jeder Person zugänglichen Websites oder auf öffentlich zugänglichen Seiten in sozialen Medien recherchieren und entsprechende Erkenntnisse verwerten.

2.2.13 Darf das Ordnungsamt Fahrzeughalterdaten ermitteln und an einen Supermarktbetreiber herausgeben?

↗ § 39 Abs. 1 StVG

Eine sächsische Gemeinde bat um datenschutzrechtliche Beratung zu folgendem Sachverhalt: Der Betreiber eines örtlichen Supermarktes und zugleich Eigentümer des betreffenden Grundstücks wandte sich an das Ordnungsamt der Gemeinde und bat um die Herausgabe der Daten eines Fahrzeughalters, dessen Pkw seit mehreren Monaten auf dem Parkplatz des Supermarktes abgestellt war, um diesen aufzufordern, dass Fahrzeug zu entfernen. Die Gemeinde war unsicher, ob das Ordnungsamt die Fahrzeughalterdaten zu diesem Zweck erheben und weitergeben darf.

Öffentliche Stellen dürfen ausschließlich aufgrund einer Rechtsgrundlage personenbezogene Daten erheben und an Dritte übermitteln, da es sich um einen Grundrechtseingriff handelt. Zunächst muss somit geprüft werden, ob der der Anfrage zugrunde liegende Sachverhalt – hier das dauerhafte Abstellen eines Pkw auf einem privaten Supermarktparkplatz – den Aufgabenbereich der Gemeinde berührt und eine gesetzliche Grundlage für die erbetene Datenverarbeitung existiert. Dafür gab es vorliegend keine Anhaltspunkte, da weder verkehrsrechtlich noch gefahrenabwehrrechtlich ein Verstoß des Fahrzeughalters bzw. eine öffentliche Gefahrenlage durch den Pkw zu erkennen waren, die ein gemeindebehördliches Einschreiten erfordert hätten. Es gab folglich bereits für ein Ermitteln der Halterdaten durch die Gemeinde weder eine aus der gesetzlichen Aufgabenerfüllung resultierende Erforderlichkeit noch eine Rechtsgrundlage; erst recht galt das für eine Übermittlung dieser personenbezogenen Daten an Dritte.

Der Eigentümer des Parkplatzgeländes ist in derartigen Fällen darauf zu verweisen, die Auskunft zum Halter bei der örtlichen Zulassungsbehörde oder beim Kraftfahrtbundesamt einzuholen. Dies ist rechtlich zulässig, Rechtsgrundlage wäre § 39 Abs. 1 Straßenverkehrsgesetz (StVG). Die genannten Stellen verfügen aufgrund ihrer gesetzlichen Aufgaben über Fahrzeughalterdaten und erteilen Auskunft, wenn Daten zur Geltendmachung, Sicherung oder Vollstreckung oder zur Befriedigung oder Abwehr von Rechtsansprüchen im Zusammenhang mit der Teilnahme am Straßenverkehr oder zur Erhebung einer Privatklage wegen im Straßenverkehr begangener Verstöße benötigt werden.

Sollte die öffentliche Stelle bereits aufgrund eigener Aufgabenerfüllung vor dem Auskunftsersuchen von Dritten Fahrzeughalterdaten verarbeitet haben, richtete sich die Zulässigkeit einer Übermittlung entweder nach § 49b Ordnungswidrigkeitengesetz (OWiG) in Verbindung mit § 475 Abs. 4 Strafprozessordnung (StPO), wenn die Erhebung der Fahrzeughalterdaten im Rahmen eines Ordnungswidrigkeitenverfahrens (zum Beispiel Ahndung einer Verkehrsord-

Was ist zu beachten?
Die Gemeinde darf selbst bei einem berechtigten Interesse Anfragender keine personenbezogenen Daten übermitteln, die für ihre eigene Aufgabenerfüllung nicht erforderlich sind und die sie allein zum Zweck der Auskunft zunächst bei einer dritten Stelle erheben müsste.

nungswidrigkeit) erfolgte, oder gemäß § 4 Abs. 1 Sächsisches Datenschutzdurchführungsgesetz (SächsDSDG), wenn die Gemeinde in einem Gefahrenabwehrvorgang gegen den Fahrzeughalter tätig geworden ist. Eine solche Konstellation lag hier allerdings nicht vor.

2.2.14 Kontenabrufverfahren nach der Abgabenordnung

↗ § 93 Abs. 8 AO, § 93 Abs. 1 und 2 AO, § 93b Abs. 2 AO, § 60 Abs. 1 SGB I

Mit einer Beschwerde rügte ein Petent, dass das Jobcenter eines Landratsamtes für ihn und seine Ehefrau ein Kontoabrufverfahren beim Bundeszentralamt für Steuern (BZSt) durchgeführt hatte. Dabei wurde das Kontoabrufverfahren nicht nur für ihn und seine Ehefrau, sondern auch für sein Kind, seine Mutter und die Eltern seiner Ehefrau durchgeführt. Die Kontenabfrage war aus seiner Sicht unberechtigt. Ich habe dazu folgende Auffassung vertreten:
Das BZSt darf nach § 93b Abs. 2 Abgabenordnung (AO) in den Fällen des § 93 Abs. 7 und 8 AO auf Ersuchen bei den Kreditinstituten einzelne Daten im automatisierten Verfahren abrufen und sie an den Ersuchenden übermitteln. Ob die Voraussetzung des Kontenabrufverfahrens vorlagen, war im Rahmen der Beschwerde des Petenten zu prüfen.

a) Das Jobcenter ist die zuständige Behörde für die Verwaltung der Grundsicherung für Arbeitssuchende nach dem Zweiten Buch Sozialgesetzbuch. Es kann daher nach § 93 Abs. 8 Nr. 1 a AO ein Ersuchen auf Auskunft über die in § 93b Abs. 1 und 1a bezeichneten Daten beim BZSt stellen.
b) Das Jobcenter konnte darlegen, dass ein vorheriges Auskunftsersuchen an die betroffenen Eheleute keine Aussicht auf Erfolg gehabt hätte. Es hatte nachvollziehbar belegt, dass es die Ehefrau als Antragstellerin und auch den Petenten im Rahmen des Antragsverfahrens auf Grundsicherung mehrmals aufgefordert hat, Nachweise zu den Einkommensverhältnissen vorzulegen. Die Nachweise sind für beide vorzulegen,

da sie als Eheleute in Bedarfsgemeinschaft leben. Dies erfolgte nach mehrmaliger Aufforderung durch das Jobcenter jedoch nur für die Antragstellerin.

c) Vor einem Abrufersuchen nach § 93 Abs. 8 AO ist die betroffene Person auf die Möglichkeit des Kontenabrufs hinzuweisen; dies kann auch durch ausdrücklichen Hinweis in amtlichen Vordrucken und Merkblättern geschehen. Nach Durchführung eines Kontenabrufs ist die betroffene Person vom Ersuchen über die Durchführung zu benachrichtigen, § 93 Abs. 9 AO.
Das Jobcenter hatte die Eheleute darauf hingewiesen, dass ein Abrufverfahren beim BZSt durchgeführt werden kann. Damit erfolgte vor dem Abrufverfahren nach § 93 Abs. 8 AO der ausdrückliche Hinweis auf die Möglichkeit des Kontenabrufs. Auch die Benachrichtigung über die Durchführung ist durch das Jobcenter erfolgt.

d) Beim Kontenabrufverfahren werden vom BZSt der Vor- und Nachname des Kontoinhabers sowie dessen Anschrift und Geburtsdatum angegeben, vergleiche § 93b Abs. 1 und 1a AO in Verbindung mit § 24c Abs. 1 Kreditwesengesetz. Anzugeben sind ebenfalls diese Daten zu Verfügungsberechtigten für das jeweilige Konto, zu dem diese Befugnis besteht. Keine Auskunft darf über Kontostände erteilt werden.
In der Kontenabfrage wurden daher nicht nur die eigenen Konten des Ehepaars, sondern auch die Konten angegeben, zu denen den beiden eine Verfügungsberechtigung zusteht. Dies gilt auch für Konten der Eltern und des Kindes, die zwar nicht unter dem Namen des Petenten oder seiner Ehefrau laufen, zu welchen beide aber eine Verfügungsbefugnis besitzen. Der Umfang der abgerufenen Daten war rechtmäßig.

e) Das Jobcenter legte mir gegenüber plausibel dar, dass die Kontenabrufe geeignet, erforderlich und auch verhältnismäßig waren, um das Antragsverfahren mit angemessenem Aufwand abzuschließen.

Auch das Übermaßverbot ist nicht verletzt. Wer aus Steuermitteln finanzierte öffentliche Leistungen ohne eigenes Leistungsäquivalent begehrt, aber zumutbaren Mitwirkungspflichten nicht nachkommt, muss Eingriffe in das Recht auf informationelle Selbstbestimmung hinnehmen, die durch überwiegendes Allgemeininteresse gerechtfertigt sind (so Landessozialgericht Baden-Württemberg, Urteil vom 22.03.2018, L 7 AS 2969/17). Da mittels der Kontenabrufverfahren lediglich Rahmendaten (Kontonummern und Verfügungsberechtigungen) abgerufen werden können, sind die sensiblen Daten, die sich aus den konkreten Verfügungsaufträgen ergeben, weiterhin geschützt.

Beim Kontenabrufverfahren können weder der Kontostand noch konkrete Kontobewegungen seitens der Sozialleistungsbehörde ermittelt werden; insoweit verbleibt es bei der Mitwirkungspflicht der Antragstellerin und des Petenten, da beide eine Bedarfsgemeinschaft bilden. Die Mitwirkungspflicht beinhaltet auch die Vorlage von Kontoauszügen durch das Ehepaar.

Was ist zu tun?
Ein Sozialleistungsträger ist befugt, ein Kontenabrufverfahren durchführen zu lassen, wenn hierfür die Voraussetzungen nach der Abgabenordnung vorliegen.

Zu den nunmehr bekannten Konten des Ehepaars sind nun im Rahmen ihrer Mitwirkungspflichten nach § 60 SGB I durch Kontoauszüge die relevanten Kontobewegungen offenzulegen.

2.2.15 Veröffentlichung von Niederschriften von Ratssitzungen durch Gemeinden und Landkreise

↗ Art. 28 Abs. 2 GG, § 36 b Satz 1 und 2 SächsGemO/
§ 32 b Satz 1 und 2 SächsLKrO, § 40 Abs. 2 Satz 5 SächsGemO/
§ 36 Abs. 2 Satz 5 SächsLKrO

Es erreichten mich mehrere Anfragen zu gemeindlichen Veröffentlichungspflichten – ob im Internet auf der Homepage, dem Bürgerinformationssystem oder klassisch im Amtsblatt, das zumeist ebenfalls ins Internet eingestellt wird.

Insbesondere kam mehrfach die Frage auf, ob die Gemeinden verpflichtet seien, auch Niederschriften von Ratssitzungen zu veröffentlichen, und aus welchen Gründen bei Gemein-

den unterschiedliche Handhabungen vorliegen. Dasselbe gilt im Übrigen auch für die sächsischen Landkreise in Anwendung der Sächsischen Landkreisordnung (SächsLKrO), die zur Sächsischen Gemeindeordnung fast wortgleich ist.

Ich musste die Anfragenden hier zunächst auf meine Stellung als datenschutzrechtliche Aufsichtsbehörde verweisen. Als solche steht es mir nicht zu, die Art und Weise gemeindlicher Aufgabenerfüllung zu bewerten, insbesondere im Lichte des verfassungsrechtlich garantierten Selbstverwaltungsrechts der Kommunen nach Art. 28 Abs. 2 Grundgesetz. Was ich in meiner aufsichtlichen Tätigkeit prüfe und bewerte sind vielmehr allein die datenschutzrechtlichen Befugnisse. Hält die Gemeinde diese ein, kann und darf ich hierzu keine weiteren Vorgaben machen.

Eine gesetzliche Verpflichtung für Kommunen, vollständige Niederschriften von Ratssitzungen zu veröffentlichen, gibt es nicht: Diese können (bei entsprechender Wahrung des Datenschutzes), müssen aber nicht veröffentlicht werden.

Welche Daten und Unterlagen veröffentlicht werden müssen, ergibt sich vielmehr abschließend aus § 36b Satz 1 und 2 SächsGemO bzw. § 32b Satz 1 und 2 SächsLKrO: Das sind Zeit, Ort und Tagesordnung der öffentlichen Sitzungen samt Beratungsunterlagen und die in öffentlicher Sitzung gefassten Beschlüsse.

Wesentlich dabei ist, dass personenbezogene Daten oder Betriebs- und Geschäftsgeheimnisse nicht offenbart werden dürfen, § 36b Satz 3 SächsGemO/§ 32b Satz 3 SächsLKrO.

Zudem kann die Gemeinde bei den zur Veröffentlichung vorgeschriebenen Beratungsunterlagen dennoch von einer Veröffentlichung absehen, wenn Maßnahmen zur Wahrung des Datenschutzes oder von Betriebs- und Geschäftsgeheimnissen nicht ohne erheblichen Aufwand oder erhebliche Veränderung einer Beratungsunterlage möglich sind, § 36b Satz 3 SächsGemO/§ 32b Satz 3 SächsLKrO. Beschlüsse sind allerdings in jedem Fall zu veröffentlichen.

Für Niederschriften gilt dagegen § 40 Abs. 2 Satz 5 Sächs GemO/§ 36 Abs. 2 Satz 5 SächsLKrO: Demnach muss den Einwohnerinnen und Einwohnern die Einsichtnahme in die

Niederschriften über die öffentlichen Sitzungen gestattet sein, darüber hinaus kann die Gemeinde/der Landkreis auch die allgemeine Einsichtnahme in elektronischer Form (elektronische Veröffentlichung) ermöglichen. Dies kann indes in entsprechender Anwendung des § 36b Satz 3 SächsGemO/ § 32b Satz 3 SächsLKrO nur nach Bereinigung (Löschung/ Schwärzung etc.) der personenbezogenen Daten erfolgen. Die klassische Vor-Ort-Einsicht bedarf der Bereinigung dagegen nicht.

Bei der Veröffentlichung von Niederschriften handelt es sich nach alledem nicht um die Umsetzung einer gesetzlichen Verpflichtung, sondern um die Anwendung des Transparenzgedankens, damit Entscheidungen des Rates besser für die Bürgerschaft nachvollzogen werden können. Einen Anspruch auf deren Veröffentlichung gibt es für Bürgerinnen und Bürger aber nicht.

Das Sächsische Transparenzgesetz kommt übrigens hier nicht zur Geltung. Dieses findet auf kommunaler Ebene nur Anwendung, wenn die betreffende Gemeinde/der Landkreis sich per Satzung zu dessen Umsetzung verpflichtet hat. Dies ist mir zumindest derzeit für keine sächsische Gemeinde/ keinen Landkreis bekannt.

Zu diesem Themenkreis verweise ich zusätzlich auf Beiträge in meinen Tätigkeitsberichten Datenschutz 2022 (2.2.2., Seite 39 ff.) und Datenschutz 2023 (1.5, Seite 36 ff.).

Tätigkeitsbericht Datenschutz 2022:
↗ sdb.de/tb2022

Tätigkeitsbericht Datenschutz 2023:
↗ sdb.de/tb2023

Was ist zu beachten?
Gemeinden und Landkreise müssen rigoros darauf achten, in Veröffentlichung der Ratsunterlagen keine personenbezogenen Daten zu offenbaren.

2.2.16 Recherchen im Sinne des § 4 Waffengesetz

↗ §§ 4, 5, 6 WaffG; Art. 6 DSGVO

Der Bundesgesetzgeber hat am 25. Oktober 2024 das „Gesetz zur Verbesserung der inneren Sicherheit und des Asylsystems" beschlossen. Artikel 5 dieses Gesetzes beinhaltet eine Änderung des Waffengesetzes. In diesem Zusammenhang wurde in § 4 der Absatz 6 neu eingefügt. Demnach ist die zuständige Behörde befugt, in öffentlich zugänglichen Quellen zu recherchieren und diese Erkenntnisse in die Prüfung nach §§ 5 und 6 Waffengesetz (WaffG) einfließen zu lassen.

Diese Ermächtigung führt bei den Anwendenden in den Behörden zu Verunsicherung, da der unbestimmte Rechtsbegriff „öffentlich zugängliche Quellen" in der Rechtsprechung einem steten Wandel unterliegt. Dies ist insbesondere den immer weiter entwickelten technischen Möglichkeiten geschuldet. Dabei ist besonders unklar, ob von dieser Ermittlungsmöglichkeit das Internet und auch soziale Medien mitumfasst sind.

Vorausstellend möchte ich darauf hinweisen, dass eine verborgene Ermittlung, das heißt, mit einem Account, der die ermittelnde Behörde nicht erkennen lässt, auf keinen Fall von der Norm umfasst ist. Ebenso wenig ist die Recherche mittels privater Accounts der Angestellten, auf Profilen mit der Einstellung „privat" (zum Beispiel durch Versenden einer Freundschaftsanfrage) oder in privaten Foren unter Vorspiegelung von aktiver Gesprächsteilnahme umfasst. In diesen Fällen sind eindeutigere, deutlichere und weitgreifendere Ermächtigungsnormen erforderlich.

Eine Recherche im Internet mittels einer Suchmaschine ist dagegen unbedenklich. Auch öffentliche Websites, die die betroffene Person betreibt und mit denen eine Außenwirkung bezweckt wird, sind umfasst.

Hinsichtlich der Ermittlung auf sozialen Plattformen und Netzwerken ist jedoch Vorsicht geboten. Von der Regelung sind nur öffentlich zugängliche Quellen, das heißt der Allgemeinheit zugängliche Quellen, umfasst. Die reine Anmeldung auf einer Plattform oder einem Netzwerk steht der Öffentlichkeit des Zugangs nicht entgegen. Dies gilt aber nur dann, wenn die Anmeldung für alle Personen möglich ist, keine weiteren Hürden bestehen als die Angabe von Grunddaten und keine gesonderte Zugangsprüfung erfolgt. Alles, was darüber hinausgeht, ist nicht öffentlich. Insbesondere wenn der Zutritt nicht automatisch erfolgt oder eine Zugangsfrage beantwortet werden muss, ist das Netzwerk oder die Plattform nicht mehr öffentlich.

Auch dann sind jedoch nur die Profile öffentlich, welche eine entsprechende Einstellung verwendet haben. Die meisten Plattformen oder Netzwerke haben inzwischen die Möglich-

keit für ihre Nutzer/innen eingeräumt, dass diese die Profile entweder privat oder öffentlich ausgestalten können. Private Accounts dürfen nicht durch weitere Schritte wie Freundschaftsanfragen oder Ähnliches erschlossen werden.
Eine weitere datenschutzrechtliche Einschränkung folgt daraus, dass die Recherche auf das für den Zweck erforderliche Maß reduziert ist. Problematisch sind in diesem Zusammenhang sogenannte überschießende Informationen, insbesondere von Dritten, welche ganz erheblich mitbetroffen sein können und für deren Verarbeitung keinerlei Rechtsgrundlage besteht. Es sollte grundsätzlich die Direkterhebung bevorzugt werden, da dies den geringsten Eingriff in die Rechte der Betroffenen darstellt. Das Internet und insbesondere soziale Netzwerke ermöglichen es mit relativ geringem Aufwand, viel über den Charakter, die Interessen, Tätigkeiten und Ansichten der betroffenen Person zu erfahren. Derartige Informationen sagen viel über die Persönlichkeitsstruktur aus. Ein entsprechend großer Eingriff in das Recht auf informationelle Selbstbestimmung stellt daher eine Recherche direkt in diesen Medien dar. Der Eingriff muss daher so gering wie möglich gehalten werden, auch für im Zweifel unbeteiligte Dritte.
Diese Erwägungen sind in jedem Einzelfall bereits vor Beginn der Recherche abzuwägen und müssen auch dauerhaft während der Recherche weiter abgewogen werden. Eine standardmäßige Abfrage, wie dies insbesondere durch § 5 Abs. 5 WaffG oder § 6 Abs. 2 und 3 WaffG festgeschrieben ist, wurde in § 4 Abs. 6 WaffG ausdrücklich nicht geregelt. Soweit also mildere Mittel ersichtlich sind oder die Informationen aufgrund der Regelungen in §§ 5 und 6 WaffG bereits vorliegen, ist eine Erforderlichkeit der Recherchen nicht mehr gegeben und die Datenerhebung folglich unrechtmäßig.

Was ist zu tun?
Für die Behörden ist die Recherche in sozialen Medien und Plattformen Ultima Ratio. Zuvor sind alle milderen Mittel zum Erkenntnisgewinn auszuschöpfen. Insbesondere handelt es sich nicht um eine standardisierte Abfrage, wie es andere Regelungen des WaffG vorsehen.

2.2.17 Auskunftserteilung durch Behörden nach § 161 Strafprozessordnung

↗ § 3 SächsDSDG, § 161 StPO, Art. 6 DSGVO

Durch eine Behörde wurde mir ein Auskunftsersuchen zur Prüfung vorgelegt. Darin wurde die Behörde aufgefordert,

Informationen über eine betroffene Person gegenüber dem Aussteller offenzulegen. Zur Begründung dieses Ersuchens wurde auf § 161 Abs. 1 Strafprozessordnung (StPO) verwiesen. Grundsätzlich regelt diese Norm die Ermittlungsbefugnisse der Staatsanwaltschaft. Über verschiedene Verweise können jedoch auch andere Behörden aufgrund dieser Norm Auskünfte erhalten, zum Beispiel die Familienkasse oder Finanzbehörden.

Das Problem an diesem Auskunftsersuchen war jedoch, dass die angeforderten Daten von der Behörde gar nicht vorgehalten und auch nicht verarbeitet werden. Rein tatsächlich hätte die Behörde die Daten zwar durch eine Abfrage erheben können, eine Rechtsgrundlage hierfür besteht jedoch nicht. Gemäß § 3 Abs. 1 Sächsisches Datenschutzdurchführungsgesetz (SächsDSDG) ist die Verarbeitung personenbezogener Daten durch öffentliche Stellen nur zulässig, wenn sie zur Erfüllung der in der Zuständigkeit des Verantwortlichen liegenden Aufgabe oder in Ausübung öffentlicher Gewalt, die dem Verantwortlichen übertragen wurde, erforderlich ist. Beides lag hier nicht vor. Die rechtsgrundlose Erhebung und Verarbeitung von Daten verstößt dabei gegen § 3 SächsDSDG und Art. 6 DSGVO.

Auch § 161 Abs. 1 StPO begründet in diesem Zusammenhang keine neue Rechtsgrundlage für die Erhebung und Verarbeitung von Daten. Die Vorschrift berechtigt ausschließlich zur Offenlegung der Daten, welche bereits bei der angefragten Behörde vorliegen und aufgrund einer eigenen Rechtsgrundlage der Behörde dort auch vorliegen dürfen.

Ich habe die Behörde hierauf hingewiesen und ihr geraten, dem Aussteller mitzuteilen, dass Sie die angeforderten Daten nicht in ihrem Aufgabenbereich verarbeitet. Zusätzlich konnte ergänzt werden, welche Behörde die Daten tatsächlich rechtmäßig verarbeitet, sodass ein neues Auskunftsersuchen gegenüber dem richtigen Empfänger erstellt werden konnte.

Was ist zu tun?

Durch die Behörde, welche das Auskunftsersuchen erhält, ist zu prüfen, ob die von der Auskunft begehrten Daten tatsächlich von ihr genutzt und verarbeitet werden. Sollte dies nicht der Fall sein, ist dies als Auskunft mitzuteilen. § 161 StPO ersetzt keine Rechtsgrundlage für die Erhebung von Daten.

2.2.18 Erforderlichkeit von Datenverarbeitungen bei einem Arbeitszeiterfassungsverfahren

↗ Art. 58 Abs. 2 Buchst. f DSGVO; Art. 5 Abs. 1 Buchst. a und c DSGVO; § 11 SächsDSDG; § 5 Abs. 3 Satz 4 SächsAZVO; § 81 Abs. 2 Nr. 12 PersVG

Im vergangenen Berichtszeitraum hat meine Behörde die Anfrage zum datenschutzkonformen Einsatz der Funktion „Anwesenheitsübersicht" eines elektronischen Zeiterfassungssystems in einem Finanzamt erreicht. Die Funktion „Anwesenheitsübersicht" ermöglicht – je nach Einstellung – den Zugriff zu den aktuellen Statusdaten sämtlicher oder auch einzelner Beschäftigter bei dem Verantwortlichen. Im Bereich der Finanzämter war die Funktion zunächst so ausgestaltet, dass jede/r Beschäftigte bei jeder/jedem anderen Beschäftigten eines Finanzamtes den Status einsehen konnte. Die Statusdaten umfassten zu Beginn die Angaben „anwesend", „Telearbeit/mobiles Arbeiten", „Dienstgang/Dienstreise", „abwesend" (mit hinterlegter Fehlzeit für geplante Abwesenheit, zum Beispiel Urlaub), „abwesend" (ohne hinterlegte Fehlzeit für ungeplante Abwesenheit, zum Beispiel Pause, Kind krank) und entstammten dem Zeiterfassungssystem. Zum Einsatz dieser Funktion, insbesondere den Zugriffsberechtigungen und den angezeigten Statusdaten der Beschäftigten, gab es einen fast einjährigen andauernden Austausch mit den Verantwortlichen und der für Fach- und Dienstaufsicht zuständigen oberen Staatsbehörde (Landesamt für Steuern und Finanzen). Zwar wurden teilweise die Zugriffsberechtigungen und auch die Anzahl der Statusdaten reduziert, dennoch musste meine Behörde Anordnungen zu (weiteren) Beschränkung von Zugriffsberechtigungen nach Art. 58 Abs. 2 Buchst. f DSGVO gegenüber den 24 Finanzämtern erlassen, da trotz fehlender Erforderlichkeit einzelnen Beschäftigten bzw. Beschäftigtengruppen weiterhin Zugriffsberechtigungen eingeräumt wurden bzw. an diesen festgehalten wurde.

Der Verantwortliche konnte sich mangels Erforderlichkeit der Zugriffsberechtigungen für einzelne Beschäftigte bzw. Beschäftigtengruppen insbesondere nicht auf die Rechtsgrundlage § 11 Abs. 1 Satz 1 Sächsisches Datenschutzdurchführungsgesetz (SächsDSDG) berufen. Das Erforderlichkeitsprinzip ergänzt und sichert das grundsätzliche Verbot einer Datenverarbeitung mit Erlaubnisvorbehalt ab (vgl. Buchner/Petri in Kühling/Buchner DS-GVO Art. 6 Rn. 5). Das bedeutet, dass eine Datenverarbeitung im Rahmen des jeweiligen Erlaubnistatbestandes nur dann zulässig ist, wenn diese auch erforderlich ist. Erforderlichkeit bedeutet, dass die vom Dienstherrn gewählte Art und Weise der Datenverarbeitung für die Verwirklichung der verfolgten Zwecke überhaupt geeignet ist, das mildeste aller gleich effektiven zur Verfügung stehenden Mittel darstellt (vgl. EG 39 S. 9 zur DSGVO) und die Schwere des mit der Datenverarbeitung bewirkten Eingriffs in das Persönlichkeitsrecht des/der Beschäftigten bei einer Gesamtabwägung nicht außer Verhältnis zu dem Gewicht der ihn rechtfertigenden Gründe steht. Zulässig ist eine Datenverarbeitung also nicht schon dann, wenn diese in Bezug auf den beabsichtigten Zweck irgendwie dienlich oder förderlich ist. Im Rahmen dieser Prüfung ist auch Art. 5 Abs. 1 Buchst. c DSGVO als ein Aspekt der Erforderlichkeit zu berücksichtigen, vgl. Urteil des EuGH vom 9. Januar 2025, Rn. 24, 28 (C-394/23). Danach müssen personenbezogene Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung"). Der Grundsatz der Datenminimierung verlangt in Bezug auf den Umfang der Daten eine möglichst weitgehende Verringerung der Anzahl der verarbeiteten Daten sowie ihrer Nutzungen, zudem eine Einschränkung der Anzahl der Betroffenen und der zugriffsberechtigten Personen.

Der Verantwortliche teilte mit, dass Zweck der Datenverarbeitung die **Personaleinsatzplanung** sei. Allerdings zeigt die Funktion „Anwesenheitsübersicht" nur an, ob sich der Beschäftigte im Moment des Aufrufs der Daten eingeloggt hat, im Dienst befindet (anwesend, abwesend) und wo er den Dienst ausübt (mobiles Arbeiten/Telearbeit, Dienstreise). Es

erschließt sich nicht, inwieweit die Information zum aktuellen An- und Abwesenheitsstatus und zur Angabe des Arbeitsortes, das heißt, einer Momentaufnahme überhaupt für eine Personaleinsatzplanung, geeignet sein soll. Insbesondere enthält die „Anwesenheitsübersicht" keine Angaben darüber, ob der/die Beschäftigte an diesem Tag überhaupt den Dienst aufnimmt, zum Beispiel aufgrund Urlaub oder Krankheit. Diese Angaben sind wiederum in bei dem Verantwortlichen geführten Dienstplänen bzw. -kalendern vorhanden, insbesondere auch zur Planung und Absicherung von sogenannte Funktionszeiten, in denen grundsätzlich die Arbeitsfähigkeit, Auskunftsfähigkeit und Arbeitsbereitschaft durch eine angemessene Besetzungsdichte in den jeweiligen Organisationseinheiten sicherzustellen ist. Diesen Widerspruch konnte der Verantwortliche nicht auflösen. Im Ergebnis war festzustellen, dass der vom Verantwortlichen angegebene Zweck der Personaleinsatzplanung mit den Informationen aus der Anwesenheitsübersicht (aktuelle Statusdaten) überhaupt nicht erreicht werden kann bzw. diese für den Zweck objektiv schon nicht geeignet sind. Allgemeine und pauschale Aussagen, dass dies für die Personaleinsatzplanung vor dem Hintergrund des orts- und arbeitszeitflexiblen Arbeitens sowie einer Vielzahl von Arbeitszeitmodellen, die nicht in Planungsszenarien gefasst werden könnten, zwingend erforderlich sei, genügen den Anforderungen an eine datenschutzrechtliche Erforderlichkeit jedenfalls nicht.

Der Verantwortliche gab als (weiteren) Zweck der Datenverarbeitung die **Organisation der Arbeitsabläufe** zur Sicherstellung der Personalplanung sowie des Personaleinsatzes an. Mit Ausnahme der Bereiche Telefonzentrale sowie der Informations- und Annahmestelle konnte eine Erforderlichkeit der Zugriffsberechtigungen zu dem vorgenannten Zweck durch den Verantwortlichen jedoch ebenfalls nicht begründet werden. Der Verantwortliche trug zwar umfangreich vor und beschrieb dabei eine Vielzahl von Anwendungsfällen und Prozessen, diese ließen jedoch teilweise Zweifel aufkommen, ob sich derartige Prozesse mit der Lebenswirklichkeit bzw. üblichen Verwaltungspraxis in Einklang bringen lassen.

So führte der Verantwortliche beispielsweise an, dass die „Anwesenheitsübersicht" zur Ausübung der Fürsorgepflicht diene. Nach Verständnis des Verantwortlichen erfordere diese Aufgabe, dass sich der Vorgesetzte regelmäßig ein lebendiges Bild, also einen höchstpersönlichen Eindruck von Beschäftigten in ihrem konkreten Arbeitsumfeld, verschaffe, was einen persönlichen, in der Regel auch spontanen Kontakt am individuellen Arbeitsplatz erforderlich mache. Möchte die Amtsleitung als Vorgesetzte/r nicht nur fachliche Angelegenheiten gegenüber dem Beschäftigten ansprechen, sondern auch die persönliche Situation der Beschäftigten (Arbeitsorganisation, Belastungssituation, individuelle Verfassung/persönlicher Gesamteindruck) feststellen, erfragen und erörtern, wäre die Amtsleitung – auch aus datenschutzrechtlichen Gründen – darauf angewiesen, den Beschäftigten allein und zumeist unangekündigt im Dienstzimmer anzutreffen. Dies könne die Amtsleitung jedoch ausschließlich über eine vorherige Einsicht in die „Anwesenheitsübersicht" sicherstellen. Nach Auffassung des Verantwortlichen könne dagegen ein telefonischer Kontakt, ein angekündigtes/terminlich abgestimmtes Aufsuchen des oder der Bediensteten in seinem Zimmer oder ein spontaner Besprechungstermin im Zimmer des bzw. der Vorgesetzten diesen persönlichen Eindruck nicht vermitteln. Dieser Zweck wirkte für meine Behörde etwas konstruiert, denn nichts hindert den Amtsleiter oder die Amtsleiterin daran, durch die Büroräume zu gehen und die Beschäftigten, die er bzw. sie allein antrifft, nach deren Befinden oder „Lebensrealität" zu befragen. Dies stellt zum einen eine weitaus datensparsamere Alternative dar, zum anderen war diesen Ausführungen auch keine Systematik in Bezug auf Auswahl der Beschäftigten, die spontan befragt werden sollen zu entnehmen, sodass auch unerheblich ist, wen der Amtsleiter bzw. die Amtsleiterin bei seinen bzw. ihren „Bürobesuchen" antrifft. Im Übrigen kann dies mittels eines Dienstplans festgestellt werden, sodass ein milderes Mittel ebenfalls gegeben ist.

Des Weiteren führte der Verantwortliche Rückkehrgespräche, Kritikgespräche oder Mitarbeiter/innen-Vorgesetzten-

gespräche sowie die Überreichung von Ernennungsurkunden als Beispiele an. Jedoch ist schwer vorstellbar, dass gerade diese ohne Terminvereinbarung, sondern ad hoc nach Einsicht in die „Anwesenheitsübersicht" spontan durchgeführt werden.

Es entstand daher der Eindruck, dass alle irgendwie denkbaren Zwecke zusammengetragen wurden, um für irgendeinen dieser Zwecke die Datenverarbeitung doch noch zu rechtfertigen. Allerdings erschöpfte sich die Begründung der Erforderlichkeit dann lediglich in pauschalen Angaben, ohne konkrete Bezüge zwischen Zweck, der Geeignetheit, milderem Mittel und Angemessenheit herzustellen.

Als weitere Voraussetzung der Erforderlichkeit muss die durch die konkrete Datenverarbeitung eintretende Beeinträchtigung der Rechte und Interessen der bzw. des betroffenen Beschäftigten in einem angemessenen Verhältnis zu dem beabsichtigten Zweck der Datenverarbeitung stehen. Dabei sind die Interessen des Arbeitgebers – hier des Dienstherrn – an der Datenverarbeitung und das Persönlichkeitsrecht der/des Beschäftigten zu einem schonenden Ausgleich zu bringen, der beide Interessen möglichst weitgehend berücksichtigt.

In diesem Zusammenhang war auch die Möglichkeit der Überwachung zu beachten. Der Verantwortliche führte dazu aus, dass es sich bei der digitalen Momentaufnahme hinsichtlich einer Anwesenheit oder Abwesenheit vom Dienst heutzutage um ein gewöhnliches Verhalten handele, das keinerlei Schlussfolgerungen auf persönliche Vorlieben oder Ähnliches zulasse, und bei einer Beschränkung hierauf vor allem eine großflächige Überwachung des Verhaltens der Beschäftigten nicht erreicht werden könne. Weiter finde laut dem Verantwortlichen keine dauerhafte Überwachung statt, die Einsicht sei auf einzelne Personen bzw. Personengruppen beschränkt, und es würden weder die Leistung noch das Verhalten oder die Inhalte der Tätigkeit verarbeitet. Nach meiner Auffassung ist in diesem Zusammenhang jedoch zu berücksichtigen, dass bei dem Einsatz von elektronischen Zeiterfassungs- und Zugangskontrollsystemen regelmäßig – zu-

mindest mittelbar – eine Mitarbeiterkontrolle durchgeführt wird (vgl. auch Zeiterfassungs- und Zugangskontrollsysteme in SPA 2017, 69). Die Zulässigkeit von (auch mittelbaren) Mitarbeiterüberwachungen im Rahmen von elektronischen Zeiterfassungssystemen unterliegt daher hohen datenschutzrechtlichen Anforderungen, die dem Persönlichkeitsschutz der Beschäftigten vor den Gefahren einer technisierten Ermittlung ihrer Verhaltens- und Leistungsdaten durch den Arbeitgeber und auch einem damit verbundenen permanenten Überwachungsdruck dienen. Hierbei ist auf den Begriff der technischen Überwachung im Sinne des § 81 Abs. 2 Nr. 12 Personalvertretungsgesetz (PersVG) abzustellen. Der technische Überwachungsbegriff ist dabei weit auszulegen, sodass eine Überwachung bereits vorliegt, wenn die technische Einrichtung objektiv zur Überwachung geeignet ist. Es kommt dabei nicht darauf an, ob mit dem Einsatz des Zeiterfassungssystems die Überwachung der Mitarbeiter/innen unmittelbar bezweckt ist. Entscheidend ist, ob durch die technische Einrichtung eine Kontrolle des Verhaltens oder der Leistung des Mitarbeiters bzw. der Mitarbeiterin möglich ist. Eine technische Überwachung ist daher nur dann zulässig, wenn sich eine Verhaltens- und Leistungskontrolle der Beschäftigten mit den erhobenen Daten technisch ausschließen lässt.

So führte der Verantwortliche aus, dass die Funktion „Anwesenheitsübersicht" zwar an Zeiterfassungsdaten anknüpfe, da sie diese für die Sichtbarkeit des Status als solchen zugrunde lege, aber selbst jedoch keine Zeiterfassung als solche darstelle und für sich allein betrachtet ungeeignet für eine mittelbare Mitarbeiterüberwachung sei. Aus der bloßen Anwesenheit oder dem Arbeitsort würden sich keine Informationen zu Menge oder Qualität der Arbeit einer/eines Beschäftigten ergeben und die Anwesenheit sei auch nicht mit der geschuldeten Dienstleistung gleichzusetzen. Die Anwesenheitsübersicht war nach Meinung des Verantwortlichen für eine Kontrolle der Leistung ungeeignet. Ebenso untauglich war die „Anwesenheitsübersicht" nach Auffassung des Verantwortlichen auch für eine „Verhaltenskontrolle".

Ich habe dem Verantwortlichen mitgeteilt, dass die „Anwesenheitsübersicht" zur Überwachung der Beschäftigten gleichwohl geeignet sei, obgleich diese keine Arbeitszeitdaten enthält, sondern den Anwesenheitsstatus der Beschäftigten ausweist. Auch die Informationen der Anwesenheitsübersicht entstammen dem Zeiterfassungssystem und obliegen und dienen, auch wenn es sich um aggregierte Inhalte handelt, allein der der Vertraulichkeit unterliegenden Personalverwaltung. Im Übrigen erfasse der Begriff der Mitarbeiterüberwachung sowohl die Leistungs- als auch die Verhaltenskontrolle. Wenngleich eine Leistungsüberwachung durch den Verantwortlichen ausgeschlossen werde, ist die „Anwesenheitsübersicht" keineswegs zur Verhaltensüberwachung untauglich, vielmehr ist diese zur Überwachung des Verhaltens der Beschäftigten nicht nur objektiv geeignet, sondern dient gerade der Überwachung, insbesondere vor dem Hintergrund des arbeitszeit- und ortsflexiblen Arbeitens und wird dazu auch eingesetzt. Denn der Verantwortliche teilte selbst mit, dass zum Beispiel die Sachgebietsleitung verpflichtet sei, den Dienstbetrieb im Sachgebiet zu überwachen, und diese nur funktioniere, wenn der Sachgebietsleitung die Möglichkeiten und „Werkzeuge" zur Überwachung bereitstünden.

Zu konstatieren ist in diesem Zusammenhang, dass Veränderungen der Arbeitswelt – auch im öffentlichen Dienst – durch die Gewährung von arbeitszeit- und ortsflexiblem Arbeiten, zu einer Informationsasymmetrie zwischen Beschäftigten und Arbeitgebern bzw. Arbeitgeberinnen führt, sodass das Bedürfnis zunimmt, die im Zuge der Digitalisierung möglichen Überwachungsformen einzusetzen und zu intensivieren (vgl. Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2. Auflage 2025, Rn. 101). Diesem Bedürfnis trägt nach Auffassung meiner Behörde der Verantwortliche durch die Zugriffsberechtigung auf die „Anwesenheitsübersicht" sowohl für die Amtsleitung als auch die Sachgebietsleitung Rechnung. Denn diese dient (auch) der Überwachung des Verhaltens der Beschäftigten, und weil dies so ist, sind damit hohe datenschutzrechtliche Anforderungen an die Zu-

lässigkeit gebunden. Mit den Beschäftigtenkontrollen sind Grundrechtseingriffe verbunden (Recht auf informationelle Selbstbestimmung), die bei der rechtlichen Beurteilung von Überwachungsmaßnahmen zu berücksichtigen sind. Dieser Persönlichkeitsschutz soll die Beschäftigten vor den Gefahren einer technisierten Ermittlung ihrer Verhaltens- und Leistungsdaten durch den/die Arbeitgeber/in und auch einen damit verbundenen permanenten Überwachungsdruck schützen. Neben dieser Überwachung der Beschäftigten durch Vorgesetzte ermöglicht die „Anwesenheitsübersicht" auch eine Überwachung der Beschäftigten untereinander bzw. gegenseitig. Dies führt quasi zu einer „Schwarmüberwachung", die im Ergebnis eine (Selbst-)Disziplinierung der Beschäftigten bzw. deren Verhaltens zur Folge hat, die der/die Arbeitgeber/in beabsichtigt, indem er/sie die technischen Möglichkeiten eröffnet, zumindest aber billigt. Beispielhaft kann die mögliche Frage von Vorgesetzten angeführt werden, aus welchen Gründen der/die Beschäftigte sich erst 10 Uhr „eingestochen" habe und nicht wie sonst üblich 7 Uhr, obgleich die Arbeitszeit flexibel gestaltet werden darf. Weiteres Beispiel für eine derartige Überwachung wäre der Fall, dass ein Mitarbeiter im System als „Büro anwesend" hinterlegt sein kann, der Beschäftigte dennoch nicht telefonisch oder persönlich erreichbar ist, da er just in diesem Moment die Toilette aufsuchte oder mit einem Kollegen in einem anderen Zimmer eine kurze/ungeplante Besprechung abhielt. Dies kann zu einem Überwachungsdruck bzw. Rechtfertigungsdruck nicht nur gegenüber dem oder der Vorgesetzten, sondern auch gegenüber anderen Beschäftigten führen; gegebenenfalls bis zu Vorhaltungen eines Fehlverhaltens hinsichtlich Erbringung der Arbeitsleistung bzw. Arbeitszeit. Vielmehr ergibt sich daraus, dass die „Anwesenheitsübersicht" für eine Mitarbeiterüberwachung nicht nur (objektiv) geeignet ist, sondern auch explizit dafür eingesetzt wird.

Eine Verhaltenskontrolle der Beschäftigten unterliegt jedoch auch hohen datenschutzrechtlichen Anforderungen. So dürfen grundsätzlich Zeiterfassungssysteme vom Arbeitgeber oder von der Arbeitgeberin zur Überwachung der Arbeitszeiten ein-

gesetzt werden. Die Arbeitszeit, die vom Arbeitnehmer bzw. der Arbeitnehmerin geleistet wird, stellt die Gegenleistung für den Entgeltanspruch des Arbeitnehmers bzw. der Arbeitnehmerin dar. Aus diesem Grund besteht für den/die Arbeitgeber/in ein berechtigtes Interesse, die Arbeitszeit der Beschäftigten zu erfassen, um die Einhaltung der vertraglich vereinbarten Arbeitszeit zu überwachen. Die Überwachung der Einhaltung der Arbeitszeiten, als auch das (unentschuldigte) Fernbleiben von der Arbeit oder die Einhaltung der Ruhezeiten etc. sind jedoch ureigenste Aufgaben der Personalverwaltung. Die Verarbeitung von personenbezogenen Beschäftigtendaten hat dementsprechend informationell abgeschottet und konzentriert bei hierfür beauftragten Beschäftigten zu erfolgen, das heißt, sie ist nur einem begrenzten Personenkreis zugänglich, der darüber hinaus zur Verschwiegenheit verpflichtet ist. Auch sind die aus den Arbeitszeiterfassungsdaten generierten Statusdaten keine äußeren, respektive zusammengefassten Informationen, die die Personalverwaltung zur Sicherung von Arbeitsabläufen weitergeben darf. Sie geben vielmehr eine ständige Beobachtungssituation wieder, die auch nicht im Erwartungshorizont der betroffenen Beschäftigten, insbesondere im Hinblick auf die Transparenz der Datenverarbeitung nach Art. 5 Abs. 1 Buchst. a DSGVO, liegt.

Die Beschäftigten der Personalverwaltung, ebenso der/die Amtsleiter/in, benötigen daher schon deshalb kein Zugriffsrecht auf die „Anwesenheitsübersicht", da diesen Einsichtsrechte in größerem Umfang bereits (auf das Zeiterfassungssystem) eingeräumt sind, soweit diese als Personalverwaltung tätig sind bzw. ihr zugewiesene Aufgaben wahrnehmen. Eine weitere Abstufung ergibt sich zu den Vorgesetzten. Grundsätzlich haben diese keinen Zugang zu Daten der Zeiterfassung. Die Regelung des § 5 Abs. 3 Satz 4 Sächsische Arbeitszeitverordnung (SächsAZVO) bestätigt dies. Danach hat der/die Vorgesetzte nur in begründeten Fällen ein Einsichtsrecht in die Aufzeichnungen der Zeiterfassung. Mit der bei den Verantwortlichen genutzten „Anwesenheitsübersicht" werden aus der Zeiterfassung generierte Informationen jedoch einem großen Nutzerkreis zur Verfügung gestellt, ohne dass dem

eine entsprechende Aufgabenzuweisung gegenübersteht. Vielmehr wird die Möglichkeit zu anlassloser Überwachung geschaffen, sowohl durch Vorgesetzte als auch durch Beschäftigte untereinander. Dies kann jedoch, auch im Hinblick auf die große Anzahl betroffener Personen, nicht angemessen sein, da die Interessen der betroffenen Beschäftigten dabei unberücksichtigt bleiben.

Lediglich für die Beschäftigten der Bereiche der Telefonzentrale und der Informations- und Annahmestelle konnte der Verantwortliche eine Erforderlichkeit, die den datenschutzrechtlichen Anforderungen entspricht, begründen. Die darüber hinaus erteilten Zugriffsberechtigungen auf die „Anwesenheitsübersicht" waren jedoch nicht erforderlich und somit datenschutzwidrig.

Im Ergebnis bleibt festzustellen, dass der Frage, wo ein Beschäftigter bzw. eine Beschäftigte aktuell tätig ist, aufgrund der Möglichkeit des flexiblen Arbeitens (in Bezug auch auf Zeit und Ort) eine wesentlich größere Bedeutung als früher zukommt. Meine Behörde verkennt auch nicht, dass damit zumeist höhere organisatorische Anforderungen sowohl für den Dienstherrn als auch für die Beschäftigten in ihrer Gemeinschaft/im Team verbunden sind. Dies entbindet den Verantwortlichen allerdings nicht von der Aufgabe, die Datenverarbeitungen nach den Grundsätzen der Erforderlichkeit und Datenminimierung zu beurteilen und dementsprechende differenzierte, auf den Einzelfall bezogene organisatorische Maßnahmen und Abstufungen innerhalb der Arbeitsorganisation (unter anderem bei Zugriffsberechtigungen) zu treffen bzw. umzusetzen.

Was ist zu tun?
Die Datenverarbeitungen sind nach den Grundsätzen der Erforderlichkeit und Datenminimierung zu beurteilen, und es sind dementsprechende differenzierte, auf den Einzelfall bezogene organisatorische Maßnahmen und Abstufungen innerhalb der Arbeitsorganisation (unter anderem bei Zugriffsberechtigungen) zu treffen bzw. umzusetzen.

2.2.19 Offenbarung von ärztlichen Diagnosen bei Fortsetzungserkrankungen

↗ Art. 9 DSGVO, § 26 Abs. 3 BDSG, § 3 EFZG

In diesem Jahr erreichten mich vielfach Anfragen von Beschäftigten, welche durch ihre Arbeitgeber/innen um Offenbarung der medizinischen Diagnose bei Einreichen einer Folgebescheinigung zur Arbeitsunfähigkeit gebeten wurden.

Das Entgeltfortzahlungsgesetz (EFZG) regelt in § 3 Abs. 1 Satz 1, dass ein Arbeitnehmer, der durch Arbeitsunfähigkeit infolge von Krankheit an seiner Arbeitsleistung gehindert wird, einen Anspruch auf Entgeltfortzahlung im Krankheitsfall gegenüber dem Arbeitgeber für die Zeit der Arbeitsunfähigkeit bis zur Dauer von sechs Wochen hat. Führt dieselbe Krankheit zu mehreren Zeiten der Arbeitsunfähigkeit, so sind diese Zeiten zu addieren. Der/Die Arbeitnehmer/in erhält dann für höchstens sechs Wochen Entgeltfortzahlung. Grundsätzlich trägt der/die Arbeitnehmer/in die Darlegungs- und Beweislast für die Anspruchsvoraussetzungen des § 3 Abs. 1 Satz 1 EFZG, das heißt, der/die Arbeitnehmerin muss unter anderem nachweisen, dass tatsächlich eine Arbeitsunfähigkeit besteht. Im Regelfall legt der/die Arbeitnehmer/in dem/der Arbeitgeber/in dazu eine sogenannte Arbeitsunfähigkeitsbescheinigung vor. Diese ist eine ärztliche Bestätigung, dass ein/e Arbeitnehmer/in krankheitsbedingt seine/ihre Arbeit nicht ausüben kann, und gilt als Anscheinsbeweis. Die Arbeitsunfähigkeitsbescheinigung enthält jedoch keine ärztlichen Diagnosen.

Wird der/die Arbeitnehmer/in infolge derselben Krankheit – nach Ausschöpfung der sechs Wochen – erneut arbeitsunfähig, so verliert er/sie wegen der erneuten Arbeitsunfähigkeit den Anspruch nach § 3 Abs. 1 Satz 1 EFZG für einen weiteren Zeitraum von höchstens sechs Wochen nicht, wenn (1.) er/sie vor der erneuten Arbeitsunfähigkeit mindestens sechs Monate nicht infolge derselben Krankheit arbeitsunfähig war oder (2.) seit Beginn der ersten Arbeitsunfähigkeit infolge derselben Krankheit eine Frist von zwölf Monaten abgelaufen ist, § 3 Abs. 1 Satz 2 EFZG.

Wird der/die Arbeitnehmer/in wiederholt arbeitsunfähig, kommt es für das Entstehen eines erneuten Anspruches auf Lohnfortzahlung gegenüber dem/der Arbeitgeber/in daher darauf an, ob die Arbeitsunfähigkeit auf einer anderen Krankheit beruht oder ob dieselbe Krankheit Auslöser für die Arbeitsunfähigkeit ist. Der letzte Fall (dieselbe Krankheit ist Auslöser der Arbeitsunfähigkeit) ist in § 3 Abs. 1 Satz 2 EFZG geregelt. Danach entfällt grundsätzlich der Anspruch auf

Lohnfortzahlung, soweit nicht eine der in § 3 Abs. 1 Satz 2 EFZG geregelten zwei Ausnahmen zutrifft.

In den mir vorliegenden Beschwerden ging es den Arbeitgebern darum, festzustellen, ob sie aufgrund einer Fortsetzungserkrankung von der Entgeltfortzahlungspflicht befreit sind, da sie für dieselbe Erkrankung schon für sechs Wochen Entgeltfortzahlung geleistet haben.

Das Bundesarbeitsgericht (BAG) hat mit Urteil vom 18. Januar 2023 (5 AZR 93/22) über die Anforderungen an die Mitwirkungspflicht des Arbeitnehmers bzw. zur Darlegungs- und Beweislast im gerichtlichen Verfahren entschieden. Das BAG hat ausgeführt, dass eine abgestufte Darlegungs- und Beweislast gilt. Das BAG führte aus:

> „Zunächst muss der Arbeitnehmer – soweit sich aus der Arbeitsunfähigkeitsbescheinigung dazu keine Angaben entnehmen lassen – darlegen, dass keine Fortsetzungserkrankung besteht. Hierzu kann er eine ärztliche Bescheinigung vorlegen. Bestreitet der Arbeitgeber, dass eine neue Erkrankung vorliegt, hat der Arbeitnehmer Tatsachen vorzutragen, die den Schluss erlauben, es habe keine Fortsetzungserkrankung bestanden. Er muss laienhaft bezogen auf den gesamten maßgeblichen Zeitraum schildern, welche gesundheitlichen Beeinträchtigungen und Beschwerden mit welchen Auswirkungen auf seine Arbeitsfähigkeit bestanden und die behandelnden Ärzte von der Schweigepflicht entbinden. Denn erst ausgehend von diesem Vortrag ist ein regelmäßig dem Arbeitgeber substantiierter Sachvortrag möglich. Auf das Bestreiten des Arbeitgebers genügt die bloße Vorlage einer ärztlichen Bescheinigung nicht mehr. Eine Arbeitsunfähigkeitsbescheinigung, die von einem anderen Arzt ausgestellt ist, kann sich auch als Erstbescheinigung ohnehin nicht zum (Nicht-)Vorliegen einer Fortsetzungserkrankung verhalten."

In dem vorgenannten Urteil hat sich das BAG auch mit dem Grundrecht auf informationelle Selbstbestimmung des Betroffenen auseinandergesetzt und ist zu dem Ergebnis gelangt, dass der Eingriff in dieses Grundrecht verhältnismäßig und damit gerechtfertigt ist, soweit die abgestufte Darlegungs- und Beweislast bei Fortsetzungserkrankungen vom Arbeitnehmer die Offenlegung von Gesundheitsdaten verlangt. Das BAG stellte insbesondere fest, dass der Eingriff auch erforderlich ist, weil keine gleich effektiven Mittel zur Verfügung stehen, die weniger stark in die informationelle Selbstbestimmung eingreifen. Weiter stellte das BAG fest, dass das Recht der Beschäftigten auf informationelle Selbstbestimmung hinter den Verfahrensgrundrechten und den Grundrechten aus Art. 12 Abs. 1,14 Abs. 1 Grundgesetz des Arbeitgebers zurücktreten.

Zusätzlich führte das BAG in dem oben genannten Urteil (Rn. 24) aus, dass auch eine vorprozessuale Datenverarbeitung beim Arbeitgeber grundsätzlich auf § 26 Abs. 3 Bundesdatenschutzgesetz (BDSG) in Verbindung mit Art. 9 Abs. 2 Buchst. b DSGVO gestützt werden kann, da eine entsprechende Datenverarbeitung in Ausübung von Rechten und zur Erfüllung rechtlicher Pflichten aus dem Arbeitsverhältnis im Sinne von § 26 Abs. 3 BDSG erfolgt, nämlich bei der Durchführung der in § 3 Abs. 1 EFZG geregelten Entgeltfortzahlungspflicht im Rahmen dessen, was zur Prüfung ihrer Voraussetzungen arbeitgeberseitig erforderlich ist.

In den mir vorliegenden Beschwerden haben sich die Arbeitgeber/innen bei ihrem Verlangen auf Offenbarung der Gesundheitsdaten gegenüber den betroffenen Beschäftigten auf dieses Urteil berufen.

Die Entscheidung des BAG befasste sich zwar vornehmlich mit den Darlegungs- und Beweisregeln im Rahmen der gerichtlichen Auseinandersetzung, stellte allerdings in einem Obiter Dictum fest, dass dies auch für die vorprozessuale Datenverarbeitung (zur Durchführung des § 3 Abs. 1 EFZG) gelte.

Unabhängig davon, ob die pauschale Verweigerung der Entgeltfortzahlung durch den/die Arbeitgeber/in mit dem Hinweis auf das Vorliegen einer Fortsetzungserkrankung den

arbeitsrechtlichen Anforderungen genügt, ergeben sich für Arbeitgeber/innen datenschutzrechtliche Folgefragen, wie zum Beispiel zur Verwaltung dieser Daten oder zu Aufbewahrungs- bzw. Löschfristen.

Soweit eine Verarbeitung von Gesundheitsdaten im Rahmen der Durchführung des § 3 Abs. 1 EFZG daher zulässig sein sollte, haben Arbeitgeber/innen die zweckgebundene Verarbeitung sicherzustellen, das heißt, dass die zur Durchführung des § 3 Abs. 1 EFZG erhobenen Daten auch nur für diese Zwecke verwendet und aufbewahrt werden dürfen. Es sind in diesem Kontext auch nur solche Verarbeitungen zulässig, die dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sind, Art. 5 Abs. 1 Buchst. c DSGVO (Grundsatz der Datenminimierung). Es ist danach zu verlangen, dass die erhobenen Gesundheitsdaten bei betrieblicher Leistungsfähigkeit getrennt von der Verarbeitung der weiteren Beschäftigtendaten erfolgen, insbesondere dürfen diese nicht in die Personalakte aufgenommen werden. Den betroffenen Beschäftigten sollte zugesichert sein, dass die personalverwaltende Stelle bzw. Vorgesetzte keine Kenntnis von den spezifischen Gesundheitsdaten erhalten. Verantwortlichen mit genügender personeller Kapazität ist zur Umsetzung anzuraten, die Gesundheitsdaten innerhalb des Unternehmens in einer informationell abgeschotteten „Vertrauensstelle" – die von der personalverwaltenden Stelle abgesetzt ist zu verarbeiten. Im Übrigen haben Verantwortliche die Anzahl der Beschäftigten, die Zugang zu den empfangenen Gesundheitsinformationen haben, auf das erforderliche Maß zu minimieren. Weiterhin ist seitens der Verantwortlichen für die konkreten Datenverarbeitungsprozesse sicherzustellen, dass erforderliche Datenschutz-Folgenabschätzungen gemäß Art. 35 DSGVO vorgenommen werden und die Verarbeitung der Gesundheitsdaten bei der Führung des Verzeichnisses der Verarbeitungstätigkeiten nach Art. 30 DSGVO ordnungsgemäß berücksichtigt wird.

Abschließend ist anzumerken, dass aus datenschutzrechtlicher Sicht das vorstehende Urteil des BAG auch Bedenken

Was ist zu tun?
Arbeitgeber/innen bzw. Dienstherren sollten zur Durchführung des § 3 Abs. 1 EFZG datenschutzkonforme Verfahrensweisen bzw. Konzepte betriebs- und dienststellenintern etablieren.

im Hinblick auf Wertungswidersprüche zu Regelungen des betrieblichen Eingliederungsmanagements und damit verbundene Verarbeitung von Gesundheitsdaten erweckt, die auch durch die vorgenannten datenschutzrechtlichen Anforderungen, insbesondere technische und organisatorische Maßnahmen (vgl. Art. 25 DSGVO), nicht aufgelöst werden.

2.3 Einwilligungsfragen

2.3.1 Veröffentlichung von Beschäftigtendaten im Internet

↗ Art. 7 Abs. 3 Satz 1 DSGVO, Art. 17 Abs. 1 Buchst. b DSGVO, § 121 Abs. 1 Satz 1 BGB

Immer wieder erreichen meine Behörde Beschwerden von Beschäftigten, die die Veröffentlichung ihrer personenbezogenen Daten auf der Internetseite ihres Arbeitgebers bzw. ihrer Arbeitgeberin rügen.
Die Veröffentlichung von Beschäftigtendaten im Internet ist nicht grundsätzlich unzulässig, bedarf jedoch für jeden Einzelfall einer Rechtsgrundlage. Zumeist stützen sich Arbeitgeber/innen auf eine Einwilligung des/der Beschäftigten. Diese Rechtsgrundlage erweist sich jedoch für Arbeitgeber/innen häufig als problematisch, da die Voraussetzungen in formeller und materieller Hinsicht oft nicht gegeben sind und der/die Beschäftigte die Einwilligung jederzeit widerrufen kann. Dies begründet für Arbeitgeber/innen die Gefahr, dass in der Vergangenheit Daten ohne Rechtsgrundlage und somit rechtswidrig verarbeitet wurden, oder im Falle des Widerrufs, dass die Daten in Zukunft nicht mehr verarbeitet werden können. Letzteres kann sich insbesondere für die Öffentlichkeitsarbeit des Arbeitgebers bzw. der Arbeitgeberin als problematisch erweisen. Die Heranziehung der Einwilligung als Rechtsgrundlage erfordert darüber hinaus die Etablierung von internen Prozessen, um die gesetzlichen Anforderungen, wie zum Beispiel die Löschung der personenbezogenen Beschäftigtendaten, datenschutzkonform umzusetzen.

So erreichte mich im letzten Berichtszeitraum die Beschwerde des Beschäftigten einer Hochschule, der in die weltweite Veröffentlichung seiner Daten (insbesondere Nachname und Foto) zunächst eingewilligt hatte, dann die Einwilligung widerrufen und umgehend die Löschung seiner Daten verlangt hatte. Eine Löschung der Daten fand zunächst trotz mehrfacher Aufforderung nicht statt. Der Beschäftigte teilte mir mit, dass er sich zunächst an die/den Fachvorgesetzte/n wandte und, nachdem seinem Löschbegehren trotz mehrfacher Aufforderung nicht nachgekommen sei, an die Personalvertretung. Die Daten seien zwar dann gelöscht worden, allerdings rügte der Beschäftigte gegenüber meiner Behörde, dass die Löschung seiner Daten nicht umgehend erfolgt sei.
Der Verantwortliche teilte in seiner Stellungnahme mit, dass die Prüfung des Löschbegehrens einige Zeit in Anspruch genommen habe. Dies begründete der Verantwortliche mit der Prüfung rechtlicher Rahmenbedingungen, insbesondere welche formalen Anforderungen an das Löschbegehren gestellt würden, ob zum Beispiel das Löschbegehren eine Unterschrift erfordere.
Gemäß Art. 7 Abs. 3 Satz 1 DSGVO hat die betroffene Person das Recht, ihre Einwilligung jederzeit zu widerrufen. Folge einer widerrufenen Einwilligung ist die Unzulässigkeit der weiteren Datenverarbeitung für die Zukunft. Der Verantwortliche ist daher verpflichtet, diese Daten unverzüglich zu löschen, Art. 17 Abs. 1 Buchst. b DSGVO. Unter dem Begriff „unverzüglich" ist, unter Rückgriff auf § 121 Abs. 1 Satz 1 Bürgerliches Gesetzbuch (BGB), zu verstehen, dass die Löschung „ohne schuldhaftes Zögern" vorzunehmen ist. Die Löschung darf nach – berechtigter – Beantragung bzw. nach Eintritt des Löschgrundes nicht länger als unvermeidlich hinausgezögert werden. Da der Verantwortliche die Möglichkeit haben muss, das Vorliegen der Voraussetzungen des Löschungsanspruchs zu prüfen, liegt ein schuldhaftes Zögern jedenfalls für den Zeitraum nicht vor, den der Verantwortliche benötigt, um mit zumutbarem Aufwand die Voraussetzungen des Anspruchs zu überprüfen.

Was ist zu tun?
Es sind interne Verwaltungsabläufe bzw. Prozesse zur Umsetzung datenschutzrechtlicher Anforderungen bzw. der adäquaten Berücksichtigung von Betroffenenrechten zu implementieren.

Der Verantwortliche ist daher gehalten, die internen Verwaltungsabläufe bzw. Prozesse so zu gestalten, dass die datenschutzrechtlichen Anforderungen, insbesondere die unverzügliche Löschung im Falle des Widerrufs der Einwilligung, eingehalten werden.

2.3.2 Krankenbesuche durch den Arbeitgeber

↗ Art. 9 DSGVO, § 26 BDSG

Unternehmen stehen in der Praxis wiederholt vor der Frage, ob und in welchem Umfang sie Beschäftigte während einer Krankschreibung telefonisch kontaktieren oder gar an deren Wohnanschrift aufsuchen dürfen. Hintergründe für das Kontaktersuchen sind zum einen oftmals Zweifel an der Arbeitsunfähigkeit selbst und zum anderen die Fürsorgepflicht, welche sich aus arbeitsschutzrechtlichen Vorgaben ergeben kann. Mehrfach erreichten meine Behörde im Berichtszeitraum Beschwerden betroffener Beschäftigter, die mit Besuchen nicht einverstanden waren und hierin (auch) einen Datenschutzverstoß sahen.

Aus datenschutzrechtlicher Sicht sind diese sogenannten Krankenbesuche häufig problematisch, da diese zum einen als Eingriff in die Privatsphäre betrachtet werden und zum anderen zumeist mit der Verarbeitung von sensiblen personenbezogenen Daten, insbesondere Gesundheitsdaten, verbunden sind.

Bei Gesundheitsdaten handelt es sich jedoch um eine besondere Kategorie personenbezogener Daten, deren Verarbeitung grundsätzlich unzulässig ist. Ausnahmen von dieser Untersagung der Datenverarbeitung ergeben sich aus Art. 9 Abs. 2 DSGVO. Für Beschäftigungsverhältnisse erlaubt § 26 Abs. 3 Satz 1 Bundesdatenschutzgesetz (BDSG) eine Verarbeitung von Gesundheitsdaten, wenn dies zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem

Ausschluss der Verarbeitung überwiegt. Beispiele für entsprechende Datenverarbeitungen kann die Unterrichtung des Betriebsrates über langzeiterkrankte Beschäftigte sein oder ärztliche Eignungsuntersuchungen. Auch das Führen von sogenannten Krankengesprächen kann unter diese Regelung gefasst werden. Dabei handelt es sich zumeist um Krankenrückkehrgespräche bzw. sogenannte Fehlzeitengespräche. Mittels dieser Gespräche sollen Fehlzeiten bzw. Arbeitsunfähigkeitszeiten reduziert werden, indem zum Beispiel gesundheitsunterstützende Maßnahmen am Arbeitsplatz durch den/die Arbeitgeber/in ergriffen werden. Zu hinterfragen ist jedoch, ob dieser Zweck mit den sogenannten Krankenbesuchen von Arbeitgebern bzw. Arbeitgeberinnen verfolgt wird und dieser überhaupt damit erreicht werden kann.

Soweit Arbeitgeber/innen davon ausgehen, dass eine Arbeitsunfähigkeit nicht besteht, sondern die Erkrankung nur vorgetäuscht ist, müssen den Arbeitgebern bzw. Arbeitgeberinnen für den konkreten Einzelfall Anhaltspunkte vorliegen. Ein hoher Krankenstand im Unternehmen genügt als Rechtfertigung nicht. Das mildere Mittel stellt in jedem Fall die Beteiligung des Medizinischen Dienstes dar. Durch dessen Stellungnahme kann auch der Beweiswert einer Arbeitsunfähigkeitsbescheinigung erschüttert werden. Im Übrigen ist für die Arbeitgeber/innen durch diese Krankenbesuche zumeist nicht erkennbar, ob der Beschäftigte tatsächlich arbeitsunfähig ist oder nicht.

Auch mittels Einwilligung ist eine Verarbeitung von Gesundheitsdaten gemäß § 26 Abs. 3 Satz 2 BDSG zulässig, wobei dies die Ausnahme darstellt. Aufgrund des zwischen Arbeitgeber/Arbeitgeberinnen und Beschäftigten bestehenden Abhängigkeitsverhältnisses mangelt es zumeist an der Freiwilligkeit der Einwilligung, die jedoch Voraussetzung für die Wirksamkeit ist. Beschäftigte sind insbesondere nicht verpflichtet, detaillierte Auskünfte über ihre Erkrankung oder deren Symptome im Rahmen dieser Krankenbesuche gegenüber dem/der Arbeitgeber/in zu offenbaren. Im Regelfall scheidet daher eine Einwilligung als Rechtsgrundlage für die Verarbeitung dieser Daten aus.

Was ist zu tun?
Datenverarbeitungen im Zusammenhang mit Krankenbesuchen von Beschäftigten sind von Arbeitgebern bzw. Arbeitgeberinnen auf ihre datenschutzrechtliche Zulässigkeit zu prüfen, insbesondere, ob eine Rechtsgrundlage gegeben ist sowie auch die Erforderlichkeit und Verhältnismäßigkeit gewahrt werden. Das mildere Mittel besteht zumeist in einer Überprüfung durch den Medizinischen Dienst der Krankenversicherung.

Auch erfordert die Einwilligung bei der Verarbeitung von Gesundheitsdaten die Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist, vgl. § 26 Abs. 3 Satz 3 BDSG. Zudem hat der/die Arbeitgeber/in den Beschäftigten über den Zweck der Datenverarbeitung und über sein Widerrufsrecht zu belehren, vgl. § 26 Abs. 3 Satz 4 BDSG. Auch diese zwei zuletzt genannten Voraussetzungen werden regelmäßig bei den Krankenbesuchen nicht gegeben sein.

2.3.3 Datenschutz bei der Nutzung eines elektronischen Schließsystems

↗ Art. 4, 6, 7 DSGVO; Art. 13 GG

Durch die Beschwerde eines Betroffenen wurde ich darauf aufmerksam, dass seitens eines Studentenwerks sowohl für Wohnbereiche als auch für die Büros der Mitarbeiter ein elektronisches Schließsystem verwendet wurde. Kleine Chips oder Karten als Ersatz für einen herkömmlichen Schlüssel bieten viele Möglichkeiten, aber auch viele Risiken.
Jeder Öffnungs- und Schließvorgang beinhaltet eine Datentransaktion. Abhängig von Modell und Einstellungen des Schließsystems können diese Daten in dem Schließmechanismen gespeichert, ausgelesen und verarbeitet werden. Dies kann einerseits zum Schutz beitragen, indem zum Beispiel ein unberechtigter Öffnungsversuch aufgezeichnet werden kann. Andererseits entsteht hierdurch auch eine Datenspeicherung auf Vorrat.
Insbesondere im Hinblick auf die Schließmechanismen von Wohnräumen, Gemeinschaftsküchen und Aufenthaltsräumen ist dabei auch der besondere Schutz des Artikels 13 Grundgesetz zu beachten. Dieser schützt die Privat- und Intimsphäre innerhalb des Wohnraumes. Unabhängig von einem eigenständigen Verstoß gegen die Unverletzlichkeit der Wohnung strahlt diese Schutzwirkung auch auf die Erhebung von Daten aus.
Im vorliegenden Fall war außerhalb einer Einwilligung keine Rechtsgrundlage für die Speicherung der Schließdaten ein-

schlägig. Nach Art. 6 Abs. 1 Buchst. a DSGVO ist eine Datenverarbeitung bei Vorliegen einer Einwilligung rechtmäßig. Die Einwilligung ist in Art. 4 Nr. 11 DSGVO legal definiert und beinhaltet insbesondere, dass man bei einer umfassenden Kenntnis des Sachverhaltes eine freiwillige Entscheidung treffen kann. Erwägungsgrund 42 Satz 5 zur DSGVO stellt dabei ausdrücklich klar, dass eine Freiwilligkeit nur dann vorliegt, wenn die betroffene Person eine echte Wahl hat und somit in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden.

Datenverarbeitungen im Beschäftigtenverhältnis, die auf eine Einwilligung gestützt werden, sind aufgrund des bestehenden Abhängigkeitsverhältnisses stets äußerst kritisch zu hinterfragen. Vor allem das Kriterium der Freiwilligkeit ist zumeist nicht erfüllt. Für die Beurteilung der Freiwilligkeit der Einwilligung sind insbesondere die im Dienst- oder Beschäftigungsverhältnis bestehende Abhängigkeit zwischen den Beschäftigten und dem Dienstherrn oder dem/der Arbeitgeber/in sowie die Umstände, unter denen die Einwilligung erteilt wird, zu berücksichtigen. Hiermit setze ich mich regelmäßig auseinander, was sich auch aus meinen Tätigkeitsberichten abzeichnet (zum Beispiel: Tätigkeitsbericht 2021, 1.1, Seite 24 ff. und Tätigkeitsbericht Datenschutz 2023, 2.2.7, Seite 68 ff.).

Hinsichtlich der Studierenden ist durch die Tatsache, dass ohne die Einwilligung in die Datenerhebung und Verarbeitung keine Vermietung möglich ist, eine Freiwilligkeit der Einwilligung ausgeschlossen. Da viele Studierende auf die günstigeren Mietbedingungen des Studentenwerks angewiesen sind, um überhaupt studieren zu können, entsteht auch hier ein Überordnungs-/Unterordnungsverhältnis, welches eine Freiwilligkeit ausschließt.

Im Ergebnis ist daher die Speicherung von Schließdaten im elektronischen Schließsystem durch das Studentenwerk nicht datenschutzgerecht erfolgt. Nachdem ich diesem meine Rechtsauffassung mitgeteilt habe, wurden sämtliche Speicherungen sofort eingestellt.

Tätigkeitsbericht 2021:
↗ sdb.de/tb2021

Tätigkeitsbericht Datenschutz 2023:
↗ sdb.de/tb2023

Was ist zu tun?
Datenvereinbarungen zu elektrischen Schließmechanismen sollten gut und aufmerksam gelesen werden. Die Mechanismen bieten viele Möglichkeiten, aber im datenrechtlichen Sinne auch viele Risiken. Eine Einwilligung in die Datenverarbeitung kann nur freiwillig erfolgen.

2.3.4 Veröffentlichung von Fotos bei Schulveranstaltungen

↗ § 23 KunstUrhG

Auch im Berichtszeitraum erreichten mich Anfragen und Beschwerden zur Veröffentlichung von Fotografien bei Schulveranstaltungen. Dabei besteht regelmäßig ein Interesse der Presse, der Schule, aber auch von Privatpersonen, den Moment für Erinnerungszwecke in einem Bild festzuhalten. Das ist verständlich und nachvollziehbar. Die Schulen dürfen diese Bilder jedoch nur in bestimmten Situationen auch veröffentlichen.

Die Verarbeitung von Daten ist für sächsische Schulen in der Sächsischen Verwaltungsvorschrift Schuldatenschutz geregelt (Sächs. VwV Schuldatenschutz vom 11. Juli 2018 [MBl. SMK S. 282], zuletzt enthalten in der Verwaltungsvorschrift vom 1. Dezember 2023 [SächsABl. SDr. S. S 287]). Diese liefert in den Anlagen auch ein Formular zur Einwilligung in die Veröffentlichung von Fotografien. Unabhängig hiervon bleiben jedoch auch andere Regelungen, insbesondere Bundesgesetze, weiterhin anwendbar, so auch das Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie (KunstUrhG).

Grundsätzlich ist eine Veröffentlichung von Fotografien nach § 22 KunstUrhG nur mit einer Einwilligung möglich. Nur in den vier in § 23 Abs. 1 KunstUrhG dargestellten Fällen ist eine Veröffentlichung auch ohne Einwilligung, das heißt, auch entgegen dem Willen der Dargestellten, zulässig. Nach § 23 Abs. 1 Nr. 3 KunstUrhG dürfen Bildnisse, welche Personen bei Versammlungen, Aufzügen oder ähnlichen Veranstaltungen zeigen, auch ohne eine Einwilligung veröffentlicht werden. Bei Schulveranstaltungen handelt es sich um kulturelle Veranstaltungen, bei welchen die Darstellenden ihr Können den anwesenden Zuschauern zur Schau stellen. Eine entsprechende Außenwirkung ist in diesem Zusammenhang vorauszusehen und in meisten Teilen erwünscht. Es handelt sich damit um einen sogenannten „einem Aufzug ähnlichen Vorgang".

Diese Möglichkeit wird jedoch durch § 23 Abs. 2 KunstUrhG begrenzt. Bei der Bezeichnung des „berechtigten Interesses" handelt es sich um einen unbestimmten Rechtsbegriff. Eine gesetzliche Normierung, was das berechtigte Interesse darstellt, gibt es nicht. In der Rechtsprechung haben sich zur Konkretisierung des Begriffes verschiedene Fallgruppen gebildet, in welchen ein berechtigtes Interesse anerkannt ist. Voran zu stellen ist, dass der bloße Unwillen nicht ausreicht. Die Teilnahme an einer Schulveranstaltung, sei es als Zuschauerin, Zuschauer oder als darstellende Person, ist Teil der Sozialsphäre. Für die Anwendbarkeit des § 23 Abs. 2 KunstUrhG müsste daher ein besonderes Interesse am Persönlichkeitsschutz oder eine konkrete Gefährdungslage für die abgebildete Person vorgetragen werden. Hinzu kommt, dass die betroffene Person ihr Verhalten auch der Gefährdungssituation anpassen muss und sich bemüht, nicht im Bild öffentlich in Erscheinung zu treten. Wer sich hingegen trotz konkreter Gefährdung der Öffentlichkeit präsentiert, kann sich auf den Schutz von § 23 Abs. 2 KunstUrhG nicht berufen.

In der Regel dürfen Schulen daher Fotografien der Schulveranstaltungen zu nicht kommerziellen Zwecken, zum Beispiel auf der Website der Schule, veröffentlichen.

Dies gilt übrigens auch dann, wenn die Veranstaltung nicht von der Schule organisiert wurde, sondern von externen Veranstaltern. Eine Berichterstattung, auch in der Presse, ist in diesen Fällen in der Regel durch § 23 KunstUrhG gestattet.

Was ist zu tun?
Auch bei Schulveranstaltungen ist die Anwendung von § 23 KunstUrhG nicht ausgeschlossen. Wer nicht auf Fotografien abgebildet und veröffentlicht werden möchte, muss selbst versuchen, außerhalb des Aufnahmebereichs zu bleiben. In besonderen Ausnahmefällen kann auch die Beschränkung des § 23 Abs. 2 KunstUrhG eingreifen, der bloße Unwillen reicht jedoch nicht aus.

2.3.5 Fremdhospitation im Schulunterricht

↗ Art. 4, 6, 7 DSGVO; § 3 SächsDSDG; §1 SächsSchulG

Im Berichtszeitraum erreichte mich die Beschwerde der Eltern eines Schülers. Es sollte eine Begutachtung durch eine Hospitation während des Unterrichtes stattfinden. Da es sich nicht um eine Fachkraft der Schule, sondern um eine außenstehende dritte Person handelte, wurde seitens der Klassenlehrerin die Zustimmung der Eltern der übrigen Kinder der Klasse eingeholt.

Im Rahmen dieser Einwilligung teilte die Klassenlehrerin auch den Namen des betroffenen Schülers mit. Dies hatten seine Eltern nicht erwartet und sahen hierin eine Datenschutzverletzung. Nachdem ich mir die entsprechenden Schriftstücke vorlegen ließ, konnte ich jedoch im Ergebnis der Auffassung der Eltern nicht folgen:

Die Datenverarbeitung und Offenlegung erfolgte rechtmäßig gemäß § 3 Abs. 1 Sächsisches Datenschutzdurchführungsgesetz (SächsDSDG) in Verbindung mit § 1 Abs. 1 Sächsisches Schulgesetz (SächsSchulG). § 3 Abs. 1 SächsDSDG erlaubt die Verarbeitung von Daten, solang dies für die Erfüllung der öffentlichen Aufgabe notwendig ist. § 1 Abs. 1 SächsSchulG definiert die Aufgabe der sächsischen Schulen als Unterrichtung und Erziehung junger Menschen in einer partnerschaftlichen Beziehung mit den Eltern.

Teil dieses Bildungs- und Erziehungsauftrages ist auch die Ermöglichung einer Hospitation. Um diese rechtmäßig umsetzen zu können, ist insbesondere bei externem Fachpersonal die Einwilligung der Sorgeberechtigten der anderen Schülerinnen und Schüler der Klasse einzuholen. Eine andere Rechtsgrundlage zur Offenlegung der Daten der übrigen Kinder gegenüber einer dritten Person besteht nicht.

Eine Einwilligung im Sinne des Art. 6 Abs. 1 Buchst. a in Verbindung mit Art. 7 DSGVO kann jedoch nur dann rechtmäßig erfolgen, wenn diese freiwillig und in Kenntnis aller Umstände erfolgt (Art. 4 Nr. 11 DSGVO). Zu dieser umfassenden Kenntnis gehört auch, zu erfahren, welchem Zweck die Fremdhospitation dient, welche Daten erfasst werden – hier auch der Umgang mit anderen Schülerinnen und Schülern während des Unterrichts – und wer für die Daten verantwortlich (im Sinne des Art. 4 Nr. 7 DSGVO) ist. Dies schließt nicht nur die Information über die Person, welche die Fremdhospitation durchführt, mit ein, sondern auch die Angabe des betroffenen Kindes. Auch eine sachliche Beschreibung des Grundes für die Fremdhospitation hat zu erfolgen. Dabei ist jedoch darauf zu achten, dass nur notwendige Daten offengelegt werden.

Was ist zu beachten?
Für eine rechtmäßige Einwilligung in die Verarbeitung von Daten im Sinne der DSGVO muss eine umfassende Kenntnis des Sachverhaltes vorliegen. Hierzu zählen insbesondere der Zweck der Verarbeitung und die Angabe, wer der Verantwortliche (Art. 4 Nr. 7 DSGVO) für die Verarbeitung ist. Dies gilt insbesondere dann, wenn Daten von Kindern betroffen sind.

Die Klassenlehrerin hat daher bei der Einholung der Einwilligungserklärungen keine Fehler gemacht. Vielmehr konnte eine rechtmäßige und datenschutzrechtlich gesicherte Fremdhospitation erfolgen.

2.3.6 Videoaufnahmen bei Fußballspielen im Kinder- und Jugendbereich mithilfe von Kameradrohnen zur taktischen Auswertung

↗ Art. 6 Abs. 1 Buchst. a und f DSGVO

Im letzten Jahr erhielt ich die Anfrage eines Amateurvereins betreffend der Zulässigkeit von Aufnahmen von einzelnen Fußballspielen mittels einer mit Videokamera ausgestatteten Drohne. Zusätzlich enthielt das Schreiben allgemeine Fragen zu Drohnen, sogenannten „Drohnenführerscheinen", Genehmigungen, der Zulässigkeit des Überflugs bestimmter Bereiche etc. Bezogen auf letztere Fragen war schon auf die Zuständigkeit der Landesdirektion Sachsen zu verweisen. Meine Behörde ist lediglich gesetzlich berufen, die Zulässigkeit der Verarbeitung personenbezogener Daten zu prüfen und verfügt hierfür über eine Zuständigkeit.
Datenschutzrechtlich war insoweit allein die Erstellung und weitere Verwendung der Videoaufnahmen als eine Form der Verarbeitung personenbezogener Daten zu betrachten. Welche Technik bzw. ob Drohnen dabei zum Einsatz kommen, war im Grunde nicht entscheidend gewesen. Der anfragende Verein als Verantwortlicher teilte mit, dass die Videoaufzeichnungen dazu dienen sollten, taktische Analysen im Nachgang durchzuführen. Aus dem Zusammenhang ergab sich, dass auch Fußballspiele im Kinder- und Jugendbereich betroffen sein sollten. Soweit Fußballspieler/innen auch als solche erkennbar sind, was zu unterstellen war, da die vorgesehene Maßnahme auf eine entsprechende fußballerische Schulung abzielte und insoweit auch einzelne Spieler/innen erkennbar sein mussten, handelt es sich dementsprechend um personenbezogene Datenverarbeitung.

Datenschutzrechtlich ist eine Verarbeitung personenbezogener Daten nur dann zulässig, wenn sich der/die Kamerabetreiber/in (Verantwortliche) auf eine wirksame Rechtsgrundlage zu stützen in der Lage ist. Diese kann sich nur aus einem der in der Vorschrift des Art. 6 Abs. 1 DSGVO aufgeführten Rechtsgründe ergeben. Der Verein als Verantwortlicher führte dazu aus, dass der Verein seine Zustimmung zu den Videoaufnahmen erteilen werde. Verbunden war diese Feststellung mit der Frage, wem die Befugnis zur Erteilung und Versagung des Rechts zu videografieren auf den Sportstätten des Vereins zustehe.

Zunächst übt der ausrichtende Verein (natürlich) das Hausrecht über seine Sportstätte aus, kann also als solcher den Einsatz von Kameradrohnen untersagen. Ungeachtet dessen stehen den Videoaufnahmen auch datenschutzrechtliche Belange entgegen. So ist, gerade im Kinder- und Jugendsportbereich, bei einer Abwägung und im Übrigen zu bedenken, dass Kinder und Jugendliche nach den Vorgaben des europäischen Gesetzgebers einen besonderen Schutz beim Umgang mit ihren personenbezogenen Daten genießen, siehe auch Art. 8 DSGVO, Erwägungsgrund 38.

Zwar lässt sich eine Verarbeitung personenbezogener Daten auch auf eine Einwilligung stützen, Art. 6 Abs. 1 Buchst. a DSGVO. Indes steht es dem Verein nicht zu, über die Verarbeitung von Bild-, Video- und gegebenenfalls Audiodaten der betroffenen Personen, Schiedsrichter/innen, gegebenenfalls Trainer/innen und auch sichtbarer Zuschauer/innen sowie der Fußballspieler/innen, gerade wenn es sich um Kinder und Jugendliche handelt, zu entscheiden. Dem liegt das vom Bundesverfassungsgericht anerkannte individuelle Recht auf informationelle Selbstbestimmung, vgl. Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 Grundgesetz (GG), zugrunde. Dieses besagt, dass jede natürliche Person als Grundrechtsträger selbst über die Preisgabe und Verwendung sie betreffender personenbezogener Daten bestimmt. Dementsprechend kann der Verein auch nicht stellvertretend für die videografierten Personen eine Einwilligung in die Verarbeitung von Bild-, Video- und gegebenenfalls Tonaufnahmen geben!

Insoweit hätte die Einwilligung individuell erfolgen müssen. Zu vergegenwärtigen ist dabei, dass die Datenschutz-Grundverordnung bei minderjährigen betroffenen Personen strenge Anforderungen an die Einwilligung der Elternsorgeberechtigten als Vertreter stellt. Ungeachtet dessen scheidet die Einwilligungslösung bei einer Vielzahl von betroffenen Personen ohnehin aus rein praktischen bzw. tatsächlichen Gründen aus, müsste doch eine wirksame, die datenschutzrechtlichen Vorgaben beachtende Umsetzung aller betroffenen Personen – bei Kindern sämtlicher Erziehungsberechtigten – eingeholt werden.

Nur theoretisch denkbar gewesen wäre noch als Rechtfertigungsgrund die Wahrnehmung berechtigter Interessen durch den Verein, den Verantwortlichen, nach Art. 6 Abs. 1 Buchst. f DSGVO. Konkret ist in dieser Vorschrift nämlich auch ausdrücklich bestimmt, dass die Belange von Kindern besonders schwer wiegen und bei der notwendigen Interessenabwägung entsprechend zu berücksichtigen sind. Insoweit war schon nicht zu erkennen, wie sich die Videoaufnahmen damit hätten rechtfertigen lassen.

Im Ergebnis konnte so eine Rechtsgrundlage für die personengenaue Erfassung, Speicherung und anschließende Weiterverwendung der personenbezogenen Videodaten der Fußballspiele zu Zwecken der Auswertung nicht bejaht werden. Dem Verein habe ich ein dementsprechendes Ergebnis vermittelt.

Was ist zu tun?

Bei Sportveranstaltungen unter Beteiligung von Kindern ist bei Bildaufnahmen, insbesondere bei Videografie, besonderes Augenmerk auf eine belastbare Rechtsgrundlage der personenbezogenen Datenverarbeitung zu legen. Im Regelfall werden im Amateursportbereich viele betroffene minderjährige Personen einschließende Videoaufnahmen nicht datenschutzkonform umsetzbar sein.

2.4 Sensible Daten, besondere Kategorien personenbezogener Daten

2.4.1 Einsichtnahme der JVA in den zahnärztlichen Heil- und Kostenplan

↗ §§ 2 Nr. 14 Buchst. d, § 3 Abs. 4, 11 Abs. 4 SächsJVollzDSG

Der Gefangene in einer sächsischen Justizvollzugsanstalt (JVA) wandte sich an mich mit der Bitte um datenschutzrechtliche Prüfung des Umgangs mit seinem zahnärztlichen Heil- und Kostenplan innerhalb verschiedener Organisationseinheiten der JVA. Der Petent erläuterte, er habe auf seiner Station seinen Heil- und Kostenplan ohne Umschlag für eine zahnärztliche Behandlung zur Einsicht erhalten. In diesem Dokument war neben den Kosten auch sein medizinischer Befund aufgeführt. Mangels Umschlag sei der Heil- und Kostenplan für jeden Mitarbeiter, der damit in Berührung gekommen ist, einsehbar gewesen. Zudem hätten die Wirtschaftsverwaltung sowie die Zahlstelle der JVA Zuarbeiten geleistet, sodass auch diese Verwaltungsbereiche Kenntnis von seinem medizinischen Befund erlangt hätten. Der Petent sei weder vom Medizinischen Dienst noch anderweitig von der JVA im Vorfeld darüber informiert worden, welche Personen/Bereiche Zugriff auf seine Gesundheitsdaten haben werden. Eine entsprechende Einwilligung habe er ebenso wenig erklärt.

Nach § 63 Abs. 1 Sächsisches Strafvollzugsgesetz (SächsStVollzG) haben die Gefangenen einen Anspruch auf notwendige medizinische Leistungen unter Beachtung des Grundsatzes der Wirtschaftlichkeit nach dem allgemeinen Standard der gesetzlichen Krankenversicherung. Die Gesundheitsversorgung von Gefangenen wird durch die Justizvollzugsanstalten bereitgestellt. Kostenträger ist der Freistaat Sachsen. Ich habe die JVA um Stellungnahme sowie um Mitteilung der Erforderlichkeit sowie der Rechtsgrundlage für die Einsichtnahme der verschiedenen Organisationseinheiten in den medizinischen Befund gebeten. Die JVA übersandte ein

Musterformular der JVA für den Heil- und Kostenplan einer zahnärztlichen Versorgung, sodass ich konkret die einzelnen Mitwirkungen – und somit Einsichtnahmen – nachvollziehen konnte. Zunächst muss der behandelnde Zahnarzt umfassende medizinischen Daten zum Befund des gesamten Gebisses des Patienten sowie zur geplanten Behandlung eintragen. Anschließend erhalten folgende Organisationseinheiten das Formular: die E-/A-Stelle (Zahlstelle), die Vollzugsgeschäftsstelle, die Wirtschaftsverwaltung sowie bei einem Härtefallantrag die Anstaltsleitung zur Prüfung und Bearbeitung. Anschließend wird der Heil- und Kostenplan zur Eröffnung einem Stationsbediensteten der jeweiligen Vollzugsabteilung vorgelegt. Dabei haben die in diesen Stellen tätigen Bediensteten der JVA Einsicht in den Heil- und Kostenplan. Die Zahl- sowie die Vollzugsgeschäftsstelle tragen personenbezogene Daten des betroffenen Gefangenen ein, die fachlich keinen Bezug zur Gesundheitsversorgung haben (zum Beispiel, welche finanziellen Mittel dem Gefangenen zur Verfügung stehen und Daten zur Vollzugsdauer).

Aus datenschutzrechtlicher Sicht ist nicht nachvollziehbar, inwieweit diese Organisationseinheiten daher Einsicht in die medizinischen Befunde benötigen. Die Wirtschaftsverwaltung prüft im Anschluss die Kostenregulierung. Hierfür ist meines Erachtens lediglich der zahnärztliche Behandlungsplan erforderlich, nicht jedoch der komplette medizinische Befund. Schließlich erfolgt die Eröffnung des Heil- und Kostenplans gegenüber dem betroffenen Gefangenen durch einen Stationsbediensteten der jeweiligen Vollzugsabteilung, da dieser, so die JVA, nach dem Geschäftsverteilungsplan der JVA die Aufgabe habe, Daten und Fakten zur Entscheidungsfindung an den Gefangenen weiterzuleiten.

Ich habe die JVA darauf hingewiesen, dass es sich bei Gesundheitsdaten gemäß § 2 Nr. 14 Buchst. d SächsJVollzDSG um eine besondere Kategorie personenbezogener Daten handelt, deren Schutz nach § 3 Abs. 4 SächsJVollzDSG besonders zu garantieren ist. So regelt der Gesetzgeber in § 11 Abs. 4 SächsJVollzDSG, dass Gesundheitsakten und Therapieakten getrennt von anderen Unterlagen zu führen und gegen un-

befugten Zugang und unbefugten Gebrauch, das heißt, auch unbefugte Einsichtnahme, zu schützen sind. Zudem bestimmt § 39 Abs. 2 SächsJVollzDSG, dass die Justizvollzugsbehörden dafür Sorge zu tragen haben, dass sich ihre Bediensteten von personenbezogenen Daten nur Kenntnis verschaffen können, wenn dies zur Erfüllung der ihnen obliegenden Aufgaben oder sonst zur Erreichung des Vollzugsziels erforderlich ist, soweit nichts anderes geregelt ist.

Danach bedarf es zur Weiterleitung eines Heil- und Kostenplans keinesfalls der Kenntnisnahme personenbezogener Gesundheitsdaten durch den Stationsdienst. Ich habe die JVA aufgefordert, umgehend dafür zu sorgen, dass Stationsbedienstete den betroffenen Gefangenen Dokumente mit personenbezogenen Daten besonderer Kategorien ausschließlich in einem verschlossenen Umschlag übergeben. Notwendig ist insoweit natürlich auch, dass dem Stationsdienst diese Dokumente bereits in einem verschlossenen Umschlag übergeben werden. Die JVA hat die Umsetzung bereits bestätigt.

Aber auch hinsichtlich der Einsichtnahmen anderer Organisationseinheiten der JVA in den medizinischen Befund sehe ich weder eine Erforderlichkeit noch eine Rechtsgrundlage. In dem Musterformular der JVA finden sich Verfügungen zur Ablage und Aufbewahrung des Heil- und Kostenplans, welcher in der aktuellen Form medizinische Befunde enthält, außerhalb der Gesundheitsakten des betroffenen Gefangenen. Dies widerspricht der gesetzlichen Pflicht der JVA zur getrennten Führung von Gesundheits- und Therapieakten von anderen Unterlagen gemäß § 11 Abs. 4 SächsJVollzDSG. Die bislang mit der Kostenregulierung befassten Stellen der JVA hatten und haben kein Recht auf Einsichtnahme in die vollständigen medizinischen Befunde der Gefangenen.

Auch eine datenschutzrechtliche Belehrung des Petenten über die Offenbarungspflicht und -befugnis von Berufsgeheimnisträgern zum Haftantritt ließ vorliegend kein anderes Ergebnis zu. Zum einen umfasste die Belehrung explizit nicht § 48 Abs. 1 SächsJVollzDSG, wonach Berufsgeheimnisträgerinnen und Berufsgeheimnisträger nach § 46 Abs. 1 Satz 1

Nr. 1 bis 3 SächsJVollzDSG befugt sind, die ihnen im Rahmen des beruflichen Vertrauensverhältnisses anvertrauten oder sonst bekannt gewordenen personenbezogenen Daten der Anstaltsleitung zu offenbaren, soweit die Gefangenen einwilligen oder dies aus ihrer Sicht zu vollzuglichen Zwecken unbedingt erforderlich ist und das Interesse der Gefangenen an der Geheimhaltung nicht überwiegt. Eine ausdrückliche Einwilligung des Petenten lag gerade nicht vor. Zum anderen habe ich – wie erläutert – größte Zweifel an der unbedingten Erforderlichkeit der Kenntnisnahme der medizinischen Befunde im zahnärztlichen Heil- und Kostenplan durch die oben genannten Stellen der JVA zu vollzuglichen Zwecken, die zudem auch noch das Interesse des Gefangenen an der Geheimhaltung überwiegen müssten.

Die JVA hat meine datenschutzrechtlichen Einwände an das Sächsische Staatsministerium der Justiz (SMJus) zur weiteren Abstimmung übermittelt. Eine Rückmeldung seitens des SMJus lag bis zum Redaktionsschluss nicht vor.

Was ist zu tun?

Bei Gesundheitsdaten handelt es sich um personenbezogene Daten, deren Schutz besonders zu garantieren ist. So sind Gesundheitsakten und Therapieakten zwingend getrennt von anderen Unterlagen zu führen und gegen unbefugten Zugang und unbefugten Gebrauch, das heißt auch unbefugte Einsichtnahme, zu schützen.

3 Betroffenenrechte

3.1 Spezifische Pflichten des Verantwortlichen

3.1.1 Datenschutzrechtliche Beschwerden im Zusammenhang mit dem Gesetz über die Selbstbestimmung in Bezug auf den Geschlechtseintrag (SBGG)

↗ §§ 6, 13 SBGG

Am 1. November 2024 ist das Gesetz über die Selbstbestimmung in Bezug auf den Geschlechtseintrag (SBGG) in Kraft getreten. Das SBGG erleichtert es trans-, intergeschlechtlichen und nichtbinären Personen, ihren Geschlechtseintrag und ihre Vornamen ändern zu lassen. Die Änderung erfolgt durch eine Erklärung gegenüber dem Standesamt. Das Gesetz tritt an die Stelle des Transsexuellengesetzes (TSG) aus dem Jahr 1980. Eine gerichtliche Entscheidung über den Antrag ist nicht mehr erforderlich. Auch die Notwendigkeit zur Einholung zweier Sachverständigengutachten entfällt. In der Folge einer Änderung des Geschlechtseintrags und des Vornamens kommt es in Fällen, in denen das Geschlecht oder die Vornamen einer Person rechtlich relevant sind, nur auf den jeweils aktuellen Geschlechtseintrag und auf aktuell eingetragene Vornamen an. Im Berichtszeitraum wandten sich zwei Personen mit Beschwerden an mich, die im Zusammenhang mit dem SBGG stehen.

Im ersten Fall erhielt die Person nach Änderung des Vornamens gemäß dem SBGG ein Schreiben des Gerichtsvollziehers unter Verwendung des abgelegten Vornamens und

sah darin einen Verstoß gegen § 6 Abs. 1 SBGG, wonach der jeweils aktuelle Geschlechtseintrag und die jeweils aktuellen Vornamen im Rechtsverkehr maßgeblich sind, soweit auf die personenstandsrechtliche Geschlechtszuordnung oder die Vornamen Bezug genommen wird und durch Gesetz nichts anderes bestimmt ist.

Nach § 57 Abs. 4 Nr. 4 Personenstandsverordnung (PStV) informiert das zuständige Standesamt unmittelbar das Melderegister über die Beurkundung der Änderung des Geschlechtseintrags und des Vornamens. Die Meldebehörden unterrichten ihrerseits nach Fortschreibung des Melderegisters die Datenempfänger des Meldewesens, soweit die einschlägigen Rechtsvorschriften eine Mitteilung aus Anlass der Änderung des Vornamens bzw. Geschlechtseintrags vorsehen. Solche regelmäßigen Datenübermittlungen an andere öffentliche Stellen, die ohne Ersuchen in allgemein bestimmten Fällen regelmäßig wiederkehrend durchgeführt werden, sind allerdings nur zulässig, soweit dies durch Bundes- oder Landesrecht bestimmt ist. Gerichtsvollzieher/innen werden seitens des Sächsischen Melderegisters nicht automatisch über die Änderung des Geschlechtseintrags und des Vornamens informiert. Die Sächsische Meldedaten-Übermittlungsverordnung (SächsMeldDÜVO) regelt solche regelmäßigen Datenübermittlungen abschließend nur für Übermittlungen an das Statistische Landesamt, die Sächsische Staatskanzlei, das Landeskriminalamt und öffentlich-rechtliche Religionsgesellschaften (unter den jeweils genannten Voraussetzungen). Zwar haben sächsische Behörden die Möglichkeit, personenbezogene Daten im Sächsischen Melderegister im Einzelfall abzurufen, zugleich ist es ihnen aber nicht zuzumuten und nach dem Grundsatz der Datenminimierung auch nicht erforderlich, sich vor jedem Schreiben an Personen über deren aktuellen Geschlechtseintrag und Vornamen zu informieren.

Ich habe die beschwerdeführende Person um Mitteilung gebeten, ob sie nach der Änderung des Vornamens den Gerichtsvollzieher entsprechend über die Änderung der Daten informiert habe, denn nur in diesem Fall wäre das Anschrei-

ben unter dem abgelegten Vornamen ein Datenschutzverstoß gewesen. Darauf erhielt ich keine Rückmeldung.
Im zweiten Fall beschwerte sich eine Person ebenfalls über einen sächsischen Gerichtsvollzieher, welcher ihr ein Schreiben unter Verwendung ihres abgelegten Vornamens sowie Geschlechts zugestellt habe. Nach Prüfung des mir vorliegenden Schreibens konnte ich zunächst feststellen, dass der Gerichtsvollzieher bezüglich der Anschrift die aktuellen Personendaten der beschwerdeführenden Person verwendete. Im Schreiben selbst wurden die personenbezogenen Daten aufgeführt, unter welchen der Eintrag im Schuldnerverzeichnis gemäß § 882 b Abs. 2 Zivilprozessordnung (ZPO) der beschwerdeführenden Person angelegt worden war, darunter der derzeitige Vorname sowie der frühere Vorname.
Dies stellt keinen Verstoß gegen § 13 SBGG (Offenbarungsverbot) dar. Nach § 13 Abs. 3 SBGG steht das Offenbarungsverbot einer weiteren Verarbeitung der bis zur Änderung des Geschlechtseintrags und der Vornamen in amtlichen Registern oder Informationssystemen enthaltenen Angaben nicht entgegen. Amtliche Register und amtliche Informationssysteme dürfen zur Nachvollziehbarkeit der Identität von Personen die bis zur Änderung des Geschlechtseintrags und der Vornamen eingetragenen Angaben verarbeiten, (auch) wenn andere Rechtsvorschriften eine Verarbeitung (nur) der aktuellen Daten vorsehen. Rechtsgrundlage für die Verarbeitung der aktuellen Daten der beschwerdeführenden Person im Schuldnerverzeichnis ist § 882b Abs. 2 Zivilprozessordnung (ZPO). § 13 Abs. 3 SBGG erweitert die jeweils vorhandene Befugnis in Bezug auf die bisherigen Daten, ohne dass die anderen Rechtsvorschriften selbst eine solche Befugnis in Bezug auf die bisherigen Daten vermitteln müssen (BT-Drs. 20/9049, S. 56).

Was ist zu tun?
Die Änderung von Geschlechtseintrag und Vornamen einer Person führt nicht zwingend dazu, dass die Verarbeitung des früheren Geschlechts und abgelegter Vornamen eine Verarbeitung unrichtiger Daten oder rechtswidrig wäre. Das Offenbarungsverbot greift nur, wenn die Änderung bekannt ist. Für amtliche Register, Informationssysteme und Dokumente sieht das Gesetz hinsichtlich der vor der Änderung erfolgten Verarbeitungen Ausnahmen vor.

3.1.2 Informationspflichten beim „Kauf auf Rechnung"

↗ Art. 13 Abs. 1 Buchst. e DSGVO, Art. 14 Abs. 1 Buchst. e DSGVO in Verbindung mit Art. 14 Abs. 3 Buchst. c DSGVO

Werden personenbezogene Daten durch einen Verantwortlichen direkt oder durch einen Dritten bei der betroffenen Person erhoben, obliegen dem Verantwortlichen Informationspflichten, welche im Einzelnen in Art. 13 und Art. 14 DSGVO geregelt sind. Zu den Informationspflichten gehört unter anderem eine Mitteilung darüber, ob und an wen erhobene personenbezogene Daten weitergeleitet werden sollen (vgl. Art. 13 Abs. 1 Buchst. e sowie Art. 14 Abs. 1 Buchst. e DSGVO). Die Informationspflichten der Art. 13 und 14 DSGVO gelten sowohl bei der Online- als auch der analogen Datenverarbeitung.

Die Nichteinhaltung der datenschutzrechtlichen Informationspflichten durch einen Verantwortlichen im Zusammenhang mit einer Bestellung im Internet war Gegenstand einer Prüfung, die ich infolge einer bei mir eingegangenen Beschwerde vorgenommen hatte. Der Beschwerdeführer hatte auf einer Internetplattform, die von einem Dritten und nicht vom Verkäufer betrieben wird, eine Bestellung abgegeben. Von den auf der Plattform angegebenen Alternativen zur Zahlung des Kaufpreises hatte der Beschwerdeführer einen „Kauf auf Rechnung" ausgewählt, wobei er offenbar davon ausgegangen war, dass er mit oder nach der Lieferung seiner Bestellung eine Rechnung vom Verkäufer erhält, die er dann bei seinem Kreditinstitut zur Zahlung anweisen kann.

Tatsächlich erhielt der Beschwerdeführer zunächst vom Verkäufer eine E-Mail mit der Mitteilung, dass dieser die Bestellung des Beschwerdeführers annimmt. Zur Zahlung des Kaufpreises hatte die E-Mail des Verkäufers einen Link zu einem Zahlungsdienstleister mit Sitz in der Europäischen Union enthalten, der die Abwicklung des „Kaufs auf Rechnung" für den Verkäufer übernommen hatte. Gegenüber dem Zahlungsdienstleister war unter dem Link unter anderem der Name und die Anschrift durch den Beschwerdeführer selbst noch einmal einzugeben.

Im Anschluss an die E-Mail des Verkäufers erhielt der Beschwerdeführer noch eine Bestellbestätigung des Betreibers der Internetplattform, der auch eine Datenschutzerklärung des Verkäufers beigefügt war.

Der Beschwerdeführer hatte in seiner Beschwerde die Weitergabe seiner Bestelldaten an den Zahlungsdienstleister durch den Verkäufer beanstandet, weil er hierüber nicht in Kenntnis gesetzt worden sei. Auch hätte er vor der Abgabe seiner Bestellung keine Informationen dazu erhalten, dass der Zahlungsdienstleister Teil des Bestellprozesses sein wird.

Für den Verkäufer bestand aus meiner Sicht zunächst keine Informationspflicht nach Art. 13 DSGVO, da dieser selbst im Zusammenhang mit der Abgabe der Bestellung durch den Beschwerdeführer keine personenbezogenen Daten von diesem erhoben hatte. Der Betreiber der Internetplattform, auf der der Beschwerdeführer seine Bestellung abgegeben hatte, hat in seiner Datenschutzerklärung angegeben, dass er der Verantwortliche für die Erhebung von personenbezogenen Daten auf der Plattform ist.

Für den Verkäufer als die nicht erhebende Stelle bestand aber gleichwohl eine Informationspflicht nach Art. 14 Abs. 1 Buchst. e DSGVO, da er personenbezogene Daten des Beschwerdeführers an einen weiteren Empfänger, hier den Zahlungsdienstleister, übermittelt hatte.

Der Verkäufer erklärte zwar gegenüber meiner Behörde, dass er keine Daten aus der Bestellung weitergegeben hätte; durch ihn wäre lediglich die von ihm vergebene Auftragsnummer sowie der zu zahlende Betrag an den Zahlungsdienstleister übermittelt worden. Bei der vom Verkäufer zu der Bestellung generierten und übermittelten Auftragsnummer handelte es sich aber gleichwohl um eine personenbezogene Information im Sinne von Art. 4 Nr. 1 DSGVO, da der Beschwerdeführer mit den Angaben, wie Name und Anschrift, die er auf der Internetseite des Zahlungsdienstleisters nochmals einzugeben hatte, auf die ihn der Link verwies, sowohl für den Verkäufer als auch für den Zahlungsdienstleister identifizierbar gewesen war.

Seiner datenschutzrechtlichen Informationspflicht über eine (mögliche) Weitergabe der personenbezogenen Daten des

Beschwerdeführers nach Art. 14 Abs. 1 Buchst. e DSGVO war der Verkäufer gegenüber dem Beschwerdeführer nachgekommen, da diesem mit der Bestellbestätigung des Inhabers der Internetplattform die Datenschutzerklärung des Verkäufers übersandt wurde. In der Datenschutzerklärung wurde in Abhängigkeit der gewählten Zahlungsart auf eine mögliche Weiterleitung von Zahlungsdaten an Dritte ausdrücklich hingewiesen.

Diese Information hatte der Beschwerdeführer aber erst erhalten, nachdem die Auftragsnummer an den Zahlungsdienstleister übermittelt worden war. Dies war verspätet, denn nach Art. 14 Abs. 3 Buchst. c DSGVO hat die Offenlegung von nicht selbst erhobenen personenbezogenen Daten gegenüber weiteren Empfängern spätestens zum Zeitpunkt der ersten Offenlegung zu erfolgen.

Infolge meiner Feststellung wurde der Verkäufer von mir aufgefordert, seinen Bestellprozess zu überprüfen und so anzupassen, dass seine Kunden rechtzeitig über eine Weitergabe der sie betreffenden personenbezogenen Daten an einen vom Verkäufer beauftragten Zahlungsdienstleister informiert werden.

Die Beschwerde betraf aber noch einen zweiten Punkt, nämlich die Frage, ob für den Verkäufer als Anbieter auf der Internetplattform - aus datenschutzrechtlicher Sicht - auch eine Verpflichtung bestand, den Beschwerdeführer schon bei der Abgabe seiner Bestellung über den Ablauf des „Kaufs auf Rechnung" im Einzelnen zu informieren. Dies habe ich aus Datenschutzsicht verneint, weil die DSGVO hierzu keine Regelungen vorsieht. Der Europäische Gerichtshof hat jedoch in seiner Entscheidung vom 15. Mai 2025, Az. C-100/24, festgestellt, dass es sich bei der Angabe eines „Kaufs auf Rechnung" im Internet um eine verkaufsfördernde Maßnahme im Sinne von Art. 6 Buchst. c RL 2000/31/EG (E-Commerce-Richtlinie) handelt, die entsprechende Aufklärungs- und Transparenzpflichten für die Anbieter zur Folge haben kann. Deren Einhaltung wäre jedoch zivil- bzw. wettbewerbsrechtlich zu klären, nicht aber durch meine Behörde. Hierauf wurde der Beschwerdeführer durch mich hingewiesen.

Was ist zu tun?
Anbieter/innen im Internet haben bei der Option „Kauf auf Rechnung" vor einer Datenweitergabe datenschutzrechtliche Informationspflichten zu beachten. Weitergehende Informationspflichten zivilrechtlicher Art sind kein Gegenstand datenschutzaufsichtlicher Prüfung.

3.1.3 Öffentliche Zustellungen und Ermittlungspflichten der Behörde

↗ §§ 1 und 2 SächsVwVfZG; § 10 VwZG

Tätigkeitsbericht Datenschutz 2022:
↗ sdb.de/tb2022

Ich hatte bereits im Tätigkeitsbericht Datenschutz 2022 (3.1.1, Seite 114 ff.) ausführlich zu den Voraussetzungen und dem Prozedere öffentlicher Zustellungen berichtet. Diese Problematik ist deswegen datenschutzrechtlich so relevant, weil mit öffentlicher Zustellung unweigerlich die Veröffentlichung von Namen (und meist letztbekannter Anschrift) einhergeht. Das Gros der öffentlichen Zustellungen findet darüber hinaus mittlerweile im Internet statt – sie sind somit weltweit abrufbar. Es sind deswegen eine sehr restriktive Handhabung und insbesondere eine besondere Sorgfalt bei der Ermittlung durch die jeweils zuständige Behörde anzusetzen.

Im Berichtszeitraum wandte sich ein Petent an mich, nachdem ihm bekannt wurde, dass eine öffentliche Zustellung gegen seine Person im kommunalen Amtsblatt erfolgte. Er teilte mit, dass ihm dies nicht erklärlich sei, da er seit vielen Jahren an derselben Anschrift wohnhaft sei und postalisch immer zu erreichen war. Die Anschrift sei der zustellenden Behörde auch bekannt gewesen.

Meine daraufhin erfolgte Prüfung mit Anhörung der betreffenden Gemeinde und Unterstützung des behördlichen Datenschutzbeauftragten hat ergeben, dass die ursprüngliche Zustellung deswegen keinen Erfolg hatte, da bei der Adressangabe der betreffende Ortsteil fehlte und der Brief deswegen als nicht zustellbar zurückkam. Da sämtliche sonstigen Angaben Straße, Ort, Postleizahl stimmten, handelte es sich offenbar um einen Fehler des Postzustellers.

Es wurde daraufhin eine Melderegisterauskunft eingeholt. Diese bestätigte grundsätzlich die verwendete Anschrift, wobei zusätzlich der betreffende (bis dahin nicht aufgeführte) Ortsteil bezeichnet war. Einen erneuten Zustellversuch hat die Behörde dennoch nicht unternommen, sondern sogleich die öffentliche Zustellung angeordnet. Damit wurden Name, Wohnort der betroffenen Person und auch die Art des Bescheides (es handelte sich um einen Steuerbescheid, was

den Vorfall noch brisanter machte) daraufhin im Amtsblatt gemäß §§ 1 und 2 Gesetz zur Regelung des Verwaltungsverfahrens- und des Verwaltungszustellungsrechts für den Freistaat Sachsen (SächsVwVfZG) in Verbindung mit § 10 Verwaltungszustellungsgesetz (VwZG) veröffentlicht.

Dieses Vorgehen ist nicht datenschutzgerecht. Ich möchte aus diesem Anlass alle sächsischen Gemeinden und Landkreise darauf hinweisen, besondere Sorgfalt bei der Prüfung der Zustellbarkeit von Bescheiden walten zu lassen.

Gemäß § 10 Abs. 1 Nr. 1 VwZG ist eine öffentliche Zustellung nämlich nur dann zulässig, wenn der Aufenthaltsort des Empfängers unbekannt ist und eine Zustellung auf andere Weise nicht möglich ist. Diese Voraussetzung ist wegen der Tragweite der Veröffentlichung immer restriktiv auszulegen. Dies bedeutet insbesondere, dass die Behörde zunächst alle ihr zumutbaren Ermittlungsmaßnahmen zur Feststellung des Aufenthaltsortes ausschöpfen muss. Dazu gehört immer die Einholung einer aktuellen Melderegisterauskunft, bei Anhaltspunkten auch ein erneuter Zustellversuch (vorliegend beispielsweise mit präziser Adresse unter Berücksichtigung des Ortsteils), Internetrecherche, aber auch Vor-Ort-Ermittlungen (auch unter Hinzuziehung von Amtshilfe, wenn die Zustelladresse nicht im eigenen Einzugsgebiet liegt). Diese Maßnahmen sind grundsätzlich als zumutbar im Sinne von § 10 Abs. 1 Nr. 1 VwZG zu werten.

Der Inhalt der Benachrichtigung der öffentlichen Zustellung ergibt sich zudem ausschließlich aus der Vorschrift des § 10 Abs. 2 VwZG. Dazu gehört die zustellende Behörde, Namen und die letzte bekannte Anschrift des Adressaten, das Datum und das Aktenzeichen des Dokuments, die Stelle, bei der das Dokument eingesehen werden kann, sowie der Hinweis, dass das Dokument öffentlich zugestellt wird (und Fristen in Gang gesetzt werden können, nach deren Ablauf Rechtsverluste drohen können). Darüber hinausgehende Angaben – insbesondere zur inhaltlichen Bezeichnung des Verwaltungsakts – sind nach dem Gesetzeswortlaut ausdrücklich nicht (mehr) zulässig. Somit war auch die gewählte Bezeichnung des Bescheides nicht zulässig.

Zudem ist auch dringend zu beachten, dass die Veröffentlichung nur bis Zweckerreichung zulässig ist. Erfolgt die Bekanntmachung einer öffentlichen Zustellung elektronisch, ist die Löschung nach zwei Wochen zu veranlassen. Nach § 10 Abs. 2 VwZG tritt dann nämlich die Fiktion der Zustellung ein, sodass zu diesem Zeitpunkt auch der Zweck erreicht wird. Zur Bündelung des Verwaltungsaufwandes kann ein Karenzaufschlag von zwei bis maximal vier weiteren Wochen zugebilligt sein, um gebündelt abgelaufene Zustellungsbenachrichtigungen zu löschen.

Was ist zu tun?
Gemeinden und Landkreise sind zur besonderen Sorgfalt bei der Prüfung und Umsetzung öffentlicher Zustellungen aufgefordert.

3.2 Auskunftsrecht

3.2.1 Auskunft nach Art. 15 DSGVO und Akteneinsicht

↗ § 25 SGB X, § 83 SGB X, Art. 15 DSGVO

Ein Petent rügte, dass ihm ein Sozialleistungsträger keine Auskunft nach Art. 15 DSGVO und keine kostenlose Kopie seiner personenbezogenen Daten gemäß Art. 15 Abs. 3 DSGVO gewährt habe, obwohl er dies beantragt habe. Angeboten worden sei ihm unter Verweis auf § 25 Zehntes Buch Sozialgesetzbuch (SGB X) lediglich die Möglichkeit der Akteneinsicht oder eine kostenpflichtige Aktenkopie.
Der Petent hatte Auskunft nach Art. 15 DSGVO und nicht Akteneinsicht beantragt. Der Bundesfinanzhof (BFH) hat mit Urteil vom 12. November 2024, IX R 20/22, entschieden, dass das Auskunftsrecht gemäß Art. 15 DSGVO inhaltlich nicht mit einem Akteneinsichtsrecht vergleichbar ist.
Das verwaltungsverfahrensrechtliche Akteneinsichtsrecht nach § 25 SGB X dient der Durchsetzung des Rechts auf ein faires Verfahren beziehungsweise des Anspruchs auf rechtliches Gehör und somit der „Waffengleichheit" im Rahmen eines konkreten laufenden Verwaltungsverfahrens. Daher heißt es in Absatz 1 der Vorschrift auch: „Die Behörde hat den Beteiligten Einsicht in die das Verfahren betreffenden Akten zu gestatten, soweit deren Kenntnis zur Geltendmachung oder Verteidigung ihrer rechtlichen Interessen erforderlich ist."

Das Akteneinsichtsrecht nach § 25 SGB X erlischt daher auch, wenn das jeweilige Verwaltungsverfahren abgeschlossen ist. Andererseits ermöglicht das Akteneinsichtsrecht nach § 25 SGB X auch die Kenntnisnahme von Daten Dritter.
Davon zu unterscheiden ist der datenschutzrechtliche Auskunftsanspruch des Betroffenen nach Artikel 15 DSGVO in Verbindung mit § 83 SGB X, der aus dem Recht auf informationelle Selbstbestimmung hergeleitet wird.
Der Petent hatte in seinem Schreiben eindeutig gegenüber dem Sozialleistungsträger dargelegt, dass es sich um einen Antrag nach Artikel 15 Abs. 3 DSGVO handelt und nicht um ein Ersuchen nach § 25 SGB X. Für eine „Umdeutung" des Antrags des Petenten, wie es durch den Sozialleistungsträger erfolgte, ist mithin kein Raum.
Der Sozialleistungsträger wurde von mir darauf hingewiesen, dem Auskunftsantrag nach Art. 15 DSGVO unverzüglich nachzukommen. Dies erfolgte dann umgehend.

Was ist zu beachten?
Ein Antrag auf Auskunft nach Art. 15 Abs. 3 DSGVO ist inhaltlich nicht mit einem Antrag auf Akteneinsicht vergleichbar.

3.2.2 Änderung der Regelungen zur Kostenerstattung für Kopien aus der Patientenakte in den Berufsordnungen der Heilberufskammern

↗ § 630g BGB, Art. 15 DSGVO, § 10 Abs. 2 (Muster-)Berufsordnung – Ärzte

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 11. September 2024 hat folgende Entschließung gefasst: „Recht auf kostenlose Erstkopie der Patientenakte kann durch eine nationale Regelung nicht eingeschränkt werden! Datenschutzaufsichtsbehörden sehen konkreten Handlungsbedarf auf Seiten der Heilberufskammern."
Darin nehmen die deutschen Aufsichtsbehörden Bezug auf das Urteil des Europäischen Gerichtshofs (EuGH) vom 26. Oktober 2023, C-307/22. Mit diesem Urteil hat sich der EuGH zum Verhältnis des Rechts auf Einsicht in die Patientenakte aus § 630g Bürgerliches Gesetzbuch (BGB) und des Rechts auf Kopie personenbezogener Daten aus Art. 15 Abs. 3 DSGVO geäußert.

Tätigkeitsbericht Datenschutz 2024:
↗ sdb.de/tb2024

Das Gericht stellte fest, dass der/die Patient/in einen Anspruch auf eine unentgeltliche erste Kopie seiner oder ihrer Akte hat. Durch eine nationale Regelung wie § 630g Abs. 2 Satz 2 BGB darf dem Patienten oder der Patientin keine Kostenlast hierfür auferlegt werden. Der Verantwortliche kann jedoch für alle weiteren Kopien ein angemessenes Entgelt auf Grundlage der Verwaltungskosten verlangen. In meinem Tätigkeitsbericht Datenschutz 2024 (9.5, Seite 277 f.) hatte ich mich mit dem Urteil befasst.

In der Entschließung weisen die deutschen Aufsichtsbehörden darauf hin, dass nach dem Urteil des EuGH nicht nur dringender Handlungsbedarf für den Bundesgesetzgeber besteht, § 630g Abs. 2 Satz 2 BGB den Vorgaben der DSGVO anzupassen. Auch die Berufsordnungen der Heilberufskammern enthalten regelmäßig entsprechende Regelungen zur Kostenerstattung für die Herausgabe von Kopien aus der Patientenakte (vergleiche § 10 Abs. 2a Muster-Berufsordnung der Bundesärztekammer), die den Vorgaben der DSGVO und der Rechtsprechung des EuGH widersprechen.

In der Entschließung wird weiter ausgeführt: „Während der Bundesgesetzgeber eine Änderung des BGB noch in dieser Legislaturperiode vornehmen wird, ist offen, ob und gegebenenfalls wann es auch zu den notwendigen berufsrechtlichen Anpassungen kommen wird."

Auf die Entschließung hin habe ich die Sächsische Landesärztekammer, die Landeszahnärztekammer und die Ostdeutsche Psychotherapeutenkammer um Mitteilung gebeten, wie sie verfahren.

Die Landeszahnärztekammer Sachsen plant, bei einer zukünftigen Änderung der Berufsordnung für die Zahnärzte im Freistaat Sachsen die Thematik entsprechend zu berücksichtigen. Die Ostdeutsche Psychotherapeutenkammer informierte, dass eine Änderung der (Muster-)Berufsordnung (MBO) auf Bundesebene abgewartet wurde. Nachdem im November 2025 vom Deutschen Psychotherapeutentag (DPT) entsprechende Änderungen beschlossen wurden, wird in der nächsten Vorstandssitzung der Ostdeutschen Psychotherapeutenkammer Mitte Dezember 2025 über eine rasche Umsetzung

Was ist zu tun?
Auch in den Berufsordnungen der Heilberufskammern ist zu berücksichtigen, dass eine Erstkopie der Patientenakte bei der Auskunft nach Art. 15 Abs. 3 DSGVO kostenlos zu erteilen ist.

beraten werden. Die Sächsische Landesärztekammer wartet die Änderung des § 10 Abs. 2 der (Muster-)Berufsordnung – Ärzte durch die Bundesärztekammer ab und beabsichtigt dann zeitnah regelungsgleich auch die Berufsordnung der Sächsischen Landesärztekammer abzuändern.

3.2.3 Herausgabe von Zugriffsdaten bei einem Mitarbeiterexzess

↗ Art. 15 Abs. 1 DSGVO, Art. 82 DSGVO, § 22 SächsDSDG

Im Berichtszeitraum kam es wiederholt zu Beschwerden im öffentlichen Bereich, mit dem Vortrag, Bedienstete von Kommunen hätten Daten von Betroffenen in der einen oder anderen Weise (privat) verarbeitet und/oder an Dritte weitergegeben. Im kommunalen Bereich haben beispielsweise Mitarbeiter/innen der Meldeämter Zugriffsmöglichkeit auf eine große Datenmenge mitunter sensibler Daten.
Ein Mitarbeiterexzess liegt immer dann vor, wenn Mitarbeiter/innen nicht (mehr) in dem ihnen zugewiesenen Aufgaben- und Befugnisbereich tätig sind und hierbei eigenmächtig personenbezogene Daten verarbeiten.
Folge dessen ist, dass die datenschutzrechtliche Verantwortlichkeit, aber auch die Haftung auf Schadensersatz aufgrund Datenschutzverletzung nach Art. 82 DSGVO sich von der Behörde auf den bzw. die Bedienstete selbst verlagert. Entsteht der betroffenen Person tatsächlich ein Schaden, haftet der bzw. die Bedienstete hierfür persönlich. Dies hat der Europäische Gerichtshof (EuGH) in einer umfassend begründeten Entscheidung bestätigt (EuGH, Urteil vom 22. Juni 2023, Az.: C-579/21 (Pankki S.).
Auch mit Bußgeldverfahren (Art. 83 DSGVO) ist zu rechnen, bei nachgewiesener Bereicherungsabsicht auch mit strafrechtlicher Verfolgung, siehe § 22 Sächsisches Datenschutzdurchführungsgesetz (SächsDSDG). Außerhalb des Datenschutzrechtes kommen auch arbeits- bzw. dienstrechtliche Sanktionen seitens des Dienstherrn in Betracht, bis hin zur Kündigung/Entlassung.

Damit die betroffene Person aber in die Lage versetzt werden kann, die ihr zustehenden Ansprüche geltend zu machen, steht ihr ein Auskunftsanspruch gegen die Behörde zu: In diesen Fällen hat die Behörde auch den Namen des/der Bediensteten zu offenbaren. Der Schutz dieser Daten (Art. 15 Abs. 4 DSGVO) muss hinter den Auskunftsanspruch zurücktreten. Zu beauskunften sind grundsätzlich auch die Protokolldaten der Zugriffe.
Hierzu hat der EuGH in oben genannter Entscheidung umfassend ausgeführt:

> „Art. 15 Abs. 1 der Verordnung 2016/6789 ist dahin auszulegen, dass Informationen, die Abfragen personenbezogener Daten einer Person betreffen und die sich auf den Zeitpunkt und die Zwecke dieser Vorgänge beziehen, Informationen darstellen, die die genannte Person nach dieser Bestimmung von dem Verantwortlichen verlangen darf. Dagegen sieht diese Bestimmung kein solches Recht in Bezug auf Informationen über die Identität der Arbeitnehmer dieses Verantwortlichen vor, die diese Vorgänge unter seiner Aufsicht und im Einklang mit seinen Weisungen ausgeführt haben, außer wenn diese Informationen unerlässlich sind, um der betroffenen Person es zu ermöglichen, die ihr durch diese Verordnung verliehenen Rechte wirksam wahrzunehmen, und vorausgesetzt, dass die Rechte und Freiheiten dieser Arbeitnehmer berücksichtigt werden. […]
>
> Was konkret die Protokolldateien des Verantwortlichen betrifft, so kann sich die Bereitstellung einer Kopie der in diesen Dateien enthaltenen Informationen als erforderlich erweisen, um der Pflicht nachzukommen, der betroffenen Person alle in Art. 15 Abs. 1 DSGVO genannten Informationen zugänglich zu machen, und um eine faire und transparente Verarbeitung zu gewährleisten. So wird es der fraglichen Person ermöglicht, die ihr nach dieser Verordnung gewährten Rechte in vollem Umfang geltend zu machen.

> Erstens lassen solche Dateien nämlich auf das Bestehen einer Datenverarbeitung schließen: Hierbei handelt es sich um eine Information, die der betroffenen Person nach Art. 15 Abs. 1 DSGVO zugänglich sein muss. Außerdem geben sie Auskunft über Häufigkeit und Intensität der Abfragen und ermöglichen es mithin der betroffenen Person, zu überprüfen, ob der ausgeführten Verarbeitung tatsächlich die von dem Verantwortlichen angegebenen Zwecke zugrunde liegen.
> Zweitens enthalten diese Dateien Informationen über die Identität der Personen, die die Abfragen vorgenommen haben."

Somit erfährt der vom EuGH bestätigte Grundsatz, dass über die Identität der Beschäftigten, die rechtmäßig und im Rahmen der dienstlichen Weisungen Daten abgerufen haben, keine Auskunft nach Art. 15 DSGVO zu erteilen ist, eine Ausnahme: in Fällen des Mitarbeiterexzesses. In diesen Fällen benötigt die betroffene Person die Identitätsangabe, um etwaige Betroffenenrechte und andere Ansprüche geltend zu machen. Auch zur Ordnungswidrigkeits- und Strafverfolgung benötigen die Behörden die Angabe der Identität des bzw. der Bediensteten. Die Stellen dürfen diese Angaben nicht verweigern.
Auch treffen die Behörde in diesen Fällen Aufklärungs- und Ermittlungspflichten. Jüngst hatte eine Behörde bei einem vermeintlichen Mitarbeiterexzess darauf verwiesen, die betroffene Person habe eine Datenschutzverletzung nicht zureichend bewiesen und vorgetragen. Dem ist nicht zu folgen: Wenn vielmehr der Anfangsverdacht einer rechtswidrigen Datenverarbeitung vorliegt und plausibel erscheint, kann die Beweislast nicht auf die betroffene Person übertragen werden, sondern ist von der Behörde selbst zu tragen.

Was ist zu tun?
Verantwortliche haben in Fällen des Mitarbeiterexzesses bei Auskünften an betroffene Personen auch die Identität des Mitarbeiters bzw. der Mitarbeiterin preiszugeben.

3.2.4 Auskunftsanspruch nach Identitätsdiebstahl in einem grenzüberschreitenden Verfahren – ein Beispiel für die Herausforderungen in der europäischen Zusammenarbeit

↗ Art. 15, 56 DSGVO

Immer wieder gibt es grenzüberschreitende Fälle, in denen Beschwerdeführer/innen erst anhand der Steuererklärung bemerken, dass jemand ohne ihr Wissen in ihrem Namen Gewinne macht, sei es, beim Glücksspiel oder mit Wertpapieren. In einem Fall erhielt ein Beschwerdeführer von seinem Finanzamt einen Einkommenssteuerbescheid für 2021, in dem Kapitalerträge aus einem Konto beim Verantwortlichen in Höhe von über 40.000 Euro berücksichtigt waren. Da der Beschwerdeführer niemals ein Konto bei dem Verantwortlichen gehabt hatte, erhob er Einspruch gegen den Steuerbescheid. Da er einen Identitätsdiebstahl befürchtete, stellte er einen Antrag auf Auskunft nach Art. 15 DSGVO beim Verantwortlichen, der auch nach Wiederholung nicht beantwortet wurde. Deshalb erhob der Beschwerdeführer im Januar eine Beschwerde bei einer anderen europäischen Aufsichtsbehörde, in deren Zuständigkeitsbereich die Hauptniederlassung des Verantwortlichen fiel, wegen Verletzung von Art. 15 Abs. 3 DSGVO. Diese wies ihn darauf hin, dass er Beschwerde „bei der deutschen Datenschutzbehörde BfDI" erheben könne, damit er gegebenenfalls vor einem deutschen Gericht klagen könne; falls sie innerhalb eines Monats nichts mehr von ihm hören sollten, würden sie den Fall abschließen. Daraufhin reichte er beim Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) eine Beschwerde ein, die Anfang März an mich abgegeben wurde.

Mitte April wurde die Beschwerde in einem Verfahren zur Bestimmung der federführenden und betroffenen Aufsichtsbehörden nach Art. 56 DSGVO in IMI, dem EU-Binnenmarktinformationssystem, eingestellt und die oben genannte europäische Aufsichtsbehörde als mutmaßlich federführende Aufsichtsbehörde bezeichnet. Nach kurzer Zeit merkte diese

an, dass sie den Fall prüfen wolle und sich rechtzeitig wieder melden würde. Dies geschah nicht vor Ablauf der Eintragungsfrist. Nach der technischen Schließung des Verfahrens wäre eine Meldung der federführenden Aufsichtsbehörde nicht mehr möglich gewesen, und die nach Art. 56 DSGVO zuständige Aufsichtsbehörde hätte den Fall nicht übernommen; mangels Zuständigkeit hätte aber auch ich in dem Verfahren nicht tätig werden können. Drei Wochen vor der technischen Schließung des Verfahrens sandte ich eine E-Mail an die zuständige Aufsichtsbehörde und wies auf die Dringlichkeit wegen eines etwaigen steuerliches Verfahrens und des Verdachts einer Straftat gegen den Beschwerdeführer hin. Darauf erhielt ich eine kurze Mitteilung, dass die Anfrage zur Beantwortung an das Team für grenzüberschreitende Fälle abgegeben wurde. Eine Woche vor der technischen Schließung des Verfahrens startete ich ein Verfahren der allgemeinen Amtshilfe nach Art. 61 DSGVO in IMI und bat unter Beteiligung der anderen sieben betroffenen Aufsichtsbehörden die oben genannte europäische Aufsichtsbehörde, sich schnellstmöglich als federführende Aufsichtsbehörde zu erklären. Ein Kommentar in IMI verwies erneut auf das Team für grenzüberschreitende Fälle. Erst acht Stunden vor der technischen Schließung des Verfahrens erklärte sich die oben genannte europäische Aufsichtsbehörde zur federführenden Aufsichtsbehörde und entschuldigte die Verspätung mit einer Rückmeldung des Verantwortlichen zu ihrer Anfrage erst vor drei Wochen.

Die Erleichterung hielt nicht lange an. Am selben Tag stellte die oben genannte europäische Aufsichtsbehörde ein Amtshilfeerfahren nach Art. 61 DSGVO in IMI ein, in dem sie mitteilte, dass sie das Verfahren mangels Betroffenheit des Beschwerdeführers einstellen wolle, da es in dem Verfahren nicht um die Auskunft über personenbezogene Daten des Beschwerdeführers ging, sondern um die des Identitätsdiebes. Ich erwiderte darauf, dass auch nachdem ein Verantwortlicher von dem Identitätsdiebstahl erfahren hat, personenbezogene Daten, die mit der Identität des Opfers in Verbindung stehen oder sich auf diese beziehen, personenbezogene Daten der betroffenen Person darstellen[2].

2 (EDSA-Leitlinien 01/2022 zu den Rechten der betroffenen Person – Auskunftsrecht, Version 2.1 v. 28. März 2023, Rz. 107).

Daraufhin bat die europäische Aufsichtsbehörde in einem weiteren Amtshilfeverfahren nach Art. 61 DSGVO um Übermittlung eines Schreibens an den Beschwerdeführer, dass sie das Verfahren übernehmen, seine personenbezogenen Daten dafür verarbeiten und ihn alle drei Monate zum Verfahrensstand informieren werden. Dieses Schreiben übersetzte ich und übersandte es dem Beschwerdeführer.
Nunmehr hoffe ich, dass der Beschwerdeführer durch die Intervention der zuständigen federführenden Aufsichtsbehörde die dringend benötigte Auskunft über die beim Verantwortlichen gespeicherten Daten des Identitätsdiebes erhält.

3.3 Recht auf Datenübertragbarkeit, Widerspruchsrecht, Sonstiges

3.3.1 Berichtigung personenbezogener Daten

↗ Art. 12 Abs. 3 DSGVO, § 58 Abs. 6 BDSG

Auch in der Verwaltung kann es zur Verarbeitung unrichtiger personenbezogener Daten kommen. Fällt dies dem/der Betroffenen auf, hat er/sie einen Anspruch auf Berichtigung, der gegenüber der verantwortlichen Behörde geltend gemacht werden kann. Die Behörde ist gesetzlich verpflichtet, unrichtige personenbezogene Daten zu berichtigen. Ob und wie der/die Betroffene von der Berichtigung informiert werden muss, entscheidet sich danach, ob die Behörde die unrichtigen personenbezogenen Daten im Rahmen eines Verwaltungsverfahrens im Anwendungsbereich der Datenschutz-Grundverordnung oder eines Ordnungswidrigkeitenverfahrens, in dem Betroffenenrechte hinsichtlich der Verarbeitung personenbezogener Daten im 3. Teil des Bundesdatenschutzgesetzes (BDSG) geregelt sind, verarbeitet hat. Die DSGVO findet keine Anwendung in Straf- und Bußgeldverfahren, Art. 2 Abs. 2 Buchst. d DSGVO; hier sind gemäß § 500 Strafprozessordnung (StPO) und über § 46 Abs. 1 Gesetz über Ordnungs-

widrigkeiten (OWiG) die Vorschriften des 3. Teils des BDSG einschlägig.

Verarbeitung unrichtiger Daten im Anwendungsbereich der DSGVO

Nach Art. 16 Satz 1 DSGVO hat die betroffene Person das Recht, von dem Verantwortlichen unverzüglich die Berichtigung sie betreffender unrichtiger personenbezogener Daten zu verlangen. Der Verantwortliche ist gemäß Art. 12 Abs. 3 DSGVO verpflichtet, den Antrag der betroffenen Person auf Berichtigung spätestens innerhalb von drei Monaten zu beantworten und gegebenenfalls zu begründen, warum er den Antrag ablehnt.

Verarbeitung unrichtiger Daten im Anwendungsbereich des 3. Teils des BDSG

Handelt die Behörde als Ordnungswidrigkeitenbehörde, hat sie dem/der Betroffenen gemäß § 58 Abs. 6 BDSG lediglich über ein Absehen von der Berichtigung oder Löschung personenbezogener Daten oder über die an deren Stelle tretende Einschränkung der Verarbeitung schriftlich zu unterrichten. Der Gesetzgeber hat damit die Pflichten der Behörde klar formuliert. Eine Benachrichtigungspflicht zählt nicht darunter. Dem/Der Betroffenen bleibt als „Kontrollmöglichkeit", einen Antrag auf Auskunft zur Speicherung seiner/ihrer personenbezogenen Daten bei der Behörde zu stellen und so gegebenenfalls die Berichtigung nachzuvollziehen.

Was ist zu tun?
Verarbeitet die Behörde unrichtige personenbezogene Daten im Rahmen der DSGVO, muss sie den Antrag auf Berichtigung des/der Betroffenen stets beantworten. Im Bereich der Strafverfolgung und des Bußgeldverfahrens gilt dies nur, wenn die Behörde die Berichtigung ablehnt.

4 Pflichten Verantwortlicher und Auftragsverarbeiter

4.1 Verantwortung für die Verarbeitung, Technikgestaltung

4.1.1 Einblicke in die sächsische Webseitenlandschaft und Nachprüfung von Google Analytics

In den letzten beiden Jahren wurden durch die SDTB insgesamt 32.981 Webseiten von sächsischen Unternehmen, Vereinen und Behörden automatisiert geprüft. Auffällig war dabei die hohe Zahl der Einbindungen von Google-Diensten ohne Einwilligung. Darunter fiel auch der Dienst Google Analytics, ein Trackingtool, das der Datenverkehrsanalyse von Websites-Besuchern bzw. -Besucherinnen dient. Wer mit diesem Tracking-Werkzeug auf seiner Website das Nutzerverhalten überwachen möchte, benötigt eine freiwillige und eindeutige Einwilligung der Nutzer/innen, und zwar bevor Daten erfasst oder im Speicher des Endgeräts abgelegt werden.

Im Sommer bis Herbst 2024 fand deshalb die Überprüfung von über 2.300 Verantwortlichen statt, die Google Analytics ohne Einwilligung einsetzten. Trotz der hohen Rate an Verantwortlichen, welche ihr Angebot aufgrund des Schreibens meiner Behörde angepasst haben (65 %), verblieb ein nicht unerheblicher Teil Verantwortlicher (803), welcher keine Änderungen vornahm. Gegen einzelne Verantwortliche aus diesem Pool wurden deshalb im Sommer 2025 gezielt aufsichtsrechtliche Verfahren angestoßen.

Zur Auswahl der Verantwortlichen wurde das Set der Seiten mit Analytics-Einbindung einer aktuellen Prüfung unterzogen, um aktuelle und valide Ergebnisse zu erhalten. Zusätzlich zur Anzahl der ohne Einwilligung kontaktierten Drittanbieter wurde die ungefähre Reichweite der Verantwortlichen bestimmt. Bei hoher Reichweite ist die Anzahl der von den Datenschutzverletzungen betroffenen Personen entsprechend größer. Im Ergebnis wurden elf Verantwortliche bestimmt, sieben davon mit erheblichen Verstößen und über 100.000 Besuchern/Monat, drei mit über 10.000 Besuchern/Monat und über 30 Drittanbieterverbindungen ohne Einwilligung sowie ein Verantwortlicher mit geringerer Reichweite, aber dem Spitzenwert von 57 kontaktierten Drittanbietern. Den Verantwortlichen wurde ein Informationsersuchen mit Ankündigung eines Verwaltungsverfahrens übermittelt. Bislang sind zudem durch Beschwerden bzw. Hinweise weitere Verantwortliche aus dem Kreis der 2.300 Verantwortlichen in entsprechende Verfahren involviert.

Bestandteil des gezielten Informationsersuchens war dabei nicht nur die Google-Analytics-Einbindung, sondern alle Datenschutzverstöße der gesamten Seite, resultierend aus einer tieferen Analyse. Neun der Verfahren wurden inzwischen nach dem Abstellen der Verstöße eingestellt bzw. befinden sich auf gutem Weg, gegen zwei Verantwortliche wird eine Untersagung der Verarbeitungen angestrebt.

Interessant war, dass ein Verantwortlicher alle Verstöße abstellte, allerdings nur für den IP-Geolokationsraum von Deutschland, was im Nachgang behoben wurde. Hier sei darauf hingewiesen, dass die DSGVO weltweit gilt, wenn Waren und Dienstleistungen in Europa angeboten werden.

Neben den Einzelverfahren wurde das Webseiten-Set weiter gepflegt, verbessert und für Prüfungen genutzt. Wirtschaftliche Fluktuationen sind dabei auch im Webseiten-Set zu sehen. Domainauflösungen, Domainumzüge, Weiterleitungen, Änderungen in der Zuständigkeit etc. führen zu steten Veränderungen im Daten-Set. Anzumerken ist hierbei, dass auch in der sächsischen IT-Landschaft ein nicht geringer Teil aufgelöster Domains teils für die Verbreitung maliziöser Inhal-

te (Phishing-Links, Spam und Schadsoftware) übernommen wird. Hier wird der noch vorhandene Bekanntheitsgrad ehemals bekannter Domains durch Kriminelle gezielt ausgenutzt. Im Oktober 2025 wurden so 29.260 Webseiten geprüft. Analysiert wurde der initiale Aufruf der Website sowie zwei weitere Unterseiten, ohne jegliche Interaktion mit der Website, also ohne erteilte Einwilligungen.

Insgesamt 65,5 % dieser Webseiten führten ohne Einwilligung **Netzwerkanfragen** an Drittanbieter durch. Im Durchschnitt waren dies rund drei Drittanbieteranfragen pro Website. Auffällig bleibt hier weiterhin die hohe Quantität der Einbindungen von Google-Diensten ohne Einwilligung. Die Korrelation der Domains nach Unternehmen zeigt dabei 8.562 Webseiten (29.3 %) mit Verbindungen zu Google LLC. Diese Verbindungen werden initiiert durch die Einbettung diverser Dienste, wie insbesondere Google Fonts, aber auch Google Tag Manager, Google Maps, Google Analytics oder Youtube (siehe Tabelle 1).

Tabelle 1:
Top 10 der Verbindungen zu Google-Domains nach Vorkommen auf Webseiten

Top 10 2025	Oktober 2025	Juni 2024	Top 10 2024
fonts.gstatic.com	16,2 % (4.740)	14,7 % (4.849)	fonts.gstatic.com
fonts.googleapis.com	14,4 % (4.216)	13,7 % (4.524)	fonts.googleapis.com
www.google.com	9,8 % (2.866)	9,1 % (3.010)	www.googletagmanager.com
www.googletagmanager.com	7 % (2.034)	7,6 % (2.512)	www.google.com
www.gstatic.com	6,4 % (1.890)	5 % (1.672)	www.gstatic.com
maps.googleapis.com	6,1 % (1.785)	4,9 % (1.614)	www.google-analytics.com
maps.gstatic.com	4,4 % (1.286)	4,5 % (1.482)	maps.googleapis.com
region1.google-analytics.com	3,1 % (918)	4,5 % (1.475)	region1.google-analytics.com
ajax.googleapis.com	2,7 % (801)	3 % (995)	ajax.googleapis.com
www.youtube.com	2,4 % (716)	2,8 % (931)	maps.gstatic.com
Google LLC	**29,3 % (8.562)**	**30,9 % (9.925)**	**Google LLC**

Verbindung	Juni 24	Oktober 24	Oktober 25
_ga Cookie	1.744 (5,3 %)	591 (1,8 %)	854 (2,9 %)
www.google-analytics.com	1.614 (4,9 %)	544 (1,6 %)	484 (1,7 %)
region1.google-analytics.com	1.475 (4,5 %)	413 (1,3 %)	918 (3,1 %)
region1.analytics.google.com	280 (0,8 %)	89 (0,3 %)	141 (0,5 %)
Analytics Gesamt	**2.304 (7 %)**	**803 (2,4 %)**	**1.217 (4,1 %)/ davon 622 (51 %) aus Juni 2024**

Tabelle 2:
Einbindung von Google Analytics ohne Einwilligung im Zeitverlauf

Veränderungen sind hierbei insbesondere hinsichtlich der Reduktion des Google Tag Managers (um 33 %) sowie des Anstiegs der Google-Maps-Einbettung (um 20 %) festzustellen.
Bezogen auf den Dienst **Google Analytics**, integrieren im Oktober 2025 wieder 1.217 Seiten (4,1 %) diesen Dienst ohne Einwilligung. Darunter sind allerdings „nur" 622 Webseiten, welche auch im Juni 2024 Analytics nutzten und nun weiterhin einsetzen. Grundlegend bedeutet dies eine weitere Reduktion um rund 8 %. Allerdings wurde der Dienst in diesem Zeitraum in 595 Webseiten neu integriert und/oder auf einer der besuchten Unterseiten „neu" detektiert.
Die Google Analytics _ga Cookies werden dabei meist als First Party Cookies eingebunden. Es kommt allerdings auch vor, dass Google Analytics direkt durch Drittanbieter-Plugins in die Webseite eingebunden wird, beispielsweise via Website Builder Services, Reservierungssysteme oder Webcam-Einbindungen. Auch hier gilt die Verantwortlichkeit desjenigen, der diese Dienste in sein Angebot integriert. Dass dieser unter Umständen gar nicht der Nutznießer der Datenverarbeitung ist, spielt keine Rolle.
Aufbereitet nach Unternehmen, ergibt sich ein ähnliches Bild wie 2024 bezüglich der generellen Drittanbieterverbindungen in den Webseiten. Externe Verbindungen werden dabei insbesondere zu großen Dienstanbietern aufgebaut wie Google, Cloudflare, Amazon und Facebook; zu Consent-Management-Anbietern wie Usercentrics oder eRecht24; Webseitenbuilder wie Jimdo oder Wordpress oder zu Services

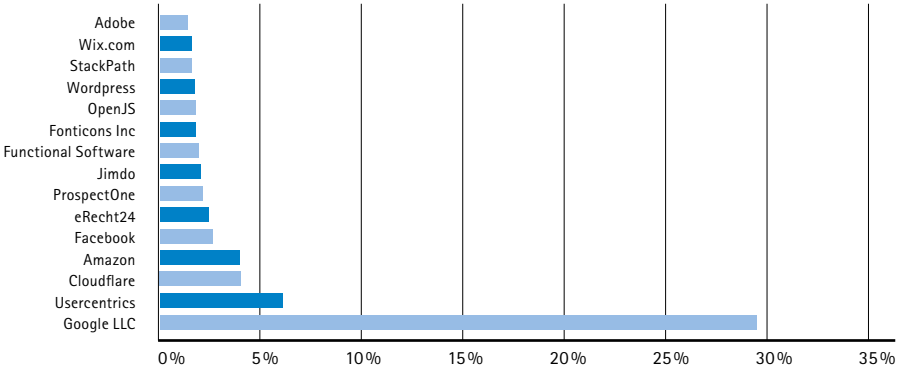


Abbildung 1:
Häufigste Drittanbieterverbindungen auf den untersuchten Webseiten

zur Einbindung externer Ressourcen wie OpenJS oder Fonticons (siehe Abbildung 1).

54,4 % der Webseiten speicherten zudem **Cookies**. Insgesamt wurden 52.967 Cookies gesetzt, im Schnitt rund zwei Cookies pro Webseite. 29,8 % der Cookies haben dabei eine Laufzeit von über einem halben Jahr. Tabelle 3 zeigt die meist gesetzten Cookies nach deren Namen.

Tabelle 3:
Meistgesetzte Cookies

Cookie-Name	Oktober 2025	Juni 2024	Cookie-Name
PHPSESSID	10 % (2.936)	9,6 % (3.159)	PHPSESSID
__Secure-ENID (Youtube)	4,7 % (1.374)	5,3 % (1744)	_ga (Google)
__cf_bm (Cloudflare)	4,0 % (1.174)	3,7 % (1207)	_gid (Google)
_ga (Google)	2,9 % (854)	2,2 % (721)	__cf_bm (Cloudflare)
VISITOR_PRIVACY_METADATA (Youtube)	2,2 % (648)	2 % (676)	CookieConsent (CookieBot)
YSC (Youtube)	2,2 % (648)	1,9 % (633)	XSRF-Token
VISITOR_INFO1_LIVE (Youtube)	2,2 % (645)	1,8 % (601)	_gat (Google)
__Secure-ROLLOUT_TOKEN (Youtube)	2,2 % (645)	1,7 % (573)	YSC (Youtube)
CookieConsent (CookieBot)	2,1 % (621)	1,7 % (572)	VISITOR_PRIVACY_METADATA (Youtube)
XSRF-TOKEN	2,0 % (594)	1,7 % (572)	VISITOR_INFO1_LIVE (Youtube)

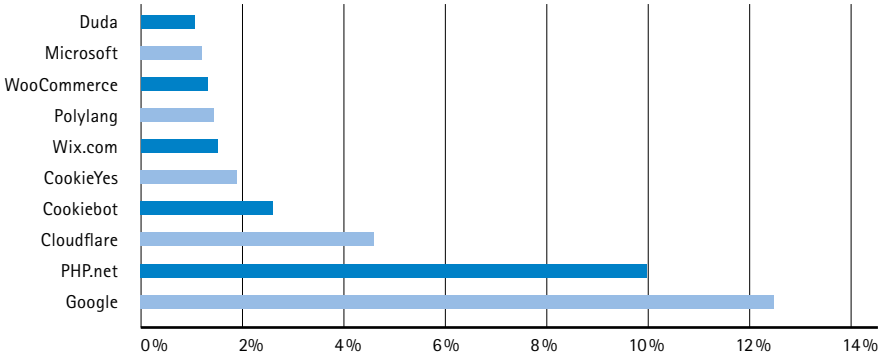


Abbildung 2:
Vorkommen von Cookies nach Unternehmen

Sichtbar ist ein Anstieg von 38 % der Nutzung von Cloudflare-Diensten für Botdetection, Youtube-Einbindungen sowie die Reduktion der Analytics-Einbindungen.

Die Cookie-Namen, korreliert mit dem potenziellen zugehörigen Dienst, zeigen einen ungefähren Einblick der Vorkommen von Cookies nach Unternehmen in den Webseiten. Abbildung 2 zeigt dabei die Verteilung der Top 10 nach Vorkommen in den Websites.

27 % der gesetzten Cookies werden von Drittanbietern in 21,1 % (6.180) der Webseiten gesetzt.

Dabei wurden in den meisten Seiten Drittanbieter-Cookies von (www).google.com (6,5 %, 1.900), (www).youtube.com (4 %, 1.175), cnd.website-start.de (388, 1,3 %) und strato-editor.com (1 %, 291) gesetzt.

Die Domains, korreliert nach Unternehmen, ergeben 9 % (2.621) Webseiten, welche Drittanbieter-Cookies von Domains der Google LLC setzen, 0,6 % der Deutschen Telekom AG und 0,45 % der Vimeo LLC.

20,7 % der Webseiten speicherten zudem **Local Storage Einträge**, welche dabei zu 98,3 % von der First-Party-Domain gesetzt werden. Tabelle 4 enthält die meist gesetzten Einträge nach Key Value, welches insbesondere die Nutzung des Local Storage durch Wordpress-Plugins, Usercentrics, Snowplow, Wix und Google-Recaptcha zeigt.

Art. 5 sowie Art. 32 DSGVO fordern von Anbietern digitaler Dienste die Gewährleistung eines angemessenen Schutz-

niveaus personenbezogener Daten. Für den Schutz von Informationen auf dem Transportweg zwischen Server und Client bietet dabei die TLS-Verschlüsselung eine angemessene Maßnahme nach dem Stand der Technik.

Grundlegend ermöglichen 87,6 % der analysierten Webseiten **TLS-Verschlüsselung**. Dies bedeutet allerdings auch, dass immer noch 12,4 % der Anbieter keine TLS-Verschlüsselung anbieten.

9,3 % der Seiten, welche TLS anbieten, ermöglichen zudem unverschlüsselte Kommunikation, da sie nicht automatisch auf die verschlüsselte Übertragung umleiten. Rund 7 % der Webseiten mit TLS-Verschlüsselung unterstützen zudem weiterhin die TLS-Versionen 1.0 und 1.1, welche veraltet sind. Hier zeigt sich erheblicher Nachbesserungsbedarf. Insbesondere für Webseiten, welche Nutzereingaben ermöglichen, ist eine sichere Übertragung zwingend notwendig.

Insgesamt unterstützen rund 80 % der Seiten eine sichere Transportverschlüsselung (TLS1.2 – 87,5 %; TLS 1.3 – 68,3 %) und leiten direkt auf https um. 20,8 % nutzen HTTP Strict Transport Security (HSTS).

Tabelle 4:
Meistgesetzte Local-Storage-Einträge

Local-Storage-Key-Name	Oktober 2025	Juni 2024	Local-Storage-Key-Name
elementor	2,8 % (831)	3,6 % (1179)	elementor
us_user_interaction	2,7 % (780)	2,8 % (928)	uc_settings
uc_settings	2,7 % (779)	2,8 % (927)	uc_user_interaction
uc_ui_version	2,6 % (756)	2,5 % (850)	uc_ui_version
snowplowOutQueue_snowplow_cf	1,6 % (463)	1,4 % (447)	snowplowOutQueue_snowplow_cf
fedops.logger.sessionId	1,5 % (437)	1,4 % (444)	debug
_grecaptcha	1,4 % (397)	1,4 % (444)	fedops.logger.sessionId
_gcl_ls	1 % (295)	1,2 % (386)	_grecaptcha
cookieNotificationHasBeenSeen	0,9 % (266)	0,9 % (289)	lastExternalReferrerTime
tnsApp	0,9 % (259)	0,9 % (289)	lastExternalReferrer

Genutzte Zertifikate werden dabei insbesondere von Let's Encrypt (>50 %), Sectigo (>25 %) sowie DigiCert (~5 %) ausgestellt.

Gehosted wurden die Seiten insbesondere bei IONOS SE (16,6 %), Strato AG (13,4 %), Neue Medien Muennich GmbH (14,1 %) sowie Hetzner Online GmbH (11,9 %). Dabei werden ca. 12,9 % der Seiten außerhalb Deutschlands und rund 3,8 % außerhalb der Europäischen Union gehosted.

Nicht jede der Drittverbindungen und nicht jedes Speicherobjekt stellt ohne Einwilligung automatisch einen Datenschutzverstoß dar. Die Aufsichtsbehörden legen an die Auslegung der Normen des Art. 6 Abs. 1 DSGVO sowie des § 25 Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG) allerdings strenge Maßstäbe an, welche von den Gerichten in der Rechtsprechung auch weitgehend akzeptiert werden. Zu einzelnen Themen (Google Analytics, Google Fonts, Google Tag Manager, Zahlungsdienste) habe ich mich in der Vergangenheit auch bereits in Tätigkeitsberichten geäußert und klargestellt, dass ein Betrieb oder ein Einbinden in die eigene Website nicht ohne ausdrückliche Zustimmung erfolgen darf.

Aufgrund der aktuellen Ergebnisse werden weitere Prüfungen folgen, insbesondere hinsichtlich der ohne Einwilligung eingebundenen Dienste Google Fonts, Google Maps, Facebook, Youtube und Zahlungsdienstleister (Klarna, Paypal, Google Pay, ...). Auch in Bezug auf Google Analytics wird geprüft. Diese Dienste können nicht auf der Grundlage eines berechtigten Interesses des Webseitenbetreibers oder der Webseitenbetreiberin eingebunden werden. Trotz des insgesamt stark angestiegenen Beschwerdeaufkommens im technischen Bereich wird meine Behörde weiterhin mit möglichst breitenwirksamen anlassunabhängigen Prüfungen und Kontrollen tätig werden.

Was ist zu tun?

Website-Betreiber/innen sind verantwortlich für alle Verarbeitungen auf der eigenen Website, auch wenn diese von Dritten als Service bereitgestellt werden. Alle Verarbeitungen müssen in der Datenschutzerklärung aufgeführt werden und bedürfen einer eigenen Rechtsgrundlage nach der DSGVO. Werden Cookies oder ähnliche Techniken verwendet, bedarf es darüber hinaus einer Rechtsgrundlage nach dem TDDDG, in aller Regel ist dies eine informierte Einwilligung, welche vorher zu erfragen ist.

4.1.2 Gericht bestätigt Auffassung der Aufsichtsbehörde zum Google Tag Manager

↗ § 25 TDDDG, Art. 6 DSGVO

In meinem Tätigkeitsbericht Datenschutz 2023 habe ich im Artikel „4.1.1 Einwilligungspflicht für Google Tag Manager" begründet, warum der Google Tag Manager – auch wenn dieser keine eigenen Cookies setzt – in jedem Fall nicht ohne vorherige Einwilligung ausgeführt werden darf.

Das Verwaltungsgericht Hannover hat in einem Urteil vom 19.03.2025 (Az.: 10 A 5385/22) diese Rechtsauffassung bestätigt.

In der Auseinandersetzung zwischen einem Verantwortlichen und dem Landesbeauftragten für den Datenschutz in Niedersachsen hat sich der Verantwortliche gegen eine Anordnung der Aufsichtsbehörde gerichtlich gewehrt. Das Gericht hat in der Urteilsbegründung meinen Artikel herangezogen und ist damit der Rechtsauffassung gefolgt.

Auch im laufenden Berichtszeitraum gab es etliche Beschwerden wegen des Einsatzes des Google Tag Managers ohne Einwilligung durch Verantwortliche in Sachsen. In allen Fällen wurden entweder ein Verzicht auf das Produkt oder eine vorherige, einfach abzulehnende Einwilligung durchgesetzt. Das Problem des Google Tag Managers besteht nicht darin, dass Elemente der Website unter Bedingungen nachgeladen werden, sondern die Übertragung von Daten an Google sowie das Auslesen von Daten aus dem Endgerät durch Google. Die eigentliche Aufgabe des „Managen" von Tags, also Code-Bestandteilen, ist datenschutzrechtlich an sich nicht problematisch, sofern für die ausgeführten Bestandteile eine Rechtsgrundlage vorhanden ist. Es existieren daher auch etliche alternative Tag Manager, welche ohne Einwilligung ausgeführt werden dürfen.

An dieser Stelle sei angemerkt, dass die Aufsichtsbehörde regelmäßig Schulungs- und Diskussionsangebote unterbreitet, um Verantwortliche und diejenigen, welche die digitalen Dienste technisch umsetzen, zu informieren und einen Aus-

Tätigkeitsbericht Datenschutz 2023:
↗ sdb.de/tb2023

Urteil VG Hannover:
↗ sdb.de/tb2504

Was ist zu tun?
Verantwortliche, welche den Google Tag Manager einsetzen wollen, können sich nicht auf berechtigtes Interesse bzw. eine Erforderlichkeit des Dienstes stützen. Vor einem Laden der Ressourcen des Google Tag Manager muss eine Einwilligung eingeholt werden, wird diese abgelehnt, muss die Website ohne den Google Tag Manager ausgeliefert werden.

tausch zu befördern. Auch im Beschwerdeverfahren ist die Aufsichtsbehörde stets gesprächsbereit.

4.1.3 Fortsetzung und Ende der anlasslosen Prüfung eines Onlinehändlers im Bereich Consumer-Elektronik

↗ § 25 TDDDG, Art. 5 Abs. 1 Buchst. a in Verbindung mit Art. 6 Abs. 1 DSGVO

Was ist zu tun?
Widersprüchliches Verhalten von Unternehmen ist zu unterlassen. Es versteht sich von selbst, dass Verstöße des Unternehmens gegen den ausdrücklich erklärten Willen der Nutzer/innen „nicht einverstanden" im Einwilligungsbanner zu Verstößen gegen die DSGVO und das TDDDG führen. Unternehmen müssen sich gegenüber Nutzerinnen und Nutzern fair verhalten und die Abläufe der Website und in der App mit den tatsächlichen Erklärungen der Nutzenden in Einklang bringen.

Im Tätigkeitsbericht Datenschutz 2024 hatte ich über die anlasslose Prüfung der angebotenen Website eines sächsisches Onlinehändlers für Consumer-Elektronik mit mehreren hundert Mitarbeitern durch das IT-Labor berichtet (4.1.1, Seite 105 f.). Ich habe das Verwaltungsverfahren im September 2025 mit einer Verwarnung wegen des Anbietens der Website mit einer gegenteilig wirkenden Ablehnungsoption auf der ersten Ebene des Einwilligungsbanners abgeschlossen. Ich gehe davon aus, dass die anlasslose Prüfung und die abschließende Verwarnung auch in Zukunft dazu dienen werden, Verstöße gegen die DSGVO und das Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG) zu verhindern, und die Verarbeitungsvorgänge vom Onlinehändler proaktiv angepasst werden.

4.1.4 Werbung nach Lettershop-Verfahren

↗ Art 4 Nr. 7 DSGVO, Art. 26 Abs. 1 Satz 1 DSGVO

Viele Werbezuschriften erhalten Empfänger und Empfängerinnen im Wege des sogenannten Lettershop-Verfahrens. Hierbei werden Adressdatensätze nicht unmittelbar von der werbenden Stelle verarbeitet, sondern von einem Adresshändler an einen Versender, den Lettershop-Betreibenden, übermittelt, der die Adressdatensätze und das zur Verfügung gestellte Werbematerial zusammenführt. Auch im letzten Berichtszeitraum erreichten mich einige Beschwerden von Personen, die die Werbezusendungen als Datenschutzverstoß ansahen.
In diesen Zusammenhängen ist regelmäßig zu klären, welche Stelle als Verantwortlicher im Sinne der Datenschutz-Grund-

verordnung anzusehen ist, das werbetreibende Unternehmen, der Lettershop-Betreiber oder der Adresshändler, vgl. Art. 4 Nr. 7 DSGVO. In der Praxis sind Lettershop-Betreibende und Adresshändler/in häufig ein und dasselbe Unternehmen. Vereinzelt wird auch bei dieser Konstellation von einer gemeinsamen Verantwortlichkeit des werbenden Unternehmens und des Adresshändlers bzw. der Adresshändlerin und des Lettershop-Betreibenden ausgegangen, vgl. Art. 26 Abs. 1 Satz 1 DSGVO. Soweit allerdings das werbende Unternehmen nicht über die Mittel der Datenverarbeitung bestimmt, ist nach Auffassung meiner Behörde nicht von einer Verantwortlichkeit des werbenden Unternehmens auszugehen, vgl. auch VG Berlin, Urteil vom 14.10.2025, 1 K 74/24. In der vorgenannten gerichtlichen Entscheidung wird darauf abgehoben, dass „für die gemeinsame Verantwortlichkeit eine Stelle ‚tatsächlich im Eigeninteresse auf die Entscheidung über die Zwecke und Mittel der Verarbeitung' Einfluss nehmen" müsse, vgl. Rn. 27 der Entscheidung.

Die tatbestandlich kumulativ erforderliche Entscheidungsmacht über Zweck und Mittel der Datenverarbeitung liegt insbesondere in solchen Fallgestaltungen nicht vor, in denen das werbende Unternehmen keinen Einfluss auf die personenbezogenen Bestandteile der Werbesendung nimmt, zum Beispiel keine Kenntnis über die Empfänger/innen der Werbepost erhält. Das Verwaltungsgericht Berlin stellt in dem oben zitierten Urteil insoweit klar: „Denn die bloße Vorgabe einer Zielgruppe (Haushalte in Berlin und Brandenburg mit zumindest überdurchschnittlicher Kaufkraft) führte auch dann nicht dazu, dass die Klägerin auf die ‚Mittel' der Datenverarbeitung Einfluss genommen hätte, wenn man die Mikrozellenselektion als Verarbeitung personenbezogener Daten versteht", ebd., Rn. 30.

Das datensparsame Verfahren der werbetreibenden Unternehmen sehe ich positiv. Letztendlich genügt ihm allein die Kenntnis von den beworbenen Personen, die sich interessiert zeigen bzw. Kunden werden. Gleichwohl ist allen Werbetreibenden zu empfehlen, sich seriöser Dienstleister/innen zu bedienen. Die Regulierung des in vielerlei Hinsicht problematischen Ad-

Was ist zu tun?

Möchten Empfänger/innen als betroffene Personen Widerspruch gegen den weiteren Empfang von Lettershop-Werbung einlegen, so ist dieser am zuverlässigsten beim Lettershop-Betreibenden selbst einzureichen. Auf die angegebenen Informationen zu dem Verantwortlichen wäre zu achten. Gleichwohl besteht eine Wahlmöglichkeit, keine Post mehr vom werbetreibenden Unternehmen oder auch vom Inhaber der Adressanschriften oder global (per Eintragung in die Robinson-Liste) zu erhalten. Anzuraten ist betroffenen Personen, sich präzise zu äußern.

resshandels bleibt daher weiterhin berechtigtes Anliegen der Datenschutzaufsichtsbehörden. Dieses Bemühen sollte nicht zur Beschneidung legitimer briefpostalischer Werbung führen.

4.1.5 Verpflichtungserklärung und SächsBRKG

↗ § 72 SächsBRKG; § 203 StGB

Im Berichtszeitraum wandte sich die Wehrleitung einer gemeindlichen Freiwilligen Feuerwehr an meine Behörde mit folgendem Anliegen:
Es gäbe Mitglieder der Feuerwehr, die sich weigern würden, von der Gemeinde vorbereitete Erklärungen zur Verpflichtung auf das Datengeheimnis sowie der Information zur Verarbeitung personenbezogener Daten zu unterzeichnen. Dies mache der Wehrleitung Sorgen, inwieweit sich das auf das Dienstverhältnis und die eigenen datenschutzrechtlichen Pflichten der Gemeinde auswirken könnte. Konkret ist hier die Frage zu beantworten: Besteht eine Pflicht der ehrenamtlichen Mitglieder zur expliziten Verpflichtung auf den Datenschutz und zur Unterzeichnung des vorgelegten Formulars?
Nach einer Abstimmung mit dem Sächsischen Staatsministerium des Innern (SMI) und der dortigen Datenschutzbeauftragten konnte ich der anfragenden Wehrleitung die Sorgen nehmen und folgende Antwort geben:
Laut einem Kurzpapier der Konferenz der unabhängigen Datenschutzbeauftragten des Bundes und der Länder – Datenschutzkonferenz (DSK) ist eine explizite Verschwiegenheitserklärung der Beschäftigten dann nicht notwendig, soweit deren Verschwiegenheit im öffentlichen Bereich gesetzlich oder tariflich ausdrücklich geregelt ist, siehe Kurzpapier der DSK Nr. 19 – „Unterrichtung und Verpflichtung von Beschäftigten auf Beachtung der datenschutzrechtlichen Anforderungen nach der DS-GVO".
Vorliegend ist es in der Tat so, dass Verschwiegenheit von Beschäftigten im öffentlichen Bereich gesetzlich ausdrücklich geregelt ist. Eine derartige Regelung findet sich in § 72

DSK-Kurzpapier Nr. 19:
↗ sdb.de/tb2505

Sächsisches Gesetz über den Brandschutz, Rettungsdienst und Katastrophenschutz (SächsBRKG):
Diese Norm lautet wie folgt:

(1) Die für die Durchführung dieses Gesetzes zuständigen Aufgabenträger, Feuerwehren, Integrierten Regionalleitstellen, Organisationen im Sinne von § 12a Absatz 2 Satz 1, die Organisierte Erste Hilfe erbringen, Leistungserbringer nach § 31 Abs. 1 Satz 2 sowie die Landesfeuerwehr- und Katastrophenschutzschule dürfen personenbezogene Daten, sofern die Datenverarbeitung nicht schon durch besondere Vorschrift nach diesem Gesetz vorgesehen ist, nur erheben und verarbeiten, soweit dies erforderlich ist. [...]
(2) Die nach Absatz 1 Befugten dürfen personenbezogene Daten sowie Betriebs- und Geschäftsgeheimnisse, die ihnen bei ihrer Tätigkeit bekannt geworden sind, nicht unbefugt offenbaren. [...]

Ich vertrete – insbesondere nach der bereits erwähnten Abstimmung mit dem SMI – die Ansicht, dass sich die Regelung des § 72 Abs. 2 nicht (nur) auf die jeweiligen Stellen/Körperschaften (vorliegend ist dies die Gemeinde), sondern auch auf die Beschäftigten selbst bezieht. Auch diese sind tatbestandlich Befugte im Sinne vorgenannter Gesetzesnorm.
Argumentiert wird hier mit der Gesetzesbegründung zur oben genannten Norm (LT-Drs. 3/9866-1, S. 42): Diese Norm ist der Strafnorm des § 203 Strafgesetzbuch (StGB) nachgebildet und bezieht sich auf Personen(kreise), das heißt die Mitarbeiter und Mitarbeiterinnen und nicht (nur) auf die Institution selbst.
Auszug aus der Gesetzesbegründung:

„Gemäß der Geheimhaltungs- und Offenbarungsvorschrift des Absatzes 2 sind die nach Absatz 1 Befugten zur Verschwiegenheit verpflichtet. Dies gilt sowohl bezüglich fremder Geheimnisse als auch in Bezug auf personenbezogene Daten, die keine Geheimnisse sind. Die Vorschrift ist § 203 Abs. 1 des Strafgesetzbuches (StGB) –

Verletzung von Privatgeheimnissen – nachgebildet. Die Begriffe „Geheimnis" und „unbefugt offenbaren" sind entsprechend den dazu entwickelten Grundsätzen zu interpretieren. Im Gegensatz zu § 203 StGB enthält Absatz 2 nur eine materielle Schweigepflicht, aber keine Strafsanktion. Der in der strafrechtlichen Norm erfasste – und damit zur Verschwiegenheit verpflichtete – Personenkreis ist nicht mit dem identisch, der im Zusammenhang mit der Durchführung von Notfallrettung und Krankentransport mit fremden Geheimnissen in Kontakt kommen kann. Daher ist neben § 203 StGB auch die Regelung in Absatz 2 erforderlich, um den Schutz der Privatsphäre des Betroffenen lückenlos zu gewährleisten."

Dies trifft alle freiwilligen und hauptberuflichen Bediensteten der Stellen im Sinne des § 72 Abs. 1 SächsBRKG: Feuerwehren, Integrierte Regionalleitstellen, Träger der Rettungsdienste und der Organisierten Erste Hilfe (§ 12a SächsBRKG) und der Landesfeuerwehr- und Katastrophenschutzschule. Dies bedeutet, dass die Verpflichtung auf das Datengeheimnis unabhängig davon besteht, ob Erklärungen unterzeichnet wurden oder nicht. Diese Erklärungen haben somit keinen konstitutiven (rechtsbildenden), sondern deklaratorischen (bestätigenden) Charakter. Sie dienen insbesondere der Dokumentation des Verantwortlichen sowie der Sensibilisierung der Personen.
Das SMI hat angekündigt, demnächst eine Mustererklärung für die Verschwiegenheitspflicht zu veröffentlichen.

Was ist zu tun?
Beschäftigte sollten stets über das Datengeheimnis belehrt werden. In vielen Fällen sind sie aber bereits per Gesetz hierzu verpflichtet.

4.2 Sicherheit der Verarbeitung

4.2.1 Sushi mit Nebenwirkungen

↗ Art. 33, 34 DSGVO

Infolge einer Beschwerde wurde die Aufsichtsbehörde auf die Website eines Sushi-Restaurants in Sachsen aufmerksam. Die Beschwerdeführerin hatte ihre Handy-Nummer in eine der bekannten Suchmaschinen eingegeben und stieß

dabei prominent auf einen Treffer auf der Website des Sushi-Restaurants, der eine Bestellung von vor über einem Jahr enthielt, mit vollem Namen, Adresse, Zahlungsinformationen und der Bestellung.

Die Beschwerde wurde umgehend geprüft, dabei wurde festgestellt, dass nicht nur die Beschwerdeführerin betroffen ist, sondern über 3.000 Bestellungen zugänglich waren. Die Bestellungen waren nicht nur nicht gesichert, es bestand auch kein Schutz gegen Webcrawler. Im Ergebnis wurden alle Bestellungen in Suchmaschinen indexiert und waren bei einer gezielten Suche offen zugänglich. Auch ein automatisiertes Abgreifen der Daten durch böswillige Angreifer war möglich. Ein wertvoller Datensatz für Phishing-Angriffe, da die Kombination aus E-Mail-Adresse und Zahlungsart in Verbindung mit Zusatzwissen (Adresse, Bestellung) sehr gut ausnutzbar ist für Angriffe auf Zugangsdaten. Die Daten mutmaßlich aller Personen, die beim Sushi-Restaurant elektronisch bestellt hatten, waren also akut in Gefahr. Die Beschwerdeführerin gab an, dass das Restaurant ihre Beschwerde dort nicht hinreichend ernst nahm und auf die App verwies, mit der die Bestellung wohl erfolgt sei.

Das Restaurant erhielt umgehend die Aufforderung, die Missstände zu beseitigen und Meldung gemäß Art. 33 DSGVO einzureichen. Da innerhalb der Frist von einer Woche keine Reaktion erfolgte, habe ich den Hosting-Provider der Website als Auftragsverarbeiter des Restaurants ermittelt und diesen auf das Datenleck auf der von ihm gehosteten Website hingewiesen. Die Reaktion erfolgte innerhalb von 24 Stunden, die Website wurde umgehend offline genommen. Zwischenzeitlich gab es einige weitere Beschwerden durch Betroffene, welche auf das Datenleck aufmerksam geworden waren, ebenfalls durch die Nutzung von Suchmaschinen.

Aufgrund der seitens des Hosting-Providers veranlassten Maßnahmen hat sich dann auch ein Kontakt mit dem Restaurant ergeben. Offenbar war man sich der Tragweite des Datenlecks nicht bewusst, da die Website nicht vom Restaurant selbst betrieben wird. An der Verantwortlichkeit gemäß DSGVO ändert das aber nichts. Im Nachgang wurde die Web-

Was ist zu tun?
Verantwortliche haben Sorge dafür zu tragen, dass Webanwendungen regelmäßig überprüft werden. Auch kleine Verantwortliche haben hinsichtlich Art. 33 DSGVO entsprechende Prozesse zu etablieren, um Meldepflichten fristgerecht nachkommen und auf Vorfälle angemessen reagieren zu können.

site vor einer erneuten Inbetriebnahme bereinigt, das Restaurant wurde verpflichtet, alle Betroffenen der Datenpanne gemäß Art. 34 DSGVO zu informieren und über mögliche Risiken aufzuklären. Weiterhin wurde festgelegt, dass das Restaurant Sorge dafür zu tragen hat, dass die von Suchmaschinen erfassten Daten aus dem Suchindex der am häufigsten genutzten Suchmaschinen zu entfernen sind.

4.2.2 Fund- und Gebrauchtsachen

↗ Art. 5, 17 DSGVO

Die Behörde wurde in diesem Jahr mit zwei Fällen beschäftigt, bei denen die fehlerhafte Entsorgung von Altgeräten im Nachgang für Aufmerksamkeit gesorgt hat. Im ersten Fall wurde der Behörde die Festplatte eines im Rahmen einer Sperrmüllaktion auf der Straße entsorgten Computers zugesandt. Die Finderin hatte den unvollständigen PC nach einigen Bastelarbeiten (Netzteil und RAM-Riegel fehlten) in Betrieb nehmen können und ist auf der noch verbauten Festplatte auf Patientenunterlagen aus einer im Ort befindlichen Physiotherapiepraxis gestoßen. Die Physiotherapiepraxis wurde damit konfrontiert, es stellte sich heraus, dass der Eigentümer der Praxis davon ausgegangen war, mit der Entfernung und Vernichtung der RAM-Riegel seinen Pflichten ausreichend nachgekommen zu sein. Die RAM-Riegel wurden fälschlicherweise als SSD-Festplatten gewertet. Im Nachhinein war daher dennoch eine Meldung der Datenpanne erforderlich.
Im zweiten Fall hat ein Mitarbeiter eines Krankenhauses ausgesonderte PCs vom Arbeitgeber erworben und diese über ein Forum für Bastler kostengünstig weiterverkauft. Einer der Käufer hat den erworbenen PC gründlicher als erwartet untersucht und ist nach Wiederherstellung einer Partition mit einem handelsüblichen Recovery-Tool auf Patientendaten (Röntgenbilder, Befunde) gestoßen. Die Herkunft der PCs ließ sich über die Seriennummer zum Krankenhaus zurückverfolgen, sodass auch hier eine Verletzung des Schutzes personenbezogener Daten im Rahmen der Entsorgung von Altgeräten ursächlich für eine Kette von Ereignissen war.

Beide Fälle, in denen nur der Zufall bei der Entdeckung der Missstände mitgeholfen hat, zeigen auf, dass es immer noch erhebliche Mängel bei Verantwortlichen bei der sachgerechten Löschung und Vernichtung von Daten bei einer Außerbetriebnahme gibt. Dass in beiden Fällen besonders schützenswerte Daten verarbeitet wurden, macht die Sache nicht besser.

Unabhängig von der Größe des Verantwortlichen, sind Lösch- bzw. Vernichtungsanforderungen insbesondere bei der Aussonderung von Technik immer zu beachten. Das gilt für alle Geräte auch dann, wenn Daten dort nur temporär (zum Beispiel in Druckern) verarbeitet werden. Hierfür bedarf es dokumentierter und überprüfbarer Prozesse. Der Baustein 60 „Löschen und Vernichten" des Standard-Datenschutzmodells benennt systematisch alle Anforderungen, die dabei zu beachten sind.

Baustein 60 „Löschen und Vernichten" des Standard-Datenschutzmodells:
↗ sdb.de/tb2506

Was ist zu tun?
Lösch- bzw. Vernichtungspflichten betreffen alle Verantwortlichen, welche personenbezogene Daten verarbeiten. Ein dokumentierter und nachweisbarer Prozess im Allgemeinen sowie für jedes im Betrieb befindliche Gerät ist hierbei erforderlich. Vor allem dann, wenn besonders schützenswerte Daten verarbeitet werden, sind die Anforderungen entsprechend detailliert auszuarbeiten.

4.2.3 Datenschutz in kommunalen Mängelmeldern

↗ Art. 12 ff., Art. 32 DSGVO

Die Beliebtheit der sogenannten kommunalen Mängelmelder nimmt immer mehr zu. Dies gilt im Übrigen nicht nur für den Freistaat Sachsen, auch in anderen Bundesländern haben die Landesdatenschutzbeauftragten hierzu bereits Hinweise erteilt. Zu nennen ist an dieser Stelle der letzte Tätigkeitsbericht des Bayerischen Landesbeauftragten für den Datenschutz (Tätigkeitsbericht 2024, 3.3.) und des Landesbeauftragten für Datenschutz und Informationsfreiheit Baden-Württemberg (Tätigkeitsbericht 2024, Seite 93).

Bei einem solchen Mängelmelder handelt es sich um ein von der Gemeinde betriebenes Portal, in dem Bürger diverse Anliegen, die der kommunalen Zuständigkeit unterliegen, melden können – sei es eine illegale Müllablagerung, kaputte Straßen, Lärmbelästigung oder vieles andere mehr. Es ist auch möglich, Lichtbilder hochzuladen, welche den Mangel zeigen. Meldungen werden sodann samt Angabe der Örtlichkeit und etwaiger Lichtbilder veröffentlicht und sind somit

im Internet weltweit einsehbar. Durch einen ebenfalls veröffentlichten Bearbeitungsstatus können die Einwohner sehen, ob der Mangel bearbeitet oder gar bereits behoben wurde.
Die sächsischen Kommunen betreiben diese Mängelmelder entweder auf der eigenen Homepage oder nutzen dafür das vom Freistaat Sachsen bereitgestellte Angebot auf dem Beteiligungsportal Sachsen.
Es werden deswegen mit dem Freistaat Sachsen – oder wenn dieses Angebot doch nicht genutzt werden soll – auch einem anderen Dienstleister Auftragsverarbeitungsverträge vereinbart. Die Kommune bleibt aber in jedem Fall für den Betrieb und die entsprechenden Veröffentlichungen datenschutzrechtlich Verantwortliche und hat somit selbst für die Einhaltung des Datenschutzes zu sorgen.
Der Mängelmelder wirft indes erhebliche datenschutzrechtliche Problemstellungen auf: Bereits die Kombination von Lichtbild und einer Örtlichkeit kann – jedenfalls, wenn diese einer von Privatpersonen bewohnten Adresse zuzuordnen ist – im Einzelfall ein personenbezogenes Datum darstellen.
Ein gravierender Fall der Offenbarung personenbezogener Daten liegt dann vor, wenn in der Meldung enthaltene personenbezogene Daten Dritter (die nicht selbst der Autor der Meldung sind) veröffentlicht werden. Auch kam es in der Praxis dazu, dass sich ein Bürger bei meiner Behörde beschwerte, dessen Name in einer der Stadtverwaltung veröffentlichten Antwort auf die Meldung erwähnt wurde. So kam es auch schon vor, dass aufgrund einer Meldung, die in einem negativen Kontext personenbezogene Daten offenbarte, Strafverfahren wegen Ehrdelikten (üble Nachrede) geführt worden sind. Dies ist selbstverständlich unbedingt zu vermeiden.
Die Offenbarung personenbezogener Daten muss deswegen durch technisch-organisatorische Maßnahmen vermieden werden. Auch wenn die Bearbeitung der eingehenden Mängelmeldungen eine kommunale Aufgabe ist und es in diesem Rahmen eine Rechtsgrundlage für Datenverarbeitung gibt, so darf man dies keinesfalls auch für die Veröffentlichung annehmen. Dass die Kommunen Beschwerden und Mängel

der Einwohner/innen entgegennehmen und diese bearbeiten, ist zu unterscheiden davon, dass diese weltweit zur Veröffentlichung gestellt werden.

So muss jede Gemeinde in eigener Verantwortlichkeit unbedingt darauf achten, dass keine Meldungen automatisiert, somit ohne vorige Prüfung durch die Kommune, veröffentlicht werden. Durch technische und organisatorische Maßnahmen ist in jedem Fall sicherzustellen, dass ein/e auf den Datenschutz geschulte/r Mitarbeiter/in jede Meldung vor Veröffentlichung manuell prüft. Anders ist aus meiner Sicht derzeit der Datenschutz nicht zu gewährleisten.

So können die Kommunen auch schon bei den vorgeschalteten Hinweisen an die Bürger/innen bei der Erstellung der Meldungen viel für den Datenschutz tun: Es sollten gut sichtbare und in zugänglicher Sprache verfasste, mit Beispielen untermauerte Hinweise platziert werden, welche Mängel für die Meldungen überhaupt geeignet sind, dass beispielsweise keine nachbarrechtlichen Belange oder Ordnungswidrigkeiten (Falschparker/innen usw.) gemeldet werden können und dass keine personenbezogenen Daten offenbart werden dürfen. Auch der eigene Name sollte am besten nicht mit aufgenommen werden.

Nochmals: Diese Hinweise sind zwar für den Datenschutz wesentlich, können aber **keinen** Ersatz für die eigenständige Prüfung durch den Verantwortlichen ersetzen. Meldungen, die beispielweise andere Personen anprangern sollen und überhaupt nichts mit der gemeindlichen Aufgabenerfüllung zu tun haben, dürfen erst gar nicht veröffentlicht werden. Enthalten geeignete Mängelmeldungen dagegen personenbezogene Daten, sind diese vor Veröffentlichung unbedingt zu löschen.

Auch die allgemeinen datenschutzrechtlichen Bestimmungen sind selbstredend zu wahren und dürfen nicht vernachlässigt werden. Auch wenn eine Veröffentlichung der personenbezogenen Daten nicht erfolgt, werden diese dennoch in der Kommune zwangsläufig verarbeitet. Dazu gehört insbesondere eine umfassende Datenschutzerklärung samt der Benennung von Rechtsgrundlagen für die Verarbeitung

Was ist zu tun?
Kommunen müssen beim Betrieb des sogenannten Mängelmelders, insbesondere bei der Veröffentlichung von Mängeln, als Verantwortliche strickt darauf achten, dass keine personenbezogenen Daten offenbart werden.

von personenbezogenen Daten der Meldenden, Belehrung über Betroffenenrechte gemäß Art. 12 ff. DSGVO, Belehrung über eine eventuell bestehende Auftragsverarbeitung, eines Löschkonzeptes und sonstiger technischer und organisatorischer Maßnahmen (Art. 32 DSGVO).

4.3 Meldung von Datenschutzverletzungen

4.3.1 Allgemeine Hinweise zur Meldepflicht von Datenschutzverletzungen

↗ Art. 5 Abs. 2 DSGVO; Art. 32, 33, 34, 83 Abs. 4 Buchst. a DSGVO

Im Zusammenhang mit der Meldepflicht von Datenschutzverletzungen gemäß Art. 33 DSGVO weise ich darauf hin, dass sämtliche Datenschutzverletzungen mir gegenüber zu melden sind. Dies ist lediglich dann ausgeschlossen, wenn die Datenschutzverletzung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.

Darüber hinaus weise ich auf die neben der grundsätzlich bestehenden Rechenschaftspflicht gemäß Art. 5 Abs. 2 DSGVO im Besonderen für die Meldefälle bestehende Dokumentationspflicht gemäß Art. 33 Abs. 5 DSGVO sowie auf die mögliche Pflicht der Benachrichtigung der betroffenen Person nach Art. 34 DSGVO hin.

Im Rahmen der Verpflichtung nach Art. 32 DSGVO hat der Verantwortliche grundsätzlich dafür Sorge zu tragen, dass die erforderlichen technischen und organisatorischen Maßnahmen umgesetzt und regelmäßig zu überprüfen sind, damit Datenschutzverletzungen, soweit es möglich ist, vermieden werden. Verstöße gegen Art. 32 DSGVO wären beispielsweise fehlende Sicherheitsupdates, fehlende Backups, fehlende Verschlüsselung, aber auch fehlende Sensibilisierungsmaßnahmen gegenüber Beteiligten.

Verstöße sowohl gegen Schutzmaßnahmen gemäß Art. 32 DSGVO als auch gegen formelle Anforderungen der Meldung

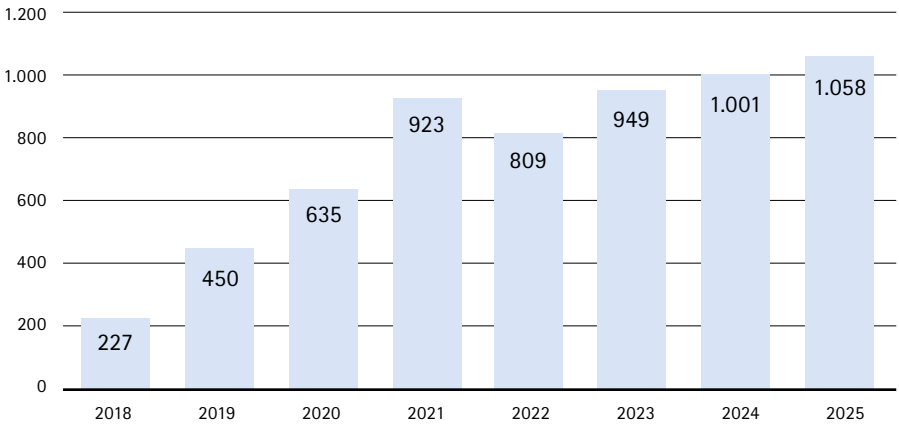
bzw. Benachrichtigung gemäß Art. 33, 34 DSGVO können Gegenstand eines bußgeldrechtlichen Verfahrens gemäß Art. 83 Abs. 4 Buchst. a DSGVO werden. Daher empfehle ich sowohl zum Schutz der Interessen der Betroffenen als auch der eigenen wirtschaftlichen Interessen der Verantwortlichen, die oben genannten dargelegten Vorkehrungen zu prüfen und stets auf aktuellem Stand zu halten.

4.3.2 Wieder neuer Höchstwert bei Meldungen nach Artikel 33 DSGVO

↗ Art. 33, 34 DSGVO

Nach Artikel 33 DSGVO sind Verantwortliche verpflichtet, im Falle der Verletzung des Schutzes personenbezogener Daten unverzüglich und möglichst binnen 72 Stunden nach Bekanntwerden der Verletzung diese der Aufsichtsbehörde zu melden, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Im Berichtszeitraum 2025 sind bei mir 1.058 solcher Meldungen eingegangen. Im Vergleich zum vorjährigen Berichtszeitraum 2024 mit 1.001 Meldungen entspricht dies einem leichten Anstieg um ca. 5 Prozent und stellt zu den vorheri-

Abbildung 3:
Meldungen von Datenschutzverletzungen



gen Berichtszeiträumen erneut einen neuen Höchstwert der jährlichen Meldungen von Datenschutzverletzungen dar.
Die folgenden Fallgruppen sind im Berichtszeitraum besonders häufig gemeldet worden:

Fehlversendung

Wie bereits in den Jahren zuvor stellt die postalische Fehlversendung von Unterlagen mit personenbezogenen Daten die häufigste Ursache für eine Datenschutzverletzung dar. Der Grund hierfür ist eine fehlerhafte Zuordnung von Dokumenten, technische Probleme bei der maschinellen Kuvertierung, falsche Adressdaten oder Verwechslungen von Namen. In den meisten Fällen ist diese Art von Datenschutzverletzungen mit einem geringen Risiko für die betroffenen Personen verbunden, da die/der unbeabsichtigte Empfänger/in den Vorfall meldet und die personenbezogenen Daten nicht missbräuchlich verwendet. Dennoch können sofortige Datenschutzmaßnahmen erforderlich sein. Hierzu zählen unter anderem die Rückforderung bzw. Vernichtung der fehlversandten Unterlagen, die korrekte Neuzustellung, die Bereinigung der fehlerhaft hinterlegten Adressdaten, die regelmäßige Sensibilisierung der handelnden Personen; allgemein ist die Ermittlung der Fehlerursache und deren Beseitigung erforderlich. Diese Maßnahmen hat der Verantwortliche zu veranlassen und im Rahmen der Meldung mitzuteilen.

Offener E-Mail-Verteiler

Ebenso ist inzwischen der offene E-Mail-Verteiler, ohne Berechtigung die E-Mail-Adresse der Empfänger zu veröffentlichen, ein Klassiker einer Datenschutzverletzung. Hierbei werden E-Mail-Adressen nicht im Blindkopie-Feld (Bcc), sondern im Kopie-Feld (Cc) oder sogar im direkten Adressfeld (An) angegeben. Diese Fallgruppe stellt in der Regel eine meldepflichtige Datenschutzverletzung dar, sofern die Empfänger nicht ausdrücklich zugestimmt haben, dass ihre E-Mail-Adresse öffentlich weitergegeben werden darf. In solchen Fällen fehlt es an einer rechtlichen Grundlage für die Verarbeitung der personenbezogenen Daten. Wie den Mel-

dungen an mich zu entnehmen ist, beruht die Nutzung eines offenen E-Mail-Verteilers in der Regel auf einem Versehen der/des Absendenden. Daher ist es sinnvoll und erforderlich, dass der Verantwortliche regelmäßig Sensibilisierungsmaßnahmen durchführt, um solchen Fehlern entgegenzuwirken.

Verlust auf dem Postweg

Nach wie vor gehört der Verlust von Unterlagen mit personenbezogenen Daten auf dem Postweg zu einer häufig gemeldeten Datenschutzverletzung, sodass dies als typische Fallgruppe einer Datenschutzverletzung benannt werden kann. Der Verbleib der Unterlagen ist hierbei in der Regel unklar, sodass das Risiko für die betroffenen Personen regelmäßig höher eingestuft wird als bei einer Fehlversendung. Im Falle einer Fehlversendung kann die/der falsche Empfänger/in den Vorfall melden, wodurch eine abschließende Risikobewertung und eine rasche Klärung möglich sind. Beim Verlust hingegen besteht die Unsicherheit über den Verbleib der Dokumente, was das Risiko einer unbefugten Nutzung oder eines unberechtigten Zugriffs erhöht. Diese Ungewissheit erfordert besondere Aufmerksamkeit und proaktive Maßnahmen seitens des Verantwortlichen, um die möglichen Risiken für die betroffenen Personen zu minimieren. Eine sorgfältige Überwachung und ein effektives Reaktionsmanagement sind daher bei Verlusten von Unterlagen auf dem Postweg essenziell.

Hacking/Schadcode

Eine weitere häufige Fallgruppe von Datenschutzverletzungen ist „Hacking/Schadcode", was auch allgemein der Cyberkriminalität zugeordnet werden kann. Hierunter fallen alle Handlungen und Straftaten, die mithilfe von Informations- und Kommunikationstechnologien ausgeführt werden. Typische Beispiele sind Spam- und Phishing-Mails, die Verschlüsselung von Systemen durch Ransomware, der Einsatz von Schadsoftware (Malware) sowie das Ausnutzen von Sicherheitslücken. In diesem Bereich ist es besonders wichtig, Sicherheitsmaßnahmen kontinuierlich zu optimieren und

potenzielle Bedrohungen aktiv zu überwachen. Durch solche Maßnahmen können im besten Fall Angriffe erkannt und verhindert werden oder sie ermöglichen schnelle und gezielte Gegenmaßnahmen, um die Auswirkungen von Cyberangriffen so gering wie möglich zu halten.
Zur Vermeidung von Meldefällen ist hinsichtlich der technisch-organisatorischen Maßnahmen stets besonderes Augenmerk auf die Informations-/Datensicherheit zu legen. Insoweit verweise ich auch auf meine Hinweise zu vorbeugenden Maßnahmen unter 4.3.4.

Kompromittierte E-Mail-Konten

Eine Unterfallgruppe der Kategorie „Hacking/Schadcode" stellen kompromittierte E-Mail-Konten dar. Eine hiermit verbundene Datenschutzverletzung ist stets mit einem hohen Risiko für alle Beteiligten zu bewerten. Bei derartigen Vorfällen gelangen unbefugte Dritte durch Hacking, Phishing oder unsichere Passwörter in den Besitz von Zugangsdaten und nutzen das Konto, um personenbezogene Daten auszuspähen, betrügerische Nachrichten zu versenden oder weiteren Schaden anzurichten. Hinsichtlich der betroffenen Personen im Sinne des Artikel 33 und 34 DSGVO sind sämtliche Personen einzubeziehen, deren personenbezogene Daten in dem E-Mail-Konto verarbeitet werden, betroffen ist insoweit nicht lediglich die/der Inhaber/in des E-Mail-Kontos.
Bezüglich möglicher Anzeichen einer Kompromittierung, zu ergreifender Sicherheitsvorkehrungen und nachträglicher Maßnahmen verweise ich auf meine ausführlichen Hinweise im Tätigkeitsbericht Datenschutz 2024, 4.4.2, Seite 124 ff.

Tätigkeitsbericht Datenschutz 2024:
↗ sdb.de/tb2024

Einbruch und Diebstahl

Neben der Fallgruppe der Cyberkriminalität, die in der Regel unmittelbar auf personenbezogene Daten ausgerichtet ist, spielen für Datenschutzverletzungen kriminelle Handlungen im Bereich von Einbruchs- und Diebstahltaten ebenso eine bedeutende Rolle. Diese Handlungen sind zwar in der Regel nicht unbedingt darauf ausgerichtet, personenbezogene Daten unberechtigt zu erlangen. Sie richten sich vielmehr auf

die Entwendung von Gegenständen, die personenbezogene Daten enthalten, wie beispielsweise Digitalkameras oder Laptops, und weniger auf die personenbezogenen Daten selbst. Das Risiko für die betroffenen Personen ist dennoch nicht zu unterschätzen, da nicht ausgeschlossen werden kann, dass in der Folge auch die mitentwendeten personenbezogenen Daten zum Gegenstand der kriminellen Handlung werden, um hieraus finanzielle Vorteile zu erzielen. Um das Risiko für die betroffenen Personen hinsichtlich dieser Fallgruppe zu minimieren, ist es besonders wichtig, den Anreiz für Diebstähle zu verringern. Dies lässt sich durch die ordnungsgemäße Sicherung technischer Geräte erreichen – etwa indem diese nicht unbeaufsichtigt gelassen werden. Zudem tragen die Verschlüsselung der gespeicherten Daten, regelmäßige Backups und ein sicherer Passwortschutz maßgeblich dazu bei, die Auswirkungen solcher Vorfälle zu begrenzen.

4.3.3 Ausgewählte Meldungen von Datenschutzverletzungen

Neben den typischen Fallgruppen der gemeldeten Datenschutzverletzungen sind folgende Einzelmeldungen erwähnenswert:

4.3.3.1 Hacking-Angriff und Abfluss von Gesundheitsdaten

↗ Art. 9, 33, 34 DSGVO

Im Berichtszeitraum beschäftigte ich mich intensiv mit der Meldung einer öffentlichen Stelle aus dem wissenschaftlichen Bereich. Im Rahmen einer vorläufigen Meldung nach Art. 33 Abs. 4 DSGVO teilte diese mir mit, dass aufgrund eines kompromittierten Nutzer-Accounts ein nicht legitimierter Zugriff auf eine Rechnereinheit erfolgen konnte. Da zum Zeitpunkt der Meldung noch forensische Untersuchungen stattfanden und die verantwortliche Stelle auch noch keine Angaben zu den betroffenen Personen und einer gegebenenfalls erforderlichen Benachrichtigung dieser treffen konnte, nahm ich Kontakt zu ihr auf. Ich forderte bis zum

Vorliegen des forensischen Abschlussberichtes bereits Zwischenberichte an. Dabei erfragte ich insbesondere die für die Risikobewertung relevanten Informationen nach Art. 33 Abs. 3 DSGVO. Die verantwortliche Stelle teilte mir mit, dass die betroffene Struktureinheit psychologische Gesundheitsdaten enthielt und auch ein Abfluss der personenbezogenen Daten vom Fileserver festgestellt wurde. Da diese Daten nach Art. 9 DSGVO als besondere Kategorien personenbezogener Daten zählen, unterliegen diese einem erhöhten Schutzbedarf und gelten als besonders sensibel. Da bei diesen in der Regel von einem hohen Risiko für die Betroffenen auszugehen ist, die verantwortliche Stelle diese aber noch nicht eindeutig ermitteln konnte, empfahl ich, nach Art. 34 Abs. 3 Buchst. c DSGVO eine öffentliche Bekanntmachung vorzunehmen. Da der Verantwortliche dabei mit mir kooperierte und diese Auffassung teilte, fragte er diesbezüglich nach Hinweisen bzw. Empfehlungen meiner Behörde, wie eine öffentliche Bekanntmachung umzusetzen ist. Diese teilte ich gerne mit und ging dabei zum Beispiel darauf ein, dass die öffentliche Bekanntmachung das Ziel verfolgt, die Betroffenen möglichst vergleichbar wirksam zu informieren. Deshalb soll diese eine möglichst weitreichende Sichtbarkeit und Erreichbarkeit für die Betroffenen gewährleisten. Dies kann zum Beispiel durch eine Veröffentlichung auf der Website des Verantwortlichen erfolgen, wobei der Beitrag dazu nicht versteckt werden darf, sondern sich vielmehr ein Banner an einer herausragenden Stelle empfiehlt. Ich bot dem Verantwortlichen an, dass dieser mir einen möglichen Entwurf der öffentlichen Bekanntmachung vorlegen kann. Nach unverzüglicher Umsetzung dieser Anforderungen stellte die verantwortliche Stelle die öffentliche Bekanntmachung online und leitete mir diese auch zu. Nach Vorlage des forensischen Abschlussberichtes konnte ich auch die getroffenen technischen und organisatorischen Maßnahmen des Verantwortlichen als verhältnismäßig und angemessen bewerten und konnte nach Vorlage aller erforderlichen Informationen den Meldevorgang abschließend bearbeiten.

4.3.3.2 Offene Kalendereinträge mit zum Teil sensiblen Daten

↗ Art. 33, 34 DSGVO

Des Weiteren meldete mir ein Verantwortlicher eine Datenschutzverletzung, wonach Kalendereinträge, die als private gekennzeichnet waren, entgegen dieser Einschränkung für unbefugte Dritte sichtbar waren. Die Einträge enthielten zusätzliche Details, wie zum Beispiel die Teilnehmenden und den Grund für Besprechungen. Besonders sensibel war dies, wenn es sich um Personalgespräche oder Gespräche mit gesundheitsrelevantem Bezug, wie zum Beispiel im Rahmen von betrieblichen Eingliederungsmaßnahmen, handelte. Da der Verantwortliche zum Zeitpunkt der Meldung noch nicht abschließend beurteilen konnte, wie das Risiko für die betroffenen Personen zu bewerten war und in der Folge zunächst offenblieb, ob die betroffenen Personen über die Datenschutzverletzung zu benachrichtigen sind, bat ich den Verantwortlichen zum einen um Darlegung der Risikobewertung und zum anderen, welche technisch-organisatorischen Maßnahmen im Zusammenhang mit der gemeldeten Datenschutzverletzung ergriffen wurden. Der Verantwortliche teilte mir daraufhin mit, dass die Folgen der Datenschutzverletzung aufgrund der Offenlegung von zum Teil sensiblen Daten als substanziell mit gegebenenfalls erheblicher Beeinträchtigung bewertet wurden. Die betroffenen Personen wurden in der Folge gemäß Art. 34 DSGVO durch den Verantwortlichen über die Datenschutzverletzung benachrichtigt. Des Weiteren teilte mir der Verantwortliche mit, dass hinsichtlich der technisch-organisatorischen Maßnahmen das Berechtigungskonzept sowie die Vorgaben, welche Details Kalendereinträge zu beinhalten haben, überarbeitet wurden. Der Meldevorgang konnte damit abgeschlossen werden.

4.3.3.3 Zusendung von Lohn- und Gehaltsabrechnungen durch einen falschen Absender

↗ Art. 33, 34 DSGVO

Ein Verantwortlicher teilte mir im Rahmen einer Meldung nach Art. 33 DSGVO mit, dass die Lohn- und Gehaltsabrechnungen für sämtliche Mitarbeitenden, die durch einen

Auftragsverarbeiter erstellt und in der Regel unmittelbar durch einen Versanddienstleister dem Verantwortlichen zugesendet werden, in diesem Fall erst über einen Umweg beim Verantwortlichen, jedoch nicht mehr verschlossen angekommen sind. Die Lohn- und Gehaltsabrechnungen sind zunächst an einen unberechtigten Dritten gegangen, der diesen Fehler feststellte und die Sendung an den zutreffenden Empfänger, hier den meldenden Verantwortlichen, weiterreichte. Der Verantwortliche benachrichtigte sofort sämtliche Mitarbeitenden über den Vorfall. Ich bat den Verantwortlichen, den Sachverhalt und insbesondere die mögliche Ursache der Fehlversendung aufklären zu lassen und entsprechend das Risiko für die Betroffenen zu bewerten. Im Rahmen der Sachverhaltsermittlung stellte sich heraus, dass die Sendung mit einem falschen Label beklebt wurde oder war. Offen blieb allerdings, wer hierfür die Verantwortung trug. Der Versanddienstleister führte aus, dass sich ein altes Label auf dem Karton befunden hatte, es jedoch auch nicht ausgeschlossen werden könne, dass das alte/falsche Label erst beim Versandprozess versehentlich auf der Sendung aufgebracht worden sei, was wiederum von einer anderen Sendung stammen könnte. Dies sei jedoch nicht mehr zweifelsfrei aufklärbar. Der Auftragsverarbeiter, der die Sendung an den Versanddienstleister weiterreichte, versicherte, stets neue Kartons zu verwenden, was ein altes Label ausschließen würde. Schlussendlich blieb die Ursache ungeklärt. Der Verantwortliche bestätigte mir in seiner abschließenden Mitteilung, dass zumindest garantiert werden kann, dass die fehlgeleitete Sendung sämtliche Lohn- und Gehaltsabrechnungen enthielt und zumindest insoweit nichts verloren ging. Weiterhin wird der Verantwortliche prüfen, sich künftig die Lohn- und Gehaltsabrechnungen auf gesichertem elektronischem Wege zukommen zu lassen. Der Meldevorgang konnte damit abgeschlossen werden.

4.3.4 Vorbeugende Maßnahmen

Nach wie vor sind Prävention/Vorsorge die richtigen Mittel, um einer Datenschutzverletzung und damit verbundenen Risiken für Betroffene sowie der Meldepflicht gemäß Art. 33 DSGVO entgegenzuwirken. Folgende Vorkehrungen sind nach wie vor zu empfehlen:

- Daten sichern! Die Daten von Firmen und Organisationen müssen unbedingt gesichert sein. Diese Backups sollten selbst nicht von Cyberangriffen erfasst werden können.
- Firewall richtig konfigurieren! Die Firewall sollte nur erforderliche Datenverbindungen zulassen. Auch ein Frühwarnsystem über ungewöhnlich hohen Datenverkehr kann Systemverantwortlichen dabei helfen, größeren Schaden abzuwenden.
- Notfallplan beachten! Für die Fälle von Cybererpressungen bzw. Hacker-Angriffen sollte ein Notfallplan vorliegen, der im Akutfall abzuarbeiten ist. Dazu gehört auch eine Regelung, wann die/der IT-Administrator/in, interne Datenschutzbeauftragte, die Datenschutzaufsichtsbehörde oder auch die Mitarbeitenden, Unternehmensleitung und Kundinnen bzw. Kunden zu informieren sind.
- Reservetechnik vorhalten! Eine dringende Empfehlung ist zudem, Reservetechnik vorzuhalten. Ermittler können das angegriffene IT-System forensisch untersuchen, während das Unternehmen trotz Cyberangriff rasch wieder arbeitsfähig ist.
- Frühzeitig kommunizieren! Verantwortliche sollten betroffene Personen oder Abteilungen auch dann schnell über den Vorfall informieren, wenn noch nicht sicher ist, ob und welche personenbezogene Daten betroffen sind.
- Weiterbildung! IT-Verantwortliche und all jene, die in Unternehmen und Organisationen für die IT-Sicherheit zuständig sind, benötigen regelmäßig Weiterbildung.

5 Internationaler Datenverkehr

5.1 Neue Angemessenheits-beschlüsse der EU-Kommission

↗ Art. 45 DSGVO

Ein Angemessenheitsbeschluss ist ein Schlüsselmechanismus in den EU-Datenschutzvorschriften, mit dem die Europäische Kommission auf Grundlage von Artikel 45 DSGVO feststellen kann, ob ein Drittland oder eine internationale Organisation ein angemessenes Datenschutzniveau bietet. Eine solche Entscheidung hat zur Folge, dass personenbezogene Daten ungehindert von Europa in das betreffende Drittland oder die betreffende internationale Organisation übermittelt werden können.

Übersicht zu bestehenden Angemessenheitsbeschlüssen:
↗ sdb.de/tb2511

Im Berichtszeitraum hat die EU-Kommission zunächst die Angemessenheitsbeschlüsse für das Vereinigte Königreich (UK) erneuert, wodurch der freie Datentransfer zwischen EU und UK bis zum 27. Dezember 2031 sichergestellt bleibt. Das UK wird weiterhin als sicheres Drittland eingestuft, da dessen Datenschutzniveau als gleichwertig mit EU-Standards gilt. Dies verhindert bürokratische Hürden für den Datenverkehr.

Mit Durchführungsbeschluss (EU) 2026/179 vom 26.01.2026 zählt nun auch Brasilien zu denjenigen Drittländern, in welche personenbezogene Daten vereinfacht übermittelt werden können. Das durch die brasilianische Rechtsordnung und das Datenschutzgesetz „Lei Geral de Proteção de Dados" vermittelte Schutzniveau ist dem der EU gleichwertig. Damit sind für viele reguläre Datentransfers zwischen Unternehmen und Organisationen in der EU und in Brasilien in der

Regel keine zusätzlichen Transferinstrumente wie Standardvertragsklauseln mehr nötig.

Neu auf dieser Liste ist ebenfalls das Europäische Patentamt (EPA) als erste internationale Organisation überhaupt, für die seitens der EU-Kommission ein Angemessenheitsbeschluss gefasst wurde. In der Vergangenheit waren Angemessenheitsbeschlüsse nur für Drittländer erlassen worden. Der entsprechende Angemessenheitsbeschluss hat zur Folge, dass personenbezogene Daten nunmehr ungehindert und ohne weitere Schutzvorkehrungen zwischen der EU (einschließlich Norwegen, Liechtenstein und Island) und dem EPA übermittelt werden können.

Was ist zu tun?

Verantwortliche sollten prüfen, ob sie von den erleichterten Übermittlungsregelungen der Angemessenheitsbeschlüsse profitieren können.

6 Sächsische Datenschutzbeauftragte

6.1 Zuständigkeit und Anforderungen an Beschwerden

6.1.1 KI-Verordnung tritt teilweise in Kraft

↗ KI-VO

Teile der „KI-Verordnung" der Europäischen Union traten 2025 in Kraft: Am 2. Februar das Verbot bestimmter KI-Praktiken und die Pflicht zur Schulung der KI-Kompetenz von Beschäftigten sowie am 2. August neue Pflichten für die Anbieter von KI-Modellen.

Auch sächsische Behörden und Unternehmen müssen sich mit den neuen Vorgaben auseinandersetzen. Mitarbeitende müssen geschult werden, und der Einsatz von KI muss überprüft werden, ob er die neuen Regeln erfüllt. Für Anbieter gelten neue Pflichten, womit gleichzeitig auch die Rechte von Betreibern von KI-Modellen gegenüber den Anbietern gestärkt werden. Trotz der Frist vom 2. August hat es die Bundesregierung jedoch weiterhin versäumt, ein Durchführungsgesetz zu verabschieden, und es ist weiterhin keine Aufsicht benannt. Die Datenschutzkonferenz hat empfohlen, diese Zuständigkeit den Datenschutzaufsichtsbehörden der Länder zu übertragen. Dieser Empfehlung schließe ich mich ausdrücklich an. Jedoch haben die Aufsichtsbehörden auch ohne diese Aufgabe bereits klar definierte Zuständigkeiten, insbesondere für die Marktüberwachung von Hochrisiko-KI im Bereich der Strafverfolgung, Justiz und Migration.

Die weiteren Teile der KI-Verordnung werden größtenteils am 2. August 2026 in Kraft treten. Ab diesem Datum gel-

Was ist zu tun?
Betreiber und Anbieter von KI-Modellen müssen seit 2025 Pflichten erfüllen und sich auf die umfassende Inkraftsetzung der KI-Verordnung 2026 vorbereiten.

ten Anforderungen auch für „Hochrisiko-KI"-Systeme, mit wenigen Ausnahmen, sowie Transparenz- und Kennzeichnungspflichten. Gleichzeitig greift die Durchsetzung durch die Aufsichtsbehörden, welche dann Verstöße ahnden und Audits durchführen können. Ich rufe alle sächsischen Unternehmen und öffentlichen Stellen dazu auf, sich frühzeitig mit den neuen Regularien auseinanderzusetzen.

6.1.2 Zuständigkeit bei unerwünschter B2B-E-Mail-Werbung

↗ § 7 UWG, Art. 2 Abs. 1 DSGVO

Das Verbot der Kaltakquise, also Werbung ohne vorherige ausdrückliche Einwilligung der Adressatin bzw. des Adressaten, per E-Mail gilt in Absolutheit nur für den Business-to-Consumer-Bereich (B2C). § 7 des Gesetzes gegen den unlauteren Wettbewerb (UWG) regelt die Grenzen der rechtlichen Zulässigkeit und die Frage der „unzumutbaren Belästigung" durch Werbung. Grundsätzlich ist eine ausdrückliche Einwilligung erforderlich und Werbung ohne vorherige ausdrückliche Einwilligung unzulässig, vgl. § 7 Abs. 2 Nr. 2 UWG. Soweit Kunden und Kundinnen nicht im Rahmen des Double-Opt-In-Verfahrens Werbemails zugestimmt haben, ist die E-Mail-Werbung unzulässig. Ausnahmen regelt § 7 Abs. 3 UWG, etwa bei Bestandskunden bzw. -kundinnen.

Trotz klarer Rechtslage mehren sich Beschwerdeeingänge bei meiner Behörde in Bezug auf E-Mail-Werbeansprachen zwischen Unternehmen (Business-to-Business – B2B). Nicht immer ist eine Datenschutzaufsichtsbehörde dafür sachlich zuständig. Und nicht jede wettbewerbsrechtlich unzulässige Werbung ist gleichzeitig ein Datenschutzverstoß. Eine sachliche Zuständigkeit der Aufsichtsbehörde kommt nur bei tatsächlicher Verarbeitung personenbezogener Daten in Betracht, Art. 2 Abs. 1 DSGVO.

Unter welchen Voraussetzungen sich aus B2B-Werbung Verstöße gegen persönlichkeitsrechtsschützende Vorschriften und den Datenschutze oder lediglich zivilrechtliche Ansprüche ergeben können, hatte der Bundesgerichtshof mit Be-

Was ist zu tun?
Für die beschriebene Form von Werbung liegt die zuständige Aufsichtsbehörde mit wenigen Ausnahmen in dem Bundesland, in dem sich die Geschäftsanschrift (nach Impressum bzw. Datenschutzerklärung) des werbenden Unternehmens befindet. In Fällen, in denen B2B-Werbung an Funktionspostfächer gerichtet worden ist und auch im Übrigen kein Personenbezug erkennbar ist, ist die Aufsichtsbehörde wegen des sachlichen Anwendungsbereichs der DSGVO nicht zur Abhilfe berufen.

schluss vom 20. Mai 2009, I ZR 218/07, entschieden. Enthält der Text der Werbe-E-Mail keinen Hinweis auf Personenbezug der Empfängerin oder des Empfängers, zum Beispiel durch namentliche Ansprache, verbleibt, was die Personenbeziehbarkeit angeht, nur die Struktur der E-Mail-Adresse der Empfängerin oder des Empfängers. Die typische Struktur einer personenbezogenen E-Mail-Adresse lautet zum Beispiel: vorname.name@firmenbezeichnung.de. Weist die genutzte E-Mail-Adresse jedoch auf ein Funktionspostfach ohne ersichtlichen Personenbezug, zum Beispiel post@firmenbezeichnung.de, so besteht für meine Behörde in Ermangelung eines Personenbezugs datenschutzaufsichtlich kein Raum zum Tätigwerden.

6.1.3 Kurioses

Gelegentlich werden bei meiner Behörde Beschwerden über Sachverhalte eingelegt, bei denen man sich fragen kann, ob die Beschwerde wirklich ernst gemeint ist. Nichtsdestotrotz werden diese von mir sachgerecht beantwortet. Nachfolgend zwei Beispiele aus dem letzten Berichtszeitraum:

6.1.3.1 Der Hasenstallfall

↗ Art. 2 Abs. 1 DSGVO

Der Beschwerdeführer schilderte mir einen aus seiner Sicht „gravierenden" Fall, der sich im ländlichen Raum zugetragen hatte. Nachdem er von einer Verwandten aufgefordert worden sei, einen auf deren Grundstück befindlichen Hasenstall kurzfristig zu beseitigen, sei an einem Morgen an der Haustür seines Hauses ein handschriftlicher Zettel angebracht worden, auf dem sein Name, die Anschrift und eine Aufforderung zur Beräumung des Hasenstalls zu lesen war. Der Beschwerdeführer erkannte hierin eine Veröffentlichung seiner personenbezogenen Daten.
Den sachlichen Anwendungsbereich der Verordnung gemäß Art. 2 Abs. 1 DSGVO erkannte ich als nicht eröffnet. Danach gilt die Datenschutz-Grundverordnung lediglich für die nichtautomatisierte Verarbeitung personenbezogener Daten,

also für handschriftliche Notizen, wenn diese in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Es fehlte offensichtlich an einer entsprechenden Speicherung in einem Dateisystem.
Insgesamt handelte es sich um einen Bagatellvorgang. Der Petent wurde im Ergebnis auf den Zivilrechtsweg verwiesen und die Beschwerde zurückgewiesen.

6.1.3.2 Angaben zu Tieren als personenbezogene Daten

↗ Art. 1 Abs. 1 bis 3 DSGVO, Art. 9 Abs. 1 DSGVO

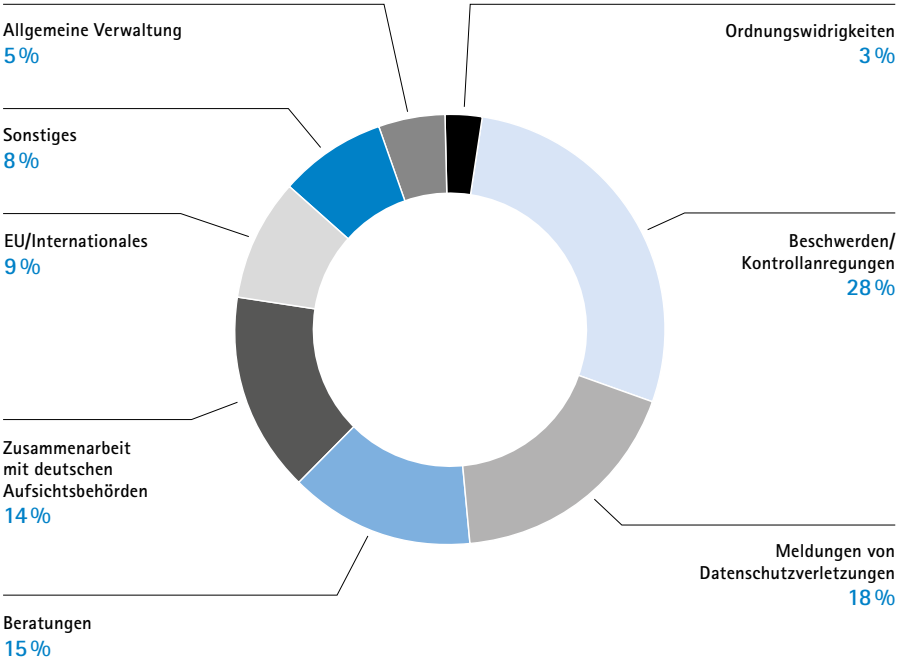
Eine Beschwerdeführerin stellte dar, dass sie seitens einer Tierarztklinik eine außergerichtliche Schadensersatzforderung übermittelt bekommen habe. Diese habe personenbezogene Daten, medizinische Angaben zu ihren Tieren enthalten. Ohne ihre Einwilligung oder Information sei dieses Schreiben seitens des Tierarztes an einen Rechtsanwalt weitergegeben worden. Auch habe sie gemäß Art. 15 DSGVO vollständige Auskunft über die tierärztliche Behandlungsdokumentation ihrer fünf Hunde verlangt. Daraufhin habe ihr die Tierarztklinik mitgeteilt, dass die Angelegenheit an den Rechtsanwalt der Tierklinik übergeben worden sei. Die Beschwerdeführerin führte weiter aus, dass diese sensiblen Informationen, zum Beispiel Diagnosen, Behandlungsdaten, Verhaltensbeobachtungen zu den Tieren, besondere Kategorien personenbezogener Daten gemäß Art. 9 DSGVO darstellen würden.
Eine Datenschutzverletzung lag nicht vor. Wie den Normtexten der Datenschutz-Grundverordnung zu entnehmen ist, bezieht sich dies nur auf besondere Kategorien von Daten natürlicher Personen, das heißt, Menschen. Tiere sind davon nicht erfasst, vgl. Art. 1 Abs. 1 bis 3, Art. 9 Abs. 1 DSGVO im Wortlaut. Die Beschwerde wurde abgewiesen.

6.2 Zahlen und Daten zu den Tätigkeiten 2025

6.2.1 Überblick zu den Arbeitsschwerpunkten

Wie in den Vorjahren war im Berichtszeitraum etwa jeder vierte neu angelegte Vorgang eine Beschwerde oder Kontrollanregung. Die Bearbeitung beansprucht mit Abstand die meisten personellen und zeitlichen Ressourcen der Fachreferate. Hingegen liegt die Bearbeitung der gemeldeten Datenschutzverletzungen nach Artikel 33 DSGVO nur bei Referat 1 (siehe 6.2.8). Analog zu den vorhergehenden Jahren handelte es sich auch 2025 bei etwa jedem fünften Vorgang um eine Datenpannen-Meldung. Beratung sowie die Zusammenarbeit mit den deutschen Datenschutzaufsichtsbehörden gehörte ebenfalls zu den Tätigkeitsschwerpunkten.

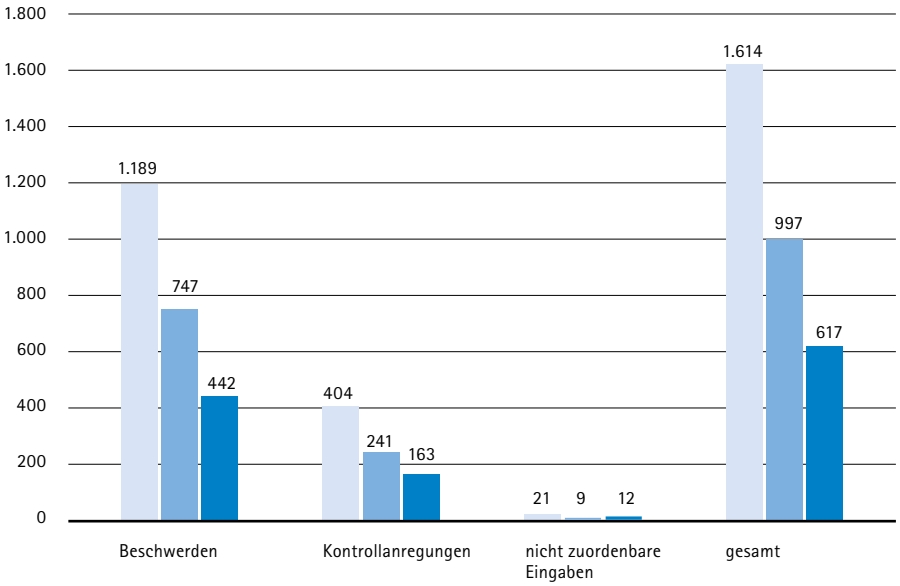
Abbildung 4:
Arbeitsschwerpunkte 2025 nach Anzahl neu angelegter Vorgänge



6.2.2 Beschwerden und Kontrollanregungen

2025 erhielt ich 1.614 Eingaben, die in meinen Zuständigkeitsbereich fielen. Der Großteil – 1.189 Fälle – stammte von Personen, die ihre Rechte durch einen Datenschutzverstoß als verletzt ansahen. In 442 Fällen wandten sich Hinweisgeber/innen, die nicht selbst betroffen waren, mit einer Kontrollanregung an mich. Im Vergleich zu 2024 legten die Eingaben insgesamt um 29 Prozent zu. Somit stieg das Aufkommen das vierte Mal in Folge und übertrifft mit großem Abstand alle bisherigen Jahre seit Wirksamwerden der Datenschutz-Grundverordnung. Der Zuwachs betraf sowohl den nichtöffentlichen als auch den öffentlichen Bereich. So ein Anstieg stellt eine große Herausforderung für eine kleine Behörde wie meine dar. Daraus resultiert zum Beispiel, dass für anlassfreie Kontrollen Kapazitäten fehlen, wodurch ich meiner Aufsichtsfunktion nur unzureichend nachkommen kann (vgl. 6.2.8).

Abbildung 5:
Beschwerden und Kontrollanregungen 2025



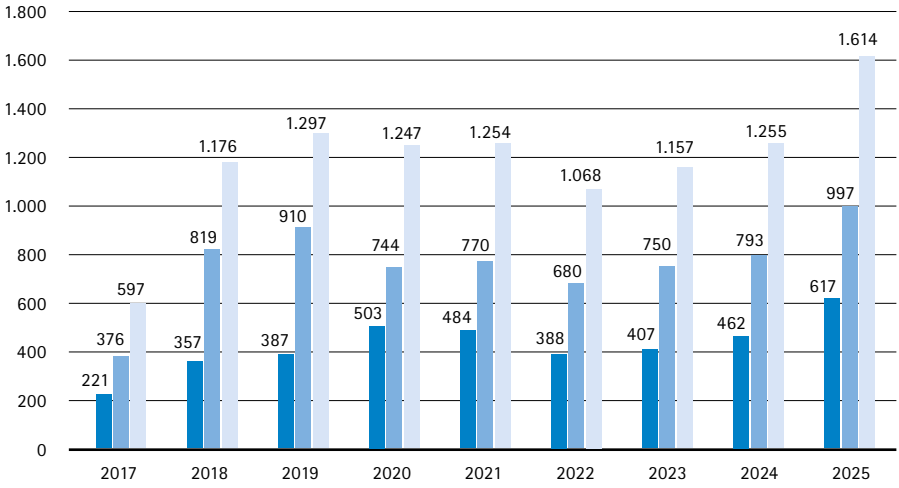


Abbildung 6:
Beschwerden und Kontrollanregungen im Zeitverlauf

- öffentlicher Bereich
- nichtöffentlicher Bereich
- Beschwerden und Kontrollanregungen gesamt

6.2.3 Beratungen

Beratungen umfassen alle schriftlichen datenschutzrechtlichen Auskünfte gegenüber privaten und öffentlichen Stellen. Mit 898 Vorgängen stieg die Anzahl um 22 Prozent gegenüber dem Vorjahr und zum dritten Mal nacheinander (2024: 736, 2023: 593). Unabhängig davon beantwortete meine Behörde auch 2025 wieder eine Vielzahl von Datenschutzfragen per Telefon. Diese Anfragen werden statistisch nicht erfasst. Der Anstieg bei den Beratungen betraf sowohl den nichtöffentlichen als auch den öffentlichen Bereich.

6.2.4 Meldungen von Datenpannen

2025 meldeten Verantwortliche 1.058 Datenschutzverletzungen – ein Plus von knapp 6 Prozent gegenüber dem Vorjahr und abermals ein neuer Höchststand. Zum Vergleich: 2024 gingen 1.001 Meldungen nach Art. 33 DSGVO bei mir ein. Neben der Registratur der Vorgänge sind die Meldungen auszuwerten und gegebenenfalls für eine aufsichtliche Nacharbeit zu kategorisieren. Einen Überblick zu den inhaltlichen Vorgängen liefern die Beiträge unter 4.3.3.

6.2.5 Register der benannten Datenschutzbeauftragten

↗ Art. 37 Abs. 1 und 7 DSGVO

Im Berichtszeitraum gingen 1.033 Meldungen zu benannten Datenschutzbeauftragten in meiner Dienststelle ein. Diese Meldungen umfassten Mitteilungen zur Benennung von behördlichen und betrieblichen Datenschutzbeauftragten, zu Änderungen oder zur Beendigung dieser Funktion.

Die übersandten Mitteilungen werden von den Fachreferaten meiner Behörde unter anderem genutzt, um die Erfüllung der Meldepflicht gemäß Art. 37 Abs. 7 DSGVO oder ein mögliches Vorliegen von Interessenskonflikten nach Art. 38 Abs. 6 DSGVO zu prüfen.

Die DSGVO sieht gemäß Art. 37 Abs. 1 für den Verantwortlichen (öffentliche Stellen generell; nichtöffentliche Stellen unter bestimmten Voraussetzungen) die Pflicht vor, eine/n Datenschutzbeauftragte/n zu benennen.

Was ist zu tun?
Nach Art. 37 Abs. 7 DSGVO hat ein Verantwortlicher oder ein Auftragsverarbeiter die Kontaktdaten der oder des Datenschutzbeauftragten nicht nur zu veröffentlichen, sondern auch der Aufsichtsbehörde mitzuteilen. Die Dokumentation der Benennung und der Erfüllung der Meldepflicht obliegt dem Verantwortlichen.

6.2.6 Förmliche Begleitung von Rechtsetzungsvorhaben

↗ Art. 36 Abs. 4 DSGVO

Nach Art. 36 Abs. 4 der Datenschutz-Grundverordnung hat der Freistaat Sachsen mich bei der Ausarbeitung eines Gesetzentwurfs oder eines Rechtsverordnungsentwurfs, der die Verarbeitung personenbezogener Daten regelt, zu konsultieren. Zumeist geschah dies bereits zu einem frühen Zeitpunkt, nämlich bei der Fertigung von Referentenentwürfen in den Staatsministerien.

Regelmäßig beteiligen mich die Landtagsfraktionen bei der Erarbeitung von Gesetzentwürfen und Änderungsanträgen, allerdings wurde ich im Berichtsjahr wahrscheinlich wegen der relativ neuen Zusammensetzung des Landtags und der Besonderheit einer Minderheitsregierung nicht konsultiert. Hinzu kamen Stellungnahmen zu verschiedenen Vorhaben, die im Zusammenhang mit der Bundesgesetzgebung standen und mit denen sich auch die Datenschutzkonferenz befasste.

Die wichtigsten im Jahr 2025 abgegebenen Stellungnahmen:

- Novelle des Sächsischen Polizeivollzugsdienstgesetzes
- Referentenentwurf Data Act – Entwurf eines Gesetzes zur Durchführung der Verordnung (EU) 2023/2854 (Data Act-Durchführungsgesetz – DA-DG)
- Änderung der Sächsischen Justizorganisationsverordnung
- Entwurf eines Gesetzes zur Durchführung der Verordnung (EU) 2024/900 des Europäischen Parlaments und des Rates über die Transparenz und das Targeting politischer Werbung (Gesetz über die Transparenz und das Targeting politischer Werbung – PWG-E)
- Anhörung zum Sächsischen Wärmeplanungskosten- und Datenbereitstellungsgesetz (SächsWPKDG)
- Stellungnahme zum Erlass zur Bereitstellung von Eigentümerdaten des amtlichen Vermessungswesens für Erneuerbare-Energien-Anlagen (EE-Anlagen)
- Anhörung zur Verordnung zur Regelung der Lehrgangs- und Prüfungsvoraussetzungen für Lebensmittelkontrolleure
- Entwurf einer Ausbildungs- und Prüfungsordnung allgemeiner Verwaltungs- und sozialwissenschaftlicher Dienst
- Entwurf eines Gesetzes zur Änderung des Sächsischen Beamtenversorgungsgesetzes; Beteiligung nach § 12 Abs. 3 Satz 2 Geschäftsordnung der Sächsischen Staatsregierung (GeschoSReg)
- Entwurf einer Verordnung der Sächsischen Staatsregierung zur Änderung dienstrechtlicher Vorschriften zum Jugendarbeitsschutz und Mutterschutz; Beteiligung nach § 119 des Sächsischen Beamtengesetzes, Entwurf einer Verordnung über die Bestimmung der Altersgrenzen bei Staatsbeamtinnen und Staatsbeamten (Altersgrenzenverordnung);

Meine Beratung zu Gesetzentwürfen bereits auf der Arbeitsebene der Ministerien hat den Vorteil, dass ich bereits zu Beginn des Gesetzgebungsverfahrens auf datenschutzrechtliche

Lösungen hinarbeiten kann. Davon sollten die Staatsministerien noch häufiger Gebrauch machen. Werde ich erst in der öffentlichen Anhörung von Gesetzentwürfen um Stellungnahme gebeten, sind oftmals bereits viele politische Kompromisse geschlossen worden, die Änderungen im Bereich des Datenschutzes auch dann erschweren, wenn sie die Beteiligten als erforderlich ansehen.

Was ist zu tun?
Staatsministerien sollten mich öfter frühzeitig bei der Erarbeitung von Rechtsregelungen einbeziehen.

6.2.7 Zusammenarbeit mit europäischen Aufsichtsbehörden über das Internal Market Information System (IMI) 2025

↗ Art. 4, 56–60 DSGVO

Über die Kommunikationsplattform der europäischen Aufsichtsbehörden, dem Internal Market Information System (IMI), habe ich im Berichtszeitraum wieder aktiv an grenzüberschreitenden Verfahren mitgewirkt. Weiterhin wurde jede Woche eine Übersicht über die neuen Verfahren im IMI erstellt, von denen ich durch „notifications" benachrichtigt werde (vgl. Tätigkeitsbericht Datenschutz 2023, 6.2.6, Seite 196 ff. und Tätigkeitsbericht Datenschutz 2024, 6.2.7, Seite 140).

Tätigkeitsbericht Datenschutz 2023:
↗ sdb.de/tb2023

Tätigkeitsbericht Datenschutz 2024:
↗ sdb.de/tb2024

Die Anzahl der neuen Verfahren variiert: In der zweiten Januarwoche 2025 waren es 35 neue Verfahren, in der 47. Kalenderwoche dagegen 91; gerade im letzten Quartal 2025 war die Zahl der neuen Beschwerden, deren Bearbeitung über das IMI abgewickelt werden müssen, um ungefähr ein Drittel gestiegen.

Die meisten meiner Eintragungen im IMI dienen weiterhin der Klarstellung, dass ich nicht betroffene Aufsichtsbehörde bin und deshalb am weiteren Verfahren über eine Beschwerde nicht mitwirke. Das ist gemäß Art. 4 Nr. 22 Buchst. a bis c DSGVO der Fall, wenn keine Beschwerde gegen den Verantwortlichen (in der Regel ein Unternehmen) erhoben wurde, die Bewohner/innen des Zuständigkeitsbereiches von der Verarbeitung nicht erheblich betroffen sind oder wenn keine Niederlassung des Verantwortlichen im Zuständigkeitsbereich vorhanden ist. Insgesamt habe ich im Berichtszeitraum diese Erklärung 294 Mal abgegeben. In 7 Verfahren meldete

ich mich als betroffene Aufsichtsbehörde, in der Regel deshalb, weil in sächsischen Zweigniederlassungen des Verantwortlichen eine Datenverarbeitung erfolgt, die auch Gegenstand der Beschwerde ist. Für die Beurteilung der Frage, ob ich betroffene Aufsichtsbehörde bin, ist häufig das Studium der Websites von Unternehmen, gegen die eine Beschwerde erhoben wurde, erforderlich. Wegen des weiten Niederlassungsbegriffs der DSGVO (vgl. Erwägungsgrund 22, Satz 2 DSGVO) können auch sächsische Standorte des Verantwortlichen, die nicht im Handelsregister verzeichnet werden, eine Niederlassung gemäß Art. 4 Nr. 22a DSGVO darstellen. Hierbei erscheinen gelegentlich auf den Websites Lockvogelangebote: Freispiele und Bonusangebote von Onlinespieleanbietern, oder ein Gramm Haschisch als Draufgabe für die erste Bestellung von Cannabis. Diese waren aber bei der Beantwortung der Frage nach einer sächsischen Niederlassung genauso wenig hilfreich wie das eines kostenlosen Ersttelefonats mit einer Wahrsagerin, welches eine französische Okkultismus-Website ermöglichen wollte, sodass ich gleich auf die Seite „About us" oder auf Wikipedia weiterklickte.

In zwei Verfahren im Rahmen der freiwilligen Amtshilfe antwortete ich auf allgemeine Anfragen europäischer Aufsichtsbehörden. In einem Verfahren ging es um eine juristische Frage im Zusammenhang mit dem Transparenzgesetz, in einem anderen um eine Datenpanne, die mir nicht gemeldet worden war.

Im Berichtszeitraum wurden zwei sächsische Beschwerden mithilfe von IMI-Verfahren an die federführende Aufsichtsbehörde übermittelt (vgl. 3.2.4). Leider misslang dies in einem dritten Fall, da die Behörde, welche für die Hauptniederlassung des Verantwortlichen zuständig war, die sächsische Beschwerde als Hinweis wertete, dem sie nicht nachgehen wollte, weil es keine weiteren Beschwerden dazu gab. Obwohl ich eine ausführliche Begründung in Deutsch und Englisch hierauf in IMI einstellte, dass es sich durchaus um eine Beschwerde handele und die niederländische Behörde als federführende Aufsichtsbehörde für Erlass der entsprechenden Entscheidungen nach Art. 60 Abs. 3 bis 9 zustän-

dig sei, übernahm die niederländische Aufsichtsbehörde das Verfahren nicht. Zurzeit wird geprüft, wie in einem solchen Fall (der in der DSGVO nicht vorgesehen ist) weiter zu verfahren ist.

Ich habe mich auch in einem Fall als federführende Aufsichtsbehörde gemäß Art. 56 Abs. 1 Satz 1 DSGVO im IMI gemeldet, da der Beschwerdegegner seine einzige Niederlassung gemäß Art. 4 Nr. 16 DSGVO in Sachsen hatte.

In einem Verfahren, über das schon im vorangegangenen Tätigkeitsbericht Datenschutz berichtet wurde (Tätigkeitsbericht Datenschutz 2024, 6.2.7, Seite 140 ff.) habe ich wieder die Federführung übernommen. Darin ergab sich Anfang 2024, als der Entwurf eines Bescheides gegen eine Firma im Bereich der E-Mobilität im IMI eingestellt werden sollte, aus dem Handelsregister, dass diese inzwischen von einer anderen Firma mit Sitz in Berlin aufgekauft worden war. Entsprechend dem Dokument des EDSA „Stellungnahme 8/2019 zur Zuständigkeit einer Aufsichtsbehörde im Falle einer Veränderung von Umständen, die die Hauptniederlassung oder die einzige Niederlassung betrifft" vom 9. Juli 2019 (Rn. 35) war die Zuständigkeit damit automatisch auf die Berliner Aufsichtsbehörde übergegangen. Das Verfahren wurde dorthin abgegeben. Eine Sachstandsanfrage Anfang 2025 im IMI der Ungarischen Aufsichtsbehörde, die die Beschwerde an die SDTB abgegeben hatte, führte zu einer erneuten Überprüfung des Handelsregisters und der Feststellung, dass die Firma sich Mitte 2024 wieder ausgegliedert hatte und sich ihre einzige Niederlassung in Leipzig befand. Da in der Kürze der Zeit ihrer Zuständigkeit die Berliner Aufsichtsbehörde nicht den Bescheidentwurf hatte erlassen können und dieser aktualisiert werden muss, ist ein Ende des Verfahrens noch nicht abzusehen. Zuerst einmal muss ich den erneuten Übergang der Federführung auch den übrigen betroffenen Aufsichtsbehörden im IMI mitteilen.

Insgesamt bin ich in fünf Verfahren federführende Aufsichtsbehörde. In einem Verfahren wurde die Beschwerde vom österreichischen Beschwerdeführer zurückgenommen, sodass mit einem entsprechenden Bescheid das Verfahren

abgeschlossen werden kann. In dem anderen Verfahren habe ich den übrigen Aufsichtsbehörden zwar einen vorläufigen Bescheidentwurf vorgestellt, es herrscht aber Uneinigkeit darüber, ob es sich um einen vollständig ablehnenden Bescheid handelt, der gemäß Art. 60 Abs. 8 DSGVO von der schwedischen Aufsichtsbehörde allein zu erlassen ist. Um einen Einspruch der schwedischen Aufsichtsbehorde zu verhindern, wird eine Einigung über den Fortgang weiterhin mit ihr gesucht.

In einem anderen Verfahren, in dem eine andere europäische Aufsichtsbehörde von mir ein Bußgeld oder eine Verwarnung als abschließende Entscheidung forderte (vgl. Tätigkeitsbericht Datenschutz 2024, 6.2.7, Seite 142 f.), wurde inzwischen Einigkeit darüber erzielt, dass das Verfahren eingestellt werden darf. Nach der Rechtsprechung des EuGH (Urteil vom 26.09.2024 – C-768/21, Rz. 43-46) kann das Ergreifen einer Abhilfemaßnahme ausnahmsweise und unter Berücksichtigung der besonderen Umstände des konkreten Falles nicht geboten sein, namentlich, sofern der Situation, die einen Verstoß gegen die DSGVO begründete, bereits abgeholfen wurde, die Verarbeitung personenbezogener Daten im Einklang mit dieser Verordnung durch den hierfür Verantwortlichen gewährleistet ist und ein solches Nichteinschreiten der Aufsichtsbehörde nicht geeignet ist, das Erfordernis eines klar durchsetzbaren Rechtsrahmens zu beeinträchtigen.

Auch die Kommunikation mit den sächsischen Beschwerdeführern auf Veranlassung einer anderen europäischen Aufsichtsbehörde wurde dieses Jahr zweimal in einem Verfahren gegen einen europäischen Anbieter von Verfolgungsdiensten für Transportmittel, der es erlaubte, auch Bewegungen des Beschwerdeführers im Internet sichtbar zu machen, durchgeführt. Die Beschwerde wurde 2021 erhoben; im November 2025 meldete sich erstmals die federführende Aufsichtsbehörde im IMI und bat um Übermittlung eines Schreibens an den Beschwerdeführer mit Fragen zu seiner Beschwerde und einer Entscheidung dieser Behörde, wonach es sich bei den Daten der Transportmittel um personenbezogene Daten handelte, innerhalb von vier Wochen. Die 23 Seiten der Ent-

scheidung und die Anfrage wurden eiligst ins Deutsche übersetzt. Der Beschwerdeführer erhielt die Anfrage umgehend. Dieser antwortete glücklicherweise am letzten Tag der von der europäischen Aufsichtsbehörde unter Androhung einer Entscheidung nach Aktenlage gesetzten Frist. Noch am späten Freitagnachmittag erhielt sie die englische Übersetzung der Stellungnahme des Beschwerdeführers einschließlich einer Entschuldigung dafür, dass er sie am Morgen auch direkt an sie gemailt hatte.

Im Dezember wurde der Beschwerdeführer zur Rückäußerung des Verantwortlichen zu dieser Stellungnahme angehört und seine neue Stellungnahme kurz vor Weihnachten noch ins Englische übersetzt und im IMI eingestellt.

Wie schon im vorangegangenen Jahr nahm ich manchmal die Beratung durch die Zentrale Anlaufstelle (ZASt) beim Bundesbeauftragten für den Datenschutz und die Informationsfreiheit bei schwierigen Fragen in Anspruch, wodurch ich zum Beispiel glücklicherweise darauf hingewiesen wurde, dass bei Beschwerderücknahme die Angelegenheit nicht einfach erledigt ist, sondern den anderen betroffenen Aufsichtsbehörden ein Beschluss zur Einstellung des Verfahrens vorzulegen ist[3]. Gerne besuchten zwei meiner Mitarbeiter/innen zwei IMI-Workshops der ZASt in der Aufsichtsbehörde in Wiesbaden. Gerade im Hinblick auf die kommende DSGVO-Verfahrensordnung[4] ist die Zusammenarbeit bei der Umsetzung der Reformen mit den Kolleginnen und Kollegen anderer deutscher Aufsichtsbehörden im AK Organisation & Struktur und bei den IMI-Workshops wichtig.

Was ist zu tun?

Mit Inkrafttreten der geänderten Verfahrensverordnung 2027 besteht zusätzlicher Personalbedarf in meiner Behörde.

3 Leitlinien 02/2022 zur Anwendung des Artikels 60 DSGVO, Rn. 99 und 116

4 https://www.europarl.europa.eu/news/en/press-room/20251017IPR30992/data-protection-clearer-rules-for-cross-border-enforcement (Stand: 21.10.2025).

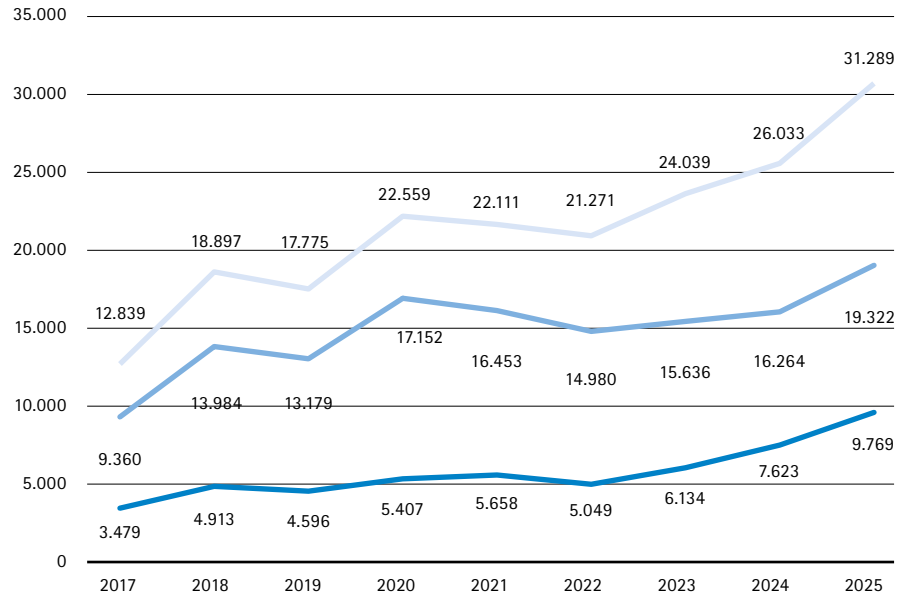


Abbildung 7:
Höchststand beim Schriftgutaufkommen

- Postausgänge
- Posteingänge
- Schriftgut gesamt

6.2.8 Ressourcen

Im Haushaltsjahr 2025 standen mir nach wie vor insgesamt 41 Stellen zur Verfügung. Angesichts des enormen Arbeitszuwachses, der auch in der Schriftgutstatistik zum Ausdruck kommt, bleibt die Situation mehr als herausfordernd, mit den bestehenden Personal- und Sachmitteln meine Aufgaben zu erfüllen. Trotzdem ist es unser Anspruch und unsere gesetzliche Pflicht, allen Bürgerinnen und Bürgern in ihren berechtigten Datenschutzanliegen zu helfen. Die Möglichkeiten, noch effizienter und digital unterstützt zu arbeiten, sind allerdings ausgeschöpft. Dass der Anstieg zulasten von Prävention, allgemeinen Veröffentlichungen, Beratungen und beschwerdeunabhängigen Prüfungen geht, zu denen ich gesetzlich auch verpflichtet bin, versuche ich zu verhindern. Allerdings kann ich mit Blick auf die aktuellen Haushaltsverhandlungen keinerlei Einsparpotenzial bei Personal und Sachhaushalt sehen, da ich sonst meinen gesetzlichen Auftrag nicht mehr erfüllen kann.

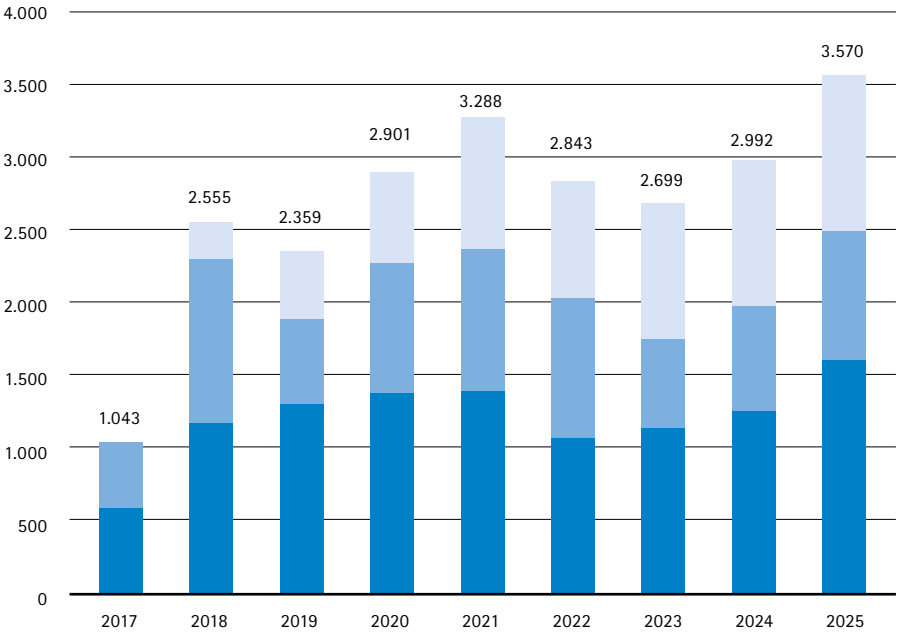


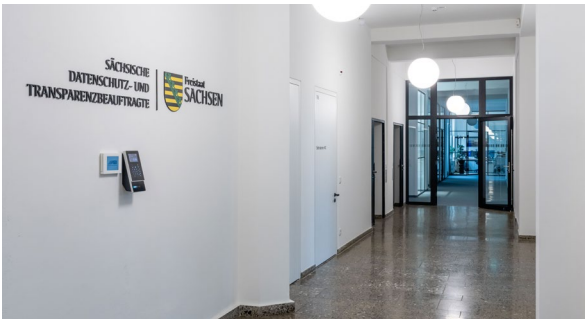
Abbildung 8:
Neuer Höchststand beim Arbeitsaufkommen in wichtigen Tätigkeitsbereichen, bezogen auf die Anzahl der Vorgänge

- Beschwerden/ Kontrollanregungen
- Beratungen
- Meldungen von Datenschutzverletzungen

Umzug der Dienststelle

Das Jahr 2025 war auch geprägt von der vorläufigen Haushalts- und Wirtschaftsführung, während derer grundsätzlich nur die absolut notwenigen Ausgaben oder Beschaffungen zur Aufrechterhaltung des Dienstbetriebes getätigt werden konnten. Nichtsdestotrotz ist es gelungen, den Umzug der Behörde in die neue Liegenschaft erfolgreich und ohne Leistungsausfall zu meistern. Der neue Behördensitz befindet sich seit dem ersten April 2025 in der Maternistraße 17 und somit in unmittelbarer Nachbarschaft zum World Trade Center Dresden. Bis dahin war die Dienststelle auf die Devrientstraße 1 und 5, also auf zwei Standorte, verteilt. Die neue Liegenschaft bietet nun den Vorteil, dass alle Büros an einem Standort vereint sind, was die interne Zusammenarbeit deutlich vereinfacht. Aber noch bedeutender ist, dass ich nun mit meiner Behörde einen Ort habe, an dem mir auch Konferenzräume zur Verfügung stehen, beispielsweise für Fortbildungen und Tagungen. So kann ich noch mehr in die

Abbildung 9:
Dienststelle in der Maternistraße 17 in Dresden



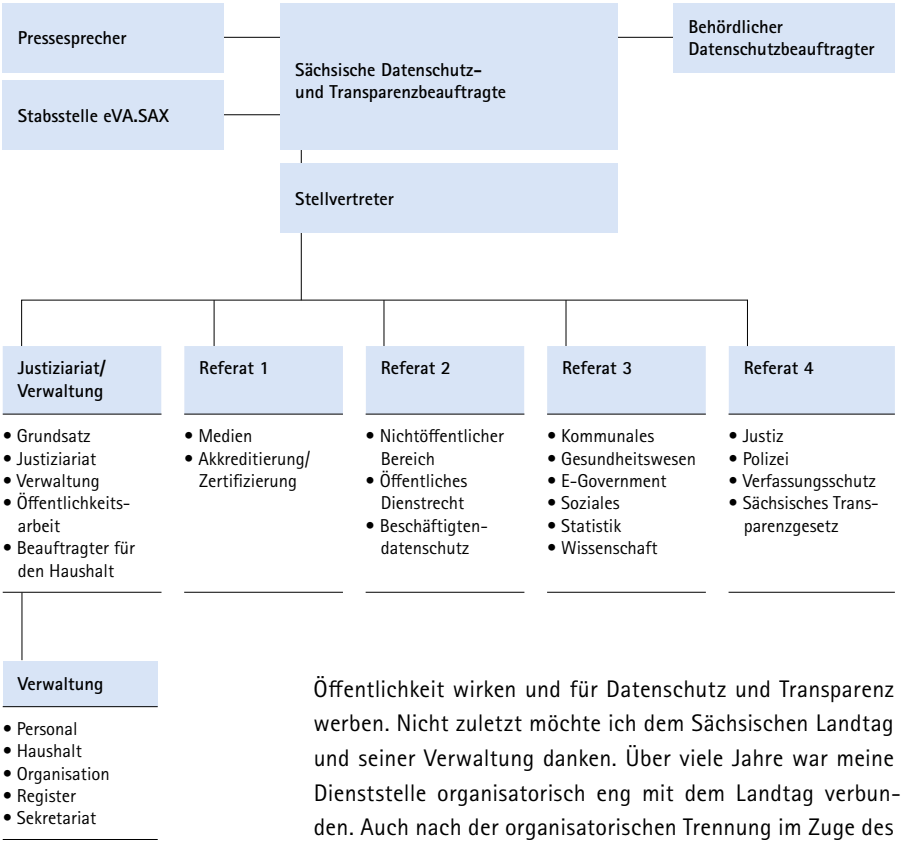


Abbildung 10:
Organigramm der Behörde
(Stand: 31.12.2025)

Öffentlichkeit wirken und für Datenschutz und Transparenz werben. Nicht zuletzt möchte ich dem Sächsischen Landtag und seiner Verwaltung danken. Über viele Jahre war meine Dienststelle organisatorisch eng mit dem Landtag verbunden. Auch nach der organisatorischen Trennung im Zuge des Inkrafttretens der DSGVO hat uns der Landtag immer unbürokratisch unterstützt. Dafür bin ich sehr dankbar.

Fortbildung der Beschäftigten meiner Behörde

Für meine Mitarbeiterinnen und Mitarbeiter lag der Hauptschwerpunkt selbstverständlich auf Fortbildungen in Fragen rund um den Umgang mit KI. Aber auch im Bereich Daten-/Internetrecht und verschiedener IT-Fachverfahren wurden wir umfangreich geschult. Daneben sorge ich im Sinne der Personalentwicklung natürlich auch für Qualifizierung im Bereich Führung, Kommunikation und Selbstentwicklung. Auch auf dem Gebiet der Fachkenntnisse der englischen Sprache bilden sich meine Mitarbeiterinnen und Mitarbeiter stetig fort.

Stabsstelle eVA.SAX

Nach der Einführung der elektronischen Vorgangsbearbeitung und Aktenführung in meiner Behörde zum 1. April 2024 konnte das Einführungsprojekt für weitestgehend alle Bereiche der Dienststelle abgeschlossen werden.
Unter Berücksichtigung der vorhandenen Rahmenbedingungen ist jedoch die Betreuung weiter sicherzustellen, laufende Prozesse stetig anzupassen und gegebenenfalls Erweiterungen von eVA.SAX im Wege der Verwaltungsdigitalisierung weiter voranzubringen oder fortzuschreiben.
Dazu bleibt die „Stabsstelle eVA.SAX" dauerhaft bestehen. Die Stabsstelle ist direkt der Behördenleitung unterstellt, berät diese bei erforderlichen Maßnahmen und setzt diese nach der Entscheidung durch die Behördenleitung und nach entsprechender Abstimmung mit dem Personalrat um.

Was ist zu tun?
Aufgrund des starken Anstiegs bei Beschwerden und Kontrollanregungen, Beratungsanfragen sowie Datenpannen ist meine Behörde personell besser auszustatten.

6.3 Datenschutzaufsichtliche Befugnisse, verwaltungsrechtliche Entscheidungen

6.3.1 Abhilfemaßnahmen

Um Verstöße gegen die DSGVO zu ahnden, kann ich nach Art. 58 Abs. 2 DSGVO verschiedene Abhilfemaßnahmen ergreifen. Davon habe ich im Berichtszeitraum wie folgt Gebrauch gemacht:

- Warnungen: 2
- Verwarnungen: 19
- Anweisungen und Anordnungen: 69
- Geldbußen (nur nach DSGVO): 8
- Widerruf von Zertifizierungen: 0

6.4 Geldbußen und Sanktionen, Strafanträge

6.4.1 Ordnungswidrigkeitenverfahren im öffentlichen Bereich

Als Sächsische Datenschutz- und Transparenzbeauftragte war ich im Berichtszeitraum zuständig für die Verfolgung und Ahndung von Ordnungswidrigkeiten im öffentlichen Bereich nach

- § 22 Abs. 1 Sächsisches Datenschutzdurchführungsgesetz (§ 22 Abs. 3 SächsDSDG),
- § 48 Abs. 1 Sächsisches Datenschutz-Umsetzungsgesetz (§ 48 Abs. 3 Satz 1 SächsDSUG),
- § 66 Abs. 1 Sächsisches Justizvollzugsdatenschutzgesetz (§ 66 Abs. 3 SächsJVollzDSG),
- § 93 Abs. 1 Sächsisches Psychisch-Kranken-Hilfe-Gesetz (§ 93 Abs. 1 SächsKHG) und
- § 85a des Zehnten Buches Sozialgesetzbuch – Sozialverwaltungsverfahren und Sozialdatenschutz – in Verbindung mit § 41 Bundesdatenschutzgesetz (BDSG), Art. 83 Abs. 5 Datenschutz-Grundverordnung (Art. 58 Abs. 2 Buchst. i DSGVO, § 14 Abs. 1 SächsDSDG).

Im Berichtszeitraum waren im öffentlichen Bereich insgesamt 66 Bußgeldverfahren anhängig. Davon wurden 12 mit einem Bußgeld abgeschlossen, wobei in einem Verfahren Einspruch gegen den erlassenen Bußgeldbescheid eingelegt worden ist. Eine Entscheidung steht noch aus. In zwei Verfahren aus dem vorherigen Berichtszeitraum ist der Bußgeldbescheid dem Grunde nach gerichtlich bestätigt worden. In einem weiteren Verfahren erfolgte ein Freispruch. 30 Verfahren befanden sich zum Ende des Berichtszeitraumes noch in Bearbeitung.

Berichtszeitraum		01.01. – 31.12.2025
anhängig gesamt		**66**
davon	Verfahren aus vorherigem Berichtszeitraum	19
	neu eingegangene Verfahren	47
abgeschlossen		**36**
davon	mit Bußgeld	12
	mit Verwarnungsgeld	0
	mit Verwarnung ohne Verwarnungsgeld	0
	eingestellt/von Verfolgung abgesehen	24
	an zuständige Behörde abgegeben	0
noch in Bearbeitung		**30**
Summe festgesetzter Buß- und Verwarnungsgelder in Euro		**7.600**

Tabelle 5:
Ordnungswidrigkeiten-verfahren im öffentlichen Bereich

Die Summe der festgesetzten Buß- und Verwarnungsgelder belief sich auf 7.600 Euro, die der rechtskräftigen auf 7.280 Euro. Die Differenz der Beträge erklärt sich aus dem Umstand, dass gegen einen Bußgeldbescheid Einspruch eingelegt wurde, über den bislang noch nicht gerichtlich entschieden wurde.

Gegenüber dem vergangenen Berichtszeitraum ist die Zahl der neu eingegangenen Ordnungswidrigkeitenverfahren leicht gestiegen. Ein Großteil der zu bearbeitenden Verfahren ist sehr komplex und mit einem erhöhten Ermittlungs- und Bearbeitungsaufwand verbunden.

Der Anteil von Ordnungswidrigkeitenverfahren, in denen Bedienstete der sächsischen Polizei in Verdacht standen oder stehen, unbefugt dienstlich erlangte personenbezogene Daten verarbeitet zu haben (ordnungswidrig gemäß § 48 Abs. 1 Nr. 1 Sächsisches Datenschutz-Umsetzungsgesetz [SächsDSUG]), ist von 85 % im vorherigen Berichtszeitraum auf nunmehr 50 % gesunken. In den verbleibenden Verfahren richtet oder richtete sich der Verdacht gegen Be-

dienstete unterschiedlichster sächsischer (Sozial-)Behörden, darunter zum Beispiel Bedienstete von Stadtverwaltungen, Schulen, Universitätsklinika oder Krankenkassen. Bislang resultierte der Mehranteil an Ordnungswidrigkeitenverfahren gegen sächsische Polizeibedienstete aus einem überdurchschnittlichen Anzeigeverhalten der Polizeidienststellen, welche datenschutzrechtliche Verstöße – auch dienstrechtlich – konsequent verfolgen. In diesem Berichtszeitraum war ein deutlicher Anstieg an Anzeigen zu verzeichnen, die sich gegen Bedienstete anderer sächsischer Behörden richteten. Diese Verfahren wurden überwiegend nicht durch die betroffenen öffentlichen Stellen selbst, sondern durch private Anzeigenerstatter/innen angestoßen.

Auch in diesem Berichtszeitraum betrafen die Ordnungswidrigkeitenverfahren regelmäßig privat motivierte Datenabrufe aus den dienstlichen Auskunfts- bzw. Informationssystemen zu Freunden/Freundinnen, Kollegen/Kolleginnen, Nachbarn/Nachbarinnen oder anderen Bekannten. Häufiger Gegenstand der Verfahren war zudem die unbefugte Übermittlung von dienstlich erlangten personenbezogenen Daten an Dritte.

Zwei Fälle, welche in dem Berichtszeitraum besonders herausragten, werden nachfolgend vorgestellt:

6.4.1.1 Zahlreiche Datenabfragen durch einen Staatsanwalt

↗ § 2 Nr. 3 SächsDSUG, OWiG

Im Jahr 2024 wurde mir von einer Staatsanwaltschaft ein Ermittlungsverfahren zur Verfolgung etwaiger datenschutzrechtlicher Ordnungswidrigkeiten übergeben. Das Ermittlungsverfahren richtete sich gegen einen dort tätigen Staatsanwalt. In einer Abteilung der betreffenden Staatsanwaltschaft war bekannt geworden, dass es in der Vergangenheit zu Zugriffen in den elektronischen Vorgangsbearbeitungssystemen durch abteilungsfremde Bedienstete gekommen war. Um festzustellen, wer konkret diese unberechtigten Datenzugriffe vornahm, wurde im Vorgangsbearbeitungssystem in einem zum damaligen Zeitpunkt aktuellen, presseträchtigen Verfahren eine Datei unter der

Bezeichnung „Haftbefehl" eingestellt. Bei der Datei handelte es sich allerdings nicht um einen tatsächlichen Haftbefehl oder ein Dokument mit inhaltlichen Angaben zum Verfahren, sondern um ein Dokument mit dem ausdrücklichen Hinweis darauf, dass Zugriffe auf Dokumente aus fremden Verfahren ohne einen dienstlichen Anlass als problematisch anzusehen und zu unterlassen sind. Wie auch bei der sächsischen Polizei werden Datenzugriffe in den elektronischen Systemen der Staatsanwaltschaften im Hintergrund protokolliert. Um herauszufinden, welche Personen die als „Haftbefehl" gekennzeichnete Datei geöffnet hatten, veranlasste die Staatsanwaltschaft daher eine Auswertung der Protokolldaten. Hierbei stellte man fest, dass eine geringe Zahl abteilungsfremder Bediensteter die Datei geöffnet hatte. Bei der Überprüfung weiterer Zugriffe stellte sich heraus, dass ein Staatsanwalt wiederholt auf zahlreiche fremde Verfahren zugegriffen hatte. Ein Bezug der Tätigkeit des Staatsanwalts zu den jeweiligen Strafverfahren, auf die er zugegriffen hatte, war für die Dienststelle nicht ersichtlich.

Gegen den betreffenden Staatsanwalt habe ich ein Ordnungswidrigkeitenverfahren eingeleitet, welches über 70 unbefugte Datenrecherchen zum Gegenstand hatte. Zum Grund der Datenabfragen gab der betroffene Staatsanwalt an, er habe die Verfahren aus fachlichem Interesse gelesen. Er habe sich so darüber informieren wollen, wie die Verfahren in anderen Abteilungen bearbeitet würden, da sich die Straftaten und deren Aufklärung deutlich von den Taten in seiner eigenen Abteilung unterschieden hätten. Ihm sei nicht bewusst gewesen, dass bereits der bloße Abruf von Verfahren, zu denen er keinen konkreten dienstlichen Bezug hatte, gegen datenschutzrechtliche Normen verstoße. Er sei davon ausgegangen, dass lediglich die Weitergabe von Daten rechtswidrig sei.

Wie für alle öffentliche Stellen gilt auch für die Staatsanwaltschaften, dass jede Verarbeitung personenbezogener Daten einen konkreten dienstlichen Anlass erfordert. Unter den Begriff der Datenverarbeitung fällt allerdings nicht nur die Übermittlung von Daten an Dritte, sondern ge-

mäß § 2 Nr. 3 Sächsisches Datenschutz-Umsetzungsgesetz (SächsDSUG) auch das Auslesen und Abfragen von personenbezogenen Daten. Dass der Betroffene sich als ermittelnder Staatsanwalt für das Ermittlungsvorgehen in Strafverfahren anderer Art interessierte, war zwar nachvollziehbar, gleichwohl begründet das allgemeine Interesse an anderen Verfahrensweisen keinen dienstlichen Anlass, der zum Abruf von Verfahrensdaten mit Personenbezug berechtigt. Die Befassung mit fremden Vorgängen zu Schulungs- oder Fortbildungszwecken kann datenschutzrechtlich zulässig sein – hierfür braucht es allerdings eine Befugnis, die den konkreten Bediensteten zu den Datenabfragen berechtigt (zum Beispiel in Form einer Genehmigung durch den entsprechenden Vorgesetzten bzw. die Dienststelle). In diesem Fall war der Betroffene nicht berechtigt, sich als „Ersatz" für Fortbildungsveranstaltungen mit Verfahren anderer Abteilungen zu befassen. Hinzu kam, dass dem Staatsanwalt spätestens nach dem Öffnen der als „Haftbefehl" gekennzeichneten Datei, die den Hinweis auf die Problematik unzulässiger Datenabrufe enthielt, hätte bewusst sein müssen, dass sein Handeln im Hinblick auf datenschutzrechtliche Bestimmungen bedenklich war. Dennoch nahm er auch in der Folgezeit weitere unberechtigte Datenabfragen vor.
Dass der Betroffene die Verstöße vollumfänglich einräumte und Einsicht für sein Fehlverhalten zeigte, habe ich bei der Zumessung der Geldbuße mildernd berücksichtigt.

6.4.1.2 Systematische Kontrolle von Kollegen und Kolleginnen durch einen Polizeibediensteten

↗ OWiG

In einem weiteren Vorgang erging nach einem langwierigen Verfahren in diesem Berichtszeitraum eine gerichtliche Entscheidung über einen im Jahr 2024 erlassenen Bußgeldbescheid. Anlass für dieses Ordnungswidrigkeitenverfahren bot ein Polizeibeamter, der Strafanzeigen und Dienstaufsichtsbeschwerden gegen mehrere Kollegen und Kolleginnen seiner Organisationseinheit wegen vermeintlicher Untätigkeit und Arbeitszeitbetrugs erstattet hatte. Über viele Monate

hinweg hatte der Beamte systematisch deren Arbeitsweise und Aufgabenerledigung kontrolliert und dokumentiert, da diese nach seiner Auffassung schwere Pflichtverletzungen begangen hatten. Aus seiner Strafanzeige und Dienstaufsichtsbeschwerde ging hervor, dass der Bedienstete unbefugt Bilder von polizeilichen Schriftstücken gefertigt sowie über einen Zeitraum von mindestens sechs Monaten Einsicht in die Arbeitszeitkonten mehrerer Kolleginnen und Kollegen genommen und davon Screenshots gefertigt hatte. Seine faktischen Zugriffsrechte für die Arbeitszeitkonten hatte der Polizeibeamte noch aus seiner vorherigen Verwendung an einem anderen Dienstort behalten – bei seinem Wechsel schien von der Dienststelle versäumt worden zu sein, ihm diese Rechte wieder zu entziehen. Darüber hinaus ergab eine Auswertung der Protokolldaten, dass der Polizeibeamte Datenabfragen in den polizeilichen Informationssystemen zu den von ihm beschuldigten Kollegen und Kolleginnen getätigt hatte.

Der Betroffene und sein Verteidiger rechtfertigten das Verhalten mit der allgemeinen Verfolgungspflicht, die den Betroffenen als Polizeibeamten treffe. Sämtliche Handlungen hätten dem Ziel gedient, die Pflichtverletzungen seiner Kolleginnen und Kollegen offenzulegen. Er habe daher auch Strafanzeige und Dienstaufsichtsbeschwerde gegen die Kollegen und Kolleginnen erhoben. Der Verteidiger verwies zudem darauf, dass dem Betroffenen in seiner vorigen Tätigkeit rechtmäßig die Zugriffsrechte für das Programm zur Arbeitszeiterfassung erteilt worden waren und diese zu keinem Zeitpunkt eingeschränkt worden seien. Dem Beamten sei nach seinem Dienstortwechsel nicht mitgeteilt worden, dass er die Einsichtsrechte in das Programm nicht mehr nutzen dürfe.

Diesen Erwägungen konnten meine Behörde und das Gericht nicht folgen. Wenngleich sich für Polizeibeamte aus ihrem Amt eine gewisse Garantenstellung hinsichtlich der öffentlichen Sicherheit und Ordnung herleitet, ergeben sich aus ebendieser beruflichen Stellung auch Einschränkungen bzw. Voraussetzungen für ein Tätigwerden. So müsste der

Polizeibeamte nach seiner konkreten Dienstpflicht örtlich und sachlich für das geschützte Rechtsgut verantwortlich sein. Zur Vermeidung polizeiinterner Parallelstrukturen und Zuständigkeitsschwierigkeiten ergibt sich aus der allgemeinen polizeilichen Handlungsbefugnis keineswegs eine umfassende – und bei Dauerdelikten über einen längeren Zeitraum angelegte – Ermittlungsbefugnis eines jeden Polizeibeamten für jeden Straftatverdacht. Handelt ein Polizeibeamter außerhalb seines örtlichen und sachlichen Zuständigkeitsbereichs, so hat er entweder selbst einen Vorgang anzulegen und ihn umgehend an die zuständige Organisationseinheit abzugeben oder jedenfalls über Anlass, Gegenstand und Ergebnis der (bisherigen) Ermittlungen einen Aktenvermerk zu fertigen und diesen an die örtlich und sachlich zuständige Polizeidienststelle zur Einleitung eines Vorgangs weiterzuleiten (vgl. OLG Bamberg, Beschluss vom 28.08.2018, Az. 2 Ss OWi 949/18). Der Beamte in diesem Fall war weder örtlich noch sachlich zuständig für gegen seine Kollegen und Kolleginnen gerichtete Ermittlungshandlungen, die er im Stillen über viele Monate geführt hatte.

Hinsichtlich der Ausführungen des Verteidigers bezüglich der Zugriffsrechte habe ich darauf verwiesen, dass auch eine innerdienstliche Zugriffsberechtigung nicht von dem Erfordernis der dienstlichen Veranlassung für Datenverarbeitungen in dienstlichen Dateisystemen befreit. Aus der technischen Zugriffsmöglichkeit oder dem Zugriffsstatus bestimmter Daten lässt sich keine Aussage über die Befugnis des einzelnen Beamten, diese abzurufen, ableiten. Nicht die Zugriffsmöglichkeit, sondern der dienstliche Anlass ist die Voraussetzung für einen befugten Abruf personenbezogener Daten aus dienstlichen Dateien. Aufgrund der weiteren Umstände des Sachverhalts war auch davon auszugehen, dass dem Beamten bewusst gewesen sein musste, dass die wohl versehentlich belassenen Zugriffsrechte nicht mit seiner dienstlichen Stellung im Einklang standen und er damit trotz technischer Möglichkeit dienstlich nicht befugt war, die Dienstzeiten seiner Kolleginnen und Kollegen einzusehen. Aus datenschutzrechtlicher Sicht kam erschwerend hinzu,

Was ist zu tun?
Eine Verarbeitung amtlicher personenbezogener Daten für private oder sonstige dienstfremde Zwecke ist keine geringfügige Verfehlung. Die Bediensteten der Behörden und öffentlichen Stellen in Sachsen als nach außen agierende Vertreterinnen und Vertreter des Freistaats sind insoweit auch künftig zu ihrer besonderen Pflichtenwahrung und Vorbildwirkung zu ermahnen. Der Ahndung von Ordnungswidrigkeiten im öffentlichen Bereich kommt nach wie vor besondere Bedeutung zu. Die Dienststellen sind verpflichtet, Zugriffsrechte auf behördliche Informationen stets aktuell zu erteilen bzw. zu entziehen.

dass der Beamte nicht nur die Arbeitszeiten der beschuldigten Kollegen und Kolleginnen, sondern gleichfalls von unbeteiligten Dritten abgerufen hatte.
Das zuständige Amtsgericht folgte auch dieser Auffassung und bestätigte den Bußgeldbescheid bei einer Reduzierung des Bußgeldes dem Grunde nach.

6.4.2 Ordnungswidrigkeitenverfahren im nichtöffentlichen Bereich

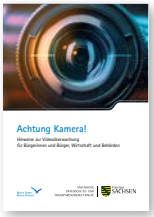
↗ Art. 83 DSGVO

Im Berichtszeitraum hatte ich 114 neue Ordnungswidrigkeitenanzeigen zu verzeichnen – das bedeutet eine Steigerung um 37 % gegenüber dem Vorjahr (83). Mehr als die Hälfte der Anzeigen (64) bezog sich dabei auf den Betrieb von Überwachungskameras (stationäre Kameras: 55, Dashcams: 7, Drohnen: 2). Damit liegt der Schwerpunkt (56 %) der bei mir eingegangenen Ordnungswidrigkeitenanzeigen auch weiterhin klar bei der Videoüberwachung (Vorjahr: 70 %).
Insgesamt waren damit im Berichtszeitraum 210 Ordnungswidrigkeitenverfahren bei mir anhängig. Von diesen konnte ich 121 Fälle abschließen und habe dabei acht Bußgelder festgesetzt.
Fünf Bußgelder betrafen den unrechtmäßigen Dashcam-Einsatz. Die Höhe dieser Bußgelder bewegte sich zwischen 75 Euro und 1.000 Euro. Vier Bußgelder wurden gegen Privatpersonen festgesetzt; das fünfte Bußgeld gegen einen Berufskraftfahrer. Dabei handelt es sich um einen Busfahrer im Reiseverkehr, der tatsächlich unverschuldet in einen Verkehrsunfall verwickelt worden war. Diesbezüglich konnte die Dashcam zwar den Unfallhergang betreffend verwertbare Beweismittel liefern, jedoch änderte dies nichts an der Tatsache, dass die Dashcam zuvor datenschutzwidrig eingesetzt worden war. Auf der sichergestellten Speicherkarte befanden sich eben nicht nur (die zulässigen) Videoaufnahmen des Unfallgeschehens, sondern auch fast acht Stunden anlassfrei erstellte Videoaufnahmen der vorangegangenen Fahrt wie auch von Standzeiten des Reisebusses. Erschwe-

Berichtszeitraum		01.01. – 31.12.2025
anhängig gesamt		**210**
davon	Verfahren aus vorherigem Berichtszeitraum	96
	neu eingegangene Verfahren	114
abgeschlossen		**121**
davon	mit Bußgeld	8
	eingestellt/von Verfolgung abgesehen	108
	an zuständige Behörde abgegeben	5
noch in Bearbeitung		**89**
Summe festgesetzte Bußgelder in Euro		**10.875**

Tabelle 6:
Ordnungswidrigkeitenverfahren im nichtöffentlichen Bereich

rend hinzu kam, dass auch die Mikrofonfunktion der Kamera aktiviert gewesen war, sodass insbesondere auch Audioaufnahmen der Reiseteilnehmer/innen und des Reiseleiters erstellt worden waren. Da (in Unkenntnis der Audioaufnahmen) keine Strafanträge durch betroffene Personen gestellt worden waren, hatte die Staatsanwaltschaft mir das Verfahren zur weiteren Verfolgung als Ordnungswidrigkeit übergeben.
Zwei Bußgelder habe ich wegen des unrechtmäßigen Betriebs stationärer Videokameras festgesetzt. Ein Bußgeld in Höhe von 7.500 Euro betraf einen Gastronomiebetrieb, in dem der gesamte Innenbereich (Gastraum, Arbeitsbereiche, insbesondere auch die Küche), mit Ausnahme der Toiletten, die Außensitze und auch die angrenzende Fußgängerpassage in ihrer gesamten Breite mittels einer Vielzahl von Videokameras überwacht worden waren. Die dabei entstandenen Videoaufnahmen von den Gästen des Gastronomiebetriebs, seinen Beschäftigten sowie von Passanten speicherte der Betreiber für mindestens 48 Stunden auf einem Videorekorder. Begründet wurde der Betrieb der Videoüberwachungsanlage lediglich mit einer abstrakten Gefahrenlage infolge der Grenznähe des Gastronomiebetriebs; konkrete Vorfälle konnten bis auf eine allgemein gehaltene Behauptung eines



„Achtung Kamera!" als PDF:
↗ sdb.de/achkam

„Achtung Kamera!" als gedruckte Broschüre:
↗ publikationen.sachsen.de/bdb/artikel/43382

Pflanzendiebstahls aus dem Außensitzbereich nicht benannt werden. Dies war keinesfalls ausreichend; zur Interessenwahrung (Eigentumsschutz) hätte es vorliegend ausgereicht, wenn sich die Videoüberwachung örtlich auf den Gastronomiebetrieb und zeitlich auf die Schließzeiten beschränkt hätte.

Tatsächlich war die Videoüberwachungsanlage aber 24 Stunden täglich in Betrieb. Die Überwachung der angrenzenden Fußgängerpassage war zu keiner Zeit zulässig. Der Inhaber des Gastronomiebetriebs hatte zudem weder ordnungsgemäß auf die Videoüberwachung hingewiesen, noch eine Datenschutz-Folgenabschätzung durchgeführt und auch keinen Datenschutzbeauftragten benannt. Auch ein Verzeichnis der Verarbeitungstätigkeiten war nicht vorhanden.

Das andere Bußgeld betraf gleichfalls eine Fußgängerpassage, die an einer Engstelle durch ein Gebäude hindurchführte. In diesem Durchgang, in dem sich auch ein Hauseingang befand, waren durch die Hausverwaltung zwei Videokameras betrieben worden. Mit diesen Kameras sollten Einbrüche und Sachbeschädigungen jedweder Art verhindert und aufgeklärt werden; die erstellten Videoaufzeichnungen waren für einen Zeitraum von bis zu sieben Tagen gespeichert worden. Von der Videoüberwachung betroffen waren der gesamte Passantenstrom sowie auch alle Personen, die eines der im Gebäude ansässigen und über den Durchgang erreichbaren Unternehmen betreten oder verlassen haben. Der Betrieb dieser beiden Kameras war rechtswidrig: Nichtöffentliche Stellen haben – im Gegensatz zur öffentlichen Hand –, von notwehrähnlichen Situationen abgesehen, nicht das Recht, durch Videoaufzeichnungen Passanten auf öffentlichen Wegen zu erfassen. Die Überwachung des öffentlichen Verkehrs ist eine staatliche und nicht von Privatpersonen oder -unternehmen wahrzunehmende Aufgabe (vgl. 1.1). Die Hausverwaltung hatte bereits im vorangegangenen Aufsichtsverfahren die beiden Kameras demontiert, alle Aufzeichnungen gelöscht und sich auch sonst kooperativ gezeigt, sodass es bei einem vergleichsweise geringen Bußgeld in Höhe von 500 Euro belassen werden konnte.

Was ist zu beachten?
Bislang sind nur wenige Dashcam-Modelle überhaupt datenschutzkonform einsetzbar. Wer hier auf Billigmodelle setzt und die Einhaltung der datenschutzrechtlichen Vorgaben nicht sorgfältig prüft, setzt sich dem Risiko eines erheblichen Bußgeldes aus.

Das letzte Bußgeld (100 Euro) wurde gegen eine Privatperson festgesetzt, die mit ihrem Smartphone in das Gelände eines Polizeireviers hineingefilmt und diese auch personenbezogene Daten enthaltende Aufnahme anschließend auf Instagram veröffentlicht hatte. Das Gelände des Polizeireviers war deutlich sichtbar und für jedermann erkennbar mit einem Verbot der Anfertigung von Foto-, Video-, Streaming- und Tonaufnahmen versehen gewesen.

6.4.3 Erzwingungshaft

↗ §§ 66, 96 OWiG

Betroffene haben die Möglichkeit, gegen einen Bußgeldbescheid mit einem Einspruch vorzugehen. Unterlassen sie dies oder nehmen sie einen eingelegten Einspruch zurück, wird der Bußgeldbescheid rechtskräftig und kann durch die Verwaltungsbehörde vollstreckt werden. Praktisch obliegt dies den Finanzämtern. Nicht immer ist die Vollstreckung aber von Erfolg gekrönt. Werden Betroffene wiederholt nicht angetroffen oder können kein pfändbares Eigentum vorweisen, geht die Vollstreckung ins Leere.
Solange die Betroffenen dabei nicht ihre Zahlungsunfähigkeit nachvollziehbar dargelegt haben, gilt es zu vermeiden, die Bußgeldforderung einfach niederzuschlagen und damit die Beitreibung aufzugeben. Andernfalls stünde es im Belieben hartnäckiger Schuldner/innen, ihre Geldbußen nicht zu bezahlen. Auch der Bezug von Sozialleistungen wie beispielsweise Sozialhilfe oder Arbeitslosengeld befreit nicht von der Zahlungsverpflichtung. Sonst bestünde auch hier die Gefahr, dass dieser Personenkreis Ordnungswidrigkeiten begehen könnte, ohne befürchten zu müssen, zur Verantwortung gezogen zu werden.
Die Anordnung der Erzwingungshaft nach § 96 Ordnungswidrigkeitengesetz (OWiG) ist für derartige Fälle gesetzlich als wirksames Beugemittel vorgesehen, um einen mutmaßlich zahlungsfähigen, aber zahlungsunwilligen Betroffenen zur Zahlung der festgesetzten Geldbuße zu veranlassen. Dabei ist zu beachten, dass die Erzwingungshaft nicht an die

Stelle der Geldbuße tritt, sondern deren Durchsetzung dient. Praktisch bedeutet dies allerdings auch, dass man eine Geldbuße dennoch aussitzen kann, denn weitere Vollstreckungsmaßnahmen bestehen dann nicht mehr; die Erzwingungshaft darf in gleicher Sache nicht wiederholt werden (§ 96 Abs. 3 Satz OWiG).

Voraussetzung der Erzwingungshaft ist ein entsprechender Antrag der Verwaltungsbehörde, der wiederum einer vorherigen Belehrung des Betroffenen bedarf. Tatsächlich ist diese Belehrung, dass Erzwingungshaft angeordnet werden kann, wenn der Betroffene weder das Bußgeld bezahlt noch seine Zahlungsunfähigkeit darlegt, aber notwendiger Bestandteil jedes Bußgeldbescheides (§ 66 Ab. 2 Nr. 3 OWiG). Die Erzwingungshaft darf nur wegen der Bußgeldforderung beantragt werden; die Zahlung der Verfahrenskosten ist auf diese Weise nicht zu erzwingen. Da es sich um eine freiheitsentziehende Maßnahme handelt, ist das Amtsgericht für die Anordnung zuständig. Das Amtsgericht entscheidet durch Beschluss; vorab erhält der Betroffene natürlich noch rechtliches Gehör.

Auf die Höhe der Geldbuße kommt es nicht an. Auch bei geringen Geldbußen wird mit einem diesbezüglichen Antrag nicht der Grundsatz der Verhältnismäßigkeit verletzt, weil die Erzwingungshaft jederzeit durch Zahlung der Geldbuße abgewendet werden kann.

Tatsächlich dürfte die Erzwingungshaft im Ergebnis jedoch kaum vollstreckt werden, da der mit der gerichtlichen Anhörung, dem gegebenenfalls nachfolgenden Beschluss zur Anordnung der Erzwingungshaft und der sich anschließenden Ladung zum Haftantritt ein erheblicher Druck auf die Betroffenen ausgeübt wird, sodass deren Bereitschaft zur Zahlung oder nachträglichen Darlegung der Zahlungsunfähigkeit entsprechend steigt.

Im Berichtszeitraum habe ich in zwei Fällen Erzwingungshaft beantragt. In ersten Fall ging es um ein Bußgeld in Höhe von 1.000 Euro wegen einer rechtswidrigen Videoüberwachung. Hier hat das Amtsgericht eine Erzwingungshaft von fünf Tagen angeordnet, deren Vollstreckung jedoch erst Mitte 2026

vorgemerkt ist. Grund dafür ist, dass der Betroffene bereits wegen einer Straftat in Haft ist und die Erzwingungshaft daher erst unmittelbar im Anschluss daran vollstreckt werden kann. Mit einer Zahlung des Bußgeldes ist in diesem Fall wohl eher nicht zu rechnen. Der andere Fall betraf eine Bußgeldforderung in Höhe von 600 Euro wegen eines rechtswidrigen Dashcam-Einsatzes. Hier hat bereits die gerichtliche Anhörung des Betroffenen dazu geführt, dass er nun Zahlungsbereitschaft signalisiert und um entsprechende Zahlungserleichterungen (Ratenzahlung) ersucht hat.

Was ist zu beachten?
Wer ein rechtskräftig festgesetztes Bußgeld nicht bezahlt und auch keine Zahlungsunfähigkeit nachweisen kann, muss auch bei geringen Bußgeldern mit der gerichtlichen Anordnung der Erzwingungshaft rechnen.

6.4.4 Änderung der Sächsischen Justizorganisationsverordnung

↗ § 68 Abs. 1, 3 OWiG, § 25 Abs. 1 SächsJOrgVO

Soweit gegen Bußgeldbescheide meiner Behörde wegen datenschutzrechtlicher Ordnungswidrigkeiten seitens der Betroffenen Einspruch eingelegt wird und keine Rücknahme des Bescheids erfolgt, ist im amtsgerichtlichen Verfahren zu entscheiden. In den Berichtszeiträumen werden immer wieder entsprechende Verfahren mit Beteiligung meiner Dienststelle als Verwaltungsbehörde eröffnet. Gemäß § 68 Abs. 1 Gesetz über Ordnungswidrigkeiten (OWiG) ist das Amtsgericht, in dessen Bezirk die Verwaltungsbehörde ihren Sitz hat, zuständig. Der Richter beim Amtsgericht entscheidet allein. Demgegenüber legte § 25 Abs. 1 Sächsische Justizorganisationsverordnung (SächsJOrgVO) seit ihrer Änderung im Jahre 2008 und in Anwendung von § 68 Abs. 3 OWiG abweichend fest, dass, soweit der Bezirk der Verwaltungsbehörde mehrere Amtsgerichtsbezirke umfasst, das Amtsgericht am Begehungsort über den Einspruch gegen den Bußgeldbescheid zu entscheiden hat. Dies betraf auch meine Behörde. Mit der Änderung im Jahr 2008 war die Zuständigkeit zur Entscheidung über den Einspruch gegen Bußgeldbescheide in Datenschutzangelegenheiten vom bis dahin zuständigen Amtsgericht Dresden, das Amtsgericht am Sitz der Sächsischen Datenschutz- und Transparenzbeauftragten, auf die Amtsgerichte am jeweiligen Begehungsort übergegangen.

Diese Änderung hatte sich, was Verfahren wegen datenschutzrechtlicher Ordnungswidrigkeiten angeht, nach meiner Überzeugung nicht bewährt, da es den Gerichten im Ergebnis an Erfahrungswerten fehlte, eine verlässliche Spruchpraxis im Hinblick auf die Bemessung der Geldbuße und die Vollzugspraxis nicht entwickelt werden konnte und eine juristische Spezialisierung verhindert wurde. Ebenso war einzubeziehen, dass bei gleichartiger Sach- und Aktenlage in einer europarechtlichen Rechtsmaterie die Entwicklung einer einheitlichen Rechtsprechungspraxis gehemmt werden würde.

Übertragbar waren die vorgenannten Nachteile auf die in den jeweiligen Amtsgerichtsbezirken zuständigen Staatsanwaltschaften, auf die die Zuständigkeit für das Verfahren von meiner Behörde übergeht, wenn der Einspruch nicht zur Rücknahme des Bußgeldbescheids führt, und die es zur Vorlage an das Amtsgericht bringen.

Gegenüber dem Justizministerium hatte ich 2025 daher angeregt, die entsprechende Vorschrift, § 25 Abs. 1 der Sächsischen Justizorganisationsverordnung, wieder abzuändern, sodass für die Verfahren wieder das Amtsgericht am Sitz meiner Behörde zuständig ist. In der Sache verlief die weitere Erörterung mit dem Ministerium offen, und meinem Anstoß wurde gefolgt.

Eine entsprechende Änderungsverordnung wurde im Sächsischen Gesetz- und Verordnungsblatt vom 22. Oktober 2025 verkündet und trat zum 1. November 2025 als Fünfzehnte Verordnung des Sächsischen Staatsministeriums der Justiz zur Änderung der Sächsischen Justizorganisationsverordnung (Sächsische Justizorganisationsverordnung – SächsJOrgVO) in Kraft.

Was ist zu beachten?
Mit Inkrafttreten der geänderten Sächsischen Justizorganisationsverordnung ab 1. November 2025 ist für Einsprüche gegen Bußgeldbescheide der Sächsischen Datenschutz- und Transparenzbeauftragten das Amtsgericht Dresden zuständig.

6.5 Öffentlichkeitsarbeit

6.5.1 Onlinekommunikation und Publikationen

Eine professionelle Öffentlichkeitsarbeit ist mir ein wichtiges Anliegen. Deshalb habe ich sie im Berichtszeitraum weiterentwickelt. Mit ihr erfülle ich die in der Datenschutz-Grundverordnung festgelegte Aufgabe, die Öffentlichkeit für die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung von personenbezogenen Daten zu sensibilisieren und zu informieren. In Abhängigkeit des jeweiligen Themas wende ich mich dabei an unterschiedliche Zielgruppen.

Informationsoffensive für besseren Schutz der eigenen Daten

Meine Daten.
Meine Freiheit.

Um für mehr Achtsamkeit im Umgang mit personenbezogenen Daten zu werben, habe ich die Initiative „Meine Daten. Meine Freiheit." gestartet. Die Kampagne richtet sich sowohl an Betroffene als auch an datenverarbeitende Stellen aus Wirtschaft, Verwaltung und Gesellschaft. Im Mittelpunkt stehen die Sensibilisierung und Schutzmaßnahmen bei der Verarbeitung persönlicher Informationen.

Hintergrund ist, dass mir in meiner Aufsichtstätigkeit immer wieder Fälle begegnen, in denen zu unbedacht Daten preisgegeben oder verwendet wurden. Dazu gehören beispielsweise die leichtfertige Weitergabe von Bankdaten, das oftmals unzulässige Anfertigen von Ausweiskopien oder der offene E-Mail-Verteiler, bei dem die Adressen für alle Empfängerinnen und Empfänger einsehbar sind. Solche und ähnliche Verstöße registrierte ich auch 2025. Wie die Zahlen belegen (vgl. 6.2.2) verzeichnete ich einen enormen Anstieg bei Beschwerden und Kontrollanregungen. Dies wiederum verdeutlicht, wie wichtig den Bürgerinnen und Bürgern die Achtung ihrer Grund- und Persönlichkeitsrechte ist. Deshalb kommt dem Datenschutz auch eine besondere Bedeutung zu. Er schützt zum Beispiel die Meinungsfreiheit und das Recht am eigenen Bild. Dessen sollte man sich im Umgang mit den

Mehr zu „Meine Daten. Meine Freiheit." und zu den Textgeneratoren erfahren:
↗ datenschutz.sachsen.de/freiheit

eigenen, aber auch mit den Daten Dritter, stets bewusst sein und entsprechend verantwortungsvoll handeln.
Darauf mache ich mit „Meine Daten. Meine Freiheit." aufmerksam.

Neuer Onlineservice hilft bei Ausübung der Betroffenenrechte

Um Bürgerinnen und Bürgern die Kommunikation mit der datenverarbeitenden Stelle zu erleichtern, habe ich im Rahmen meiner Initiative Textgeneratoren entwickelt.
Mit diesen Onlineanwendungen zu den wichtigsten Betroffenenrechten lassen sich unkompliziert passende Schreiben an den datenschutzrechtlich Verantwortlichen erstellen. Dazu genügt es, einige Daten zur eigenen Person, zum Adressaten sowie zum Anliegen in ein Webformular einzutragen. Anschließend erzeugt der Dienst eine PDF- und eine Textdatei. Diese können heruntergeladen und zum Beispiel per E-Mail an ein Unternehmen oder eine Behörde weitergeleitet werden.

Neue Formate: Newsletter und Webinare

Mit der Initiative „Meine Daten. Meine Freiheit." habe ich mein Informations- und Beratungsangebot weiter ausgebaut. Erstmals erschien 2025 der Newsletter „Datenschutz und Transparenz in Sachsen", mit dem ich mich an die oben genannten Zielgruppen wende. Außerdem habe ich eine Live-Webinar-Reihe zu nachgefragten Datenschutzthemen gestartet (siehe 6.5.3). Darüber hinaus sollen künftig auch andere Videoformate genutzt werden, insbesondere Tutorials, um zielgruppengerecht und praxisnah für Datenschutz zu sensibilisieren.

Anmeldung zum Newsletter „Datenschutz und Transparenz in Sachsen":
↗ sdb.de/newsletter

Pflege und Weiterentwicklung bestehender Kommunikationsmittel

Unter social.sachsen.de betreibe ich eine eigene Instanz des datenschutzfreundlichen Kurznachrichtendiensts Mastodon. Diese stelle ich auch anderen öffentlichen Stellen aus dem Freistaat Sachsen zur Verfügung, einige machen davon bereits Gebrauch. Dem Profil meiner Behörde social.sachsen.de/@sdtb folgen mittlerweile rund 1.500 andere Accounts.

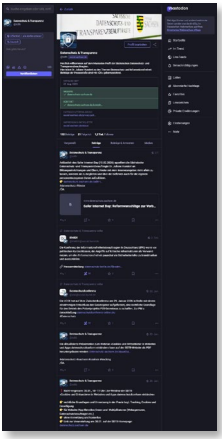


Abbildung 11:
Mastodon-Profil der SDTB

Mastodon bietet zudem die Möglichkeit, den „News-Feed" eines (Behörden-)Profils beispielsweise auf der jeweiligen (Behörden-)Website einzubinden, was wiederum die Reichweite des Profils erhöht (siehe datenschutz.sachsen.de). Zudem werden Bürgerinnen und Bürger auch ohne Mastodon-Account über die neusten Posts informiert, wenn sie den RSS-Feed des jeweiligen Kanals abonniert haben, zum Beispiel https://social.sachsen.de/@sdtb.rss für mein Profil.

Aktuelle Meldungen publiziere ich ebenso auf meiner Website. Gegenüber den Vorjahren habe ich 2025 auch hier mein Angebot ausgeweitet. Das lässt sich auch an der gestiegenen Anzahl der Nachrichten im News-Bereich ablesen. Weiterhin stelle ich auf meinem Internetauftritt nun auch Informationen zum Datenschutz für Kinder zur Verfügung. Dafür habe ich eine Themenseite eingerichtet, mit der ich insbesondere Eltern sowie pädagogische Fachkräfte dabei unterstützen möchte, Kindern den richtigen Umgang mit ihren Daten zu vermitteln. Auf der Seite finden sich nach Themen sortiert, Links zu Webinaren, Podcasts, Leitfäden, Unterrichtsmaterialien, Spielen und vielem mehr. In diesem Zusammenhang habe ich auch häufige Fragen zum Datenschutz in der Schule beantwortet, beispielsweise, was Eltern und Angehörige beim Fotografieren und Filmen auf Schulveranstaltungen beachten sollten und ob Lehrkräfte ihr privates Endgerät für Aufzeichnungen nutzen dürfen.

Themenseite „Datenschutz für Kinder":
↗ sdb.de/tb2507

Themenseite „Datenschutz in der Schule":
↗ sdb.de/tb2508

6.5.2 Presse- und Medienarbeit

Die Themen, mit denen sich Journalistinnen und Journalisten mit ihren Fragen an mich wendeten, waren im Berichtsjahr bunt gemischt. Aufgeschlüsselt nach Bereichen, entfielen die meisten Anfragen auf die Arbeit der Polizei. Insbesondere die Novelle des Sächsischen Polizeivollzugsdienstgesetzes (siehe 8.5), Datenabfragen und die Nutzung von Überwachungssoftware waren von Interesse. Weiterhin kontaktierten mich Medienschaffende verstärkt zu Fällen, bei denen Videoüberwachung bzw. Bild- und Tonaufnahmen eine Rolle

spielten, beispielsweise in Stadtratssitzungen, bei Schulveranstaltungen oder zum Kameraeinsatz durch Unternehmen oder Privatpersonen. Angesichts der hohen medialen Präsenz rund um die Entwicklungen bei der Künstlichen Intelligenz ist es sicherlich keine Überraschung, dass mich auch etliche Anfragen dazu erreichten, speziell im Bildungsbereich oder im Hinblick auf einzelne Anbieter und deren Anwendungen. Nicht immer ging es bei den Anfragen um kurze datenschutzrechtliche Einschätzungen. So nahm ich beispielsweise auch an einer zweistündigen Radiodiskussion zur Chatkontrolle teil. Eher im kleineren Umfang betrafen Presseanfragen den Bereich der Transparenz bzw. Informationsfreiheit.

Neben der Beantwortung der oftmals tagesaktuellen Themen veröffentlichte ich 13 Pressemitteilungen, darunter zum Fotografieren und Filmen in der Schule, dem KI-Training von LinkedIn und dem steigenden Aufkommen von Eingaben zur Videoüberwachung.

Was ist zu tun?
Pressemitteilungen meiner Behörde können über den Medienservice des Freistaates Sachsen kostenfrei abonniert werden: www.medienservice.sachsen.de

6.5.3 Fortbildungen, Infoveranstaltungen und fachlicher Austausch

Im Jahr 2025 konnten die Weiterbildungs- und Schulungsangebote durch meine Behörde für andere datenverarbeitende Stellen und sonstige Interessierte weiter verbessert werden. Meine Bediensteten waren beispielsweise regelmäßig mit verschiedenen Datenschutzthemen an Fortbildungseinrichtungen der öffentlichen Verwaltung tätig, am häufigsten am Fortbildungszentrum des Freistaates Sachsen in Meißen und am Landesamt für Schule und Bildung. Aber auch ein spezifisches In-House-Seminar im Bereich Datenschutz wurde in einem Landratsamt angeboten.

Des Weiteren biete ich seit Herbst 2025 im Rahmen meiner Initiative „Meine Daten. Meine Freiheit." (siehe 6.5.1) Onlineseminare zu nachgefragten Datenschutzthemen an. Zu Beginn der neuen Reihe widmete ich mich der Prävention und den Meldepflichten bei Datenpannen. Ende November 2025 konnten sich Bürgerinnen und Bürger über die private Videoüberwachung im Wohnumfeld informieren: Wann

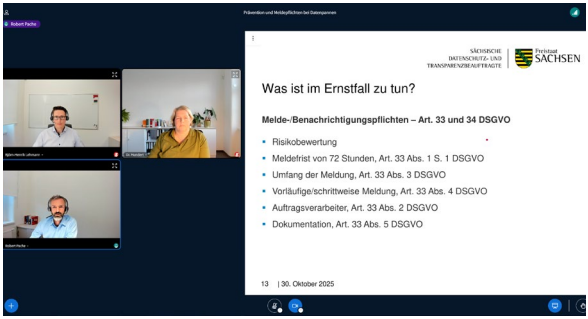
und wie ist der Kameraeinsatz überhaupt zulässig? Worauf ist besonders zu achten? Und wann schreite ich als Aufsichts- und Ordnungswidrigkeitenbehörde ein? Die Links zu den Onlineseminaren wurden am Veranstaltungstag auf www.datenschutz.sachsen.de veröffentlicht. Dort und über meinen Newsletter finden Interessierte auch weitere Details, die Präsentationen sowie Termine und Themen für 2026.

Wichtige Datenschutzthemen griff auch der 1. Mitteldeutsche Datenschutztag auf, der am 4. März 2025 in Magdeburg stattfand. Zum Teilnehmerkreis gehörten vor allem behördliche und externe Datenschutzbeauftragte, aber auch an Datenschutz Interessierte. Bei der Organisation kooperierte ich mit dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit, der Landesbeauftragten für den Datenschutz Sachsen-Anhalt und dem Berufsverband der Datenschutzbeauftragten Deutschlands e. V. (BvD). Das Besondere an dem Format ist, dass die Teilnehmenden die Gelegenheit haben, sich nicht nur untereinander auszutauschen, sondern ihre Fragen direkt mit den Fachleuten aus den Aufsichtsbehörden besprechen können. In den Vorträgen widmeten wir uns beispielsweise der „Digitalisierung von Verwaltungsprozessen: Datenschutz frühzeitig mitdenken", „Nutzung von KI (LLM) in der Verwaltung" oder dem „AI Act: Auch ein Datenschutzthema".

Fazit: Der Datenschutztag stieß auf reges Interesse und war für die Beteiligten ein wertvoller Beitrag zur fachlichen Weiterbildung, zum gegenseitigen Verständnis und zum Erfahrungsaustausch.

Gelegenheit zum Dialog mit meiner Behörde bot ebenso der „Tag der offenen Tür des Sächsischen Landtags", an dem sich Bürgerinnen und Bürger mit ihren Fragen direkt vor Ort an mich wenden konnten. Diese Veranstaltung hatte der Landtag – wie seit vielen Jahren Tradition – wieder auf den 3. Oktober gelegt. An meinem Stand informierten wir sowohl über den rechtskonformen Umgang mit personenbezogenen Daten als auch über die Möglichkeiten, wie man mithilfe des Transparenzgesetzes amtliche Informationen

Abbildung 12:
rechts: Die Organisatoren des 1. Mitteldeutschen Datenschutztags, Tag der offenen Tür im Sächsischen Landtag,
unten: Webinar zu Prävention und Meldepflichten bei Datenpannen, Workshop für Bürgerpolizistinnen und -polizisten zur Videoüberwachung



erhalten kann. Beides war im Berichtszeitraum auch Thema beim E-Learning-Kurs „Wer sieht mich?", der unter anderem von der Sächsischen Landeszentrale für politische Bildung organisiert wurde. Die Veranstaltung unterstützte ich wie in den Vorjahren mit einem Vortrag.

Von Gesetzes wegen bin ich (beratendes) Mitglied im IT-Kooperationsrat, im Landespräventionsrat und im statistischen Beirat. Auch diese Sitzungen nutzte ich für den fachlichen Austausch.

7 Zusammenarbeit der Datenschutzaufsichtsbehörden, Datenschutzkonferenz

Protokolle der DSK-Tagungen:
↗ sdb.de/tb2212

Im Jahr 2025 veröffentlichten der Europäische Datenschutzausschuss (EDSA) und die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) eine Vielzahl an Leitlinien, Positionierungen, Entschließungen und Orientierungshilfen, um den Schutz personenbezogener Daten sicherzustellen – insbesondere zu neuen Technologien, wissenschaftlicher Forschung sowie zum Zusammenspiel der Datenschutz-Grundverordnung mit anderen Digital-Rechtsakten. Sowohl die Arbeit des EDSA als auch die der DSK trägt wesentlich dazu bei, dass Verantwortliche die bestehenden und neuen Regelungen besser umsetzen können und somit das Grundrecht auf Datenschutz gewahrt bleibt.

Abbildung 13:
110. Konferenz der DSK vom 10. bis 12. Dezember 2025 in Berlin

7.1 Materialien der Datenschutzkonferenz – Entschließungen

Entschließungen sind öffentliche Stellungnahmen der DSK zu datenschutzpolitischen Fragen, beispielsweise zur Einführung eines neuen Gesetzes.

- DSGVO-Reform: Rechtssicherheit und Innovation gehen Hand in Hand – Anpassungen für KI erforderlich (12.12.2025)
- DSGVO-Reform: IT-Hersteller in die Verantwortung nehmen! (12.12.2025)
- Verbesserung des Datenschutzes von Kindern in der Datenschutz-Grundverordnung (20.11.2025)
- Automatisierte Datenanalyse durch Polizeibehörden verfassungskonform gestalten! (17.09.2025)
- Ohne Sicherheit keine Freiheit – Ohne Freiheit keine Sicherheit (16.06.2025)
- Confidential Cloud Computing (16.06.2025)
- Eckpunkte für eine freiheitliche und grundrechtsorientierte digitale Zukunft (26.03.2025)

7.2 Materialien der Datenschutzkonferenz – Beschlüsse

Beschlüsse sind Positionen, die die Auslegung datenschutzrechtlicher Regelungen beziehungsweise entsprechende Empfehlungen betreffen.

- Standardisierter Prüfprozess zu datenschutzrechtlichen Anforderungen bei EfA-Onlinediensten nach Onlinezugangsgesetz (OZG) (Dezember 2025)
- Positionspapier: Datenschutz bei der Terminverwaltung durch Heilberufspraxen (16.06.2025)
- Meldung von Mieter:innendaten an Grundversorger (28.05.2025)

7.3 Materialien der Datenschutzkonferenz – Orientierungshilfen

Orientierungshilfen und Standardisierungen sind fachliche Anwendungshilfen für Verantwortliche, Auftragsverarbeiter, Herstellerinnen und Hersteller und die Öffentlichkeit.

- Orientierungshilfe zu ausgewählten Fragestellungen des neuen Onlinezugangsgesetzes (OZG) (Anwendungshilfe für Stellen, die länderübergreifende Onlinedienste nach OZG betreiben oder nutzen) (Dezember 2025)
- Orientierungshilfe zur Zusammenarbeit mehrerer Aufsichtsbehörden im Rahmen von § 5 Gesundheitsdatennutzungsgesetz – GDNG (Dezember 2025)
- Datenschutzrechtliche Besonderheiten generativer KI-Systeme mit RAG-Methode (Oktober 2025)
- Anwendungshinweise zu den Anforderungen an Datenübermittlungen an Drittländer im Rahmen der wissenschaftlichen Forschung zu medizinischen Zwecken (September 2025)
- Empfehlungen für Informationspflichten bei Datenübermittlungen an Drittländer im Rahmen der wissenschaftlichen Forschung zu medizinischen Zwecken (Anlage zu Orientierungshilfe zu Anwendungshinweisen) (September 2025)
- Orientierungshilfe zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und beim Betrieb von KI-Systemen (Juni 2025)

7.4 Materialien der Datenschutzkonferenz – Anwendungshinweise

Anwendungshinweise sollen beim praktischen Vollzug der Datenschutz-Grundverordnung unterstützen.

- Anforderungen an datenschutzrechtliche Zertifizierungsprogramme (17.11.2025)

7.5 Materialien der Datenschutzkonferenz – Stellungnahmen

Stellungnahmen sind Positionen, die unter anderem in gerichtlichen Verfahren oder Gesetzgebungsverfahren abgegeben werden.

- Stellungnahme der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) zum Entwurf des zweiten Staatsvertrags zur Änderung des Staatsvertrags zur Neuregulierung des Glücksspielwesens in Deutschland (2. Änderungsglücksspielstaatsvertrag 2021) (21.10.2025)
- Stellungnahme der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zum Entwurf eines Gesetzes zur Durchführung der Verordnung über künstliche Intelligenz (KI-VO) (10.10.2025)
- Stellungnahme der unabhängigen Datenschutzaufsichtsbehörden der Länder zum Entwurf eines Gesetzes zur Durchführung der Verordnung (EU) 2023/2854 (Data Act-Durchführungsgesetz – DA-DG) (13.03.2025)

7.6 Materialien der Datenschutzkonferenz – Sonstiges

- Merkblatt zu Verständigungen in datenschutzrechtlichen Verfahren über Geldbußen (Dezember 2025)
- Musterrichtlinien für das Verfahren über Geldbußen der Datenschutzaufsichtsbehörden (MRiDaVG) (16.06.2025)

7.7 Dokumente des Europäischen Datenschutzausschusses: Leitlinien, Empfehlungen, bewährte Verfahren

Der Europäische Datenschutzausschuss (EDSA) verabschiedete die nachstehend aufgeführten Dokumente.

- Leitlinien 02/2024 zu Artikel 48 DSGVO (04.06.2025)
- Empfehlungen 1/2025 zum Welt-Anti-Doping-Kodex 2027 der WADA (11.02.2025)

7.8 Leitung einer Arbeitsgruppe zum Datenschutz beim Mobilfunkstandard 6G

Joint Communication and Sensing (JCAS) beschreibt die grundlegende Idee, bestehende Funk-Kommunikation (elektromagnetische Wellen) so anzupassen, dass sie gleichzeitig als Funk-Sensorik (Radarfunktionalität) genutzt werden kann. Das heißt die Möglichkeit, Kommunikation und Sensing (Radar) in einem System und Frequenzspektrum zu betreiben. Entsprechend wird potenziell jedes Gerät, welches Funk-Kommunikation betreiben kann, auch in der Lage sein, als Radarsensor zu fungieren, was einen weitaus flächendeckenderen Einsatz zur Folge haben kann.
JCAS kann dabei in Verbindung mit unterschiedlichen Arten von Kommunikationssystemen bzw. -technologien verwendet werden. So soll zum einen das WLAN-Sensing mit der Entwicklung des IEEE 802.11bf Standards etabliert werden. Zum anderen soll mit der Entwicklung des neuen Mobilfunkstandards der 6. Generation (6G), welcher voraussichtlich um das Jahr 2030 eingeführt wird, JCAS auch im Mobilfunk etabliert werden.

Diese sensorischen Fähigkeiten, integriert als Basisdienst in zukünftigen Mobilfunknetzen, bieten eine Menge potenzieller Anwendungsbereiche. Andererseits ermöglicht JCAS aber auch eine übergreifende und weitreichende Überwachung des öffentlichen wie auch des privaten Raumes und erzeugt damit regulative Herausforderungen im Hinblick auf den Schutz personenbeziehbarer Daten.
Meiner Behörde wurde deshalb 2025, in Zusammenarbeit mit weiteren Aufsichtsbehörden, die Leitung einer Unterarbeitsgruppe 6G des Arbeitskreises Technik übertragen, welche sich mit den datenschutzrechtlichen Herausforderungen von JCAS auseinandersetzen und entsprechende Handlungsempfehlungen erarbeiten soll. Der Schwerpunkt richtet sich dabei auf die Bewertung möglicher Rechtsgrundlagen bzw. die Untersuchung möglicher Anwendungsszenarien hinsichtlich ihrer Vereinbarkeit mit datenschutzrechtlichen Vorgaben. Die Arbeitsgruppe versucht dabei in enger Zusammenarbeit mit der Forschung zu agieren.

7.9 Niederlassung oder Hauptsitz? Falsche Angabe der sächsischen Aufsichtsbehörde als mutmaßlich federführende Aufsichtsbehörde im IMI

↗ Art. 4 Nr. 16 a, 56 DSGVO

Selten genug wird Sachsen im europäischen Internal Market Information System (IMI) als mutmaßlich federführende Aufsichtsbehörde für einen grenzüberschreitenden Fall angegeben, weil nicht alle europäischen Aufsichtsbehörden sich im Detail mit den Zuständigkeiten der 18 deutschen Aufsichtsbehörden befassen wollen. Die spanische Aufsichtsbehörde bezeichnete aber exakt mich, weil die Beschwerde sich gegen ein in Dresden ansässiges Unternehmen richtete, welches die Daten des Beschwerdeführers an Dritte weitergegeben hatte.

Eine nähere Beschäftigung mit der Website und der Datenschutzerklärung des Verantwortlichen zeigte, dass das Unternehmen vor zehn Jahren von einem größeren Unternehmen aufgekauft worden war, welches seinen Hauptsitz in einem anderen deutschen Bundesland hatte.

Gemäß Art. 16 Nr. 4 a DSGVO ist die Hauptverwaltung in der Union die Hauptniederlassung gemäß Art. 56 Abs. 1 DSGVO, und die Aufsichtsbehörde, in deren Zuständigkeitsbereich diese fällt, ist für die Fallbearbeitung federführend zuständig, es sei denn, die Entscheidungen hinsichtlich der Zwecke und Mittel der Verarbeitung personenbezogener Daten werden in einer anderen Niederlassung des Verantwortlichen in der Union getroffen, und diese Niederlassung ist befugt, diese Entscheidungen umsetzen zu lassen.

Im IMI trug ich also ein, dass eine andere Aufsichtsbehörde die federführende Aufsichtsbehörde sei, weil die Hauptverwaltung des Verantwortlichen in einem nicht näher bezeichneten anderen Bundesland läge, und meldete mich wegen der sächsischen Niederlassung „nur" als betroffene Aufsichtsbehörde gemäß Art. 4 Nr. 22a DSGVO. Am selben Tag setzte ich mich mit dem zuständigen Sachbearbeiter der Aufsichtsbehörde des anderen Bundeslandes telefonisch und per Mail in Verbindung und fragte nach seiner Einschätzung, da sich bis dahin noch keine andere Aufsichtsbehörde im IMI als federführend gemeldet hatte.

Eine Woche später kommentierte die spanische Aufsichtsbehörde im IMI meine Eintragung, dass zumindest aus der Datenschutzerklärung des Verantwortlichen sich seine Hauptniederlassung in Dresden ergäbe, und ich meine Behauptung mit Unterlagen belegen sollte.

Die andere deutsche Aufsichtsbehörde hatte schon angekündigt, die Federführung übernehmen zu wollen, da sie nach Rücksprache mit dem dortigen Datenschutzbeauftragten des Verantwortlichen wusste, dass Entscheidungen über die Verarbeitungen in der dortigen Hauptverwaltung erfolgten. Um ihr nicht vorzugreifen, äußerte ich mich zu der spanischen Anfrage im IMI nicht mehr. Nach einigen Tagen meldete sich diese andere Aufsichtsbehörde als federführende Aufsichts-

behörde in dem oben genannten Verfahren und übernahm damit den Fall.
Diese glückliche Lösung wäre ohne die regelmäßige Zusammenarbeit der mit IMI befassten Mitarbeitenden im Arbeitskreis Organisation und Struktur der DSK und die IMI-Schulungen in der Kürze der Zeit nicht möglich gewesen.

7.10 Mitarbeit in nationalen und europäischen Arbeitsgruppen zur statistischen Erfassung der Ausstattung und der Tätigkeiten der Aufsichtsbehörden

Wie bereits in meinem Tätigkeitsbericht Datenschutz 2024 dargestellt, setze ich mich für die statistische Erfassung der Tätigkeiten der deutschen und europäischen Aufsichtsbehörden durch Mitarbeit in europäischen und nationalen Arbeitsgruppen ein. Im europäischen Kontext sind einheitliche Definitionen der geforderten statistischen Angaben eine Voraussetzung für vergleichbare Zahlen. Deshalb wurde ein „Drafting Team" von einer Expertengruppe des Europäischen Datenschutzausschusses (EDSA) eingerichtet, an welcher auch eine Vertreterin meiner Behörde teilnahm. Anfang November 2024 wurde das von diesem Team erarbeitete Papier mit Vorschlägen für statistische Erhebungen vom EDSA einstimmig angenommen (vgl. Tätigkeitsbericht Datenschutz 2024, 7.9, Seite 176 f.).

Tätigkeitsbericht Datenschutz 2024:
↗ sdb.de/tb2024

Daraufhin wurde 2025 ein freiwilliges Pilotprojekt zur statistischen Erhebung durchgeführt, an dem ich teilnahm. Die Antworten der 5 beteiligten Aufsichtsbehörden wurden von der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) zu einer deutschen Gesamtantwort zusammengefasst. Nach Auswertung des Piloten stimmte in der 107. Plenumssitzung der EDSA am 09.07.2025 dem nach dem Pilotprojekt überarbeiteten Fragebogen und Begriffsdefinitionen zu.

Danach werden die Zahlen jährlich abgefragt und vom EDSA zu einem Bericht verarbeitet. Die Zahlen für 2024 und 2025 sollen Anfang 2026 abgefragt werden. Die einzelnen Aufsichtsbehörden sollen ihre statistischen Erfassungsverfahren zügig darauf einstellen. Allerdings wird in den kommenden Jahren auch der neuen Verfahrensverordnung für die DSGVO Rechnung zu tragen sein, die 15 Monate nach ihrer Veröffentlichung anwendbar sein wird (siehe: sdb.de/tb2509).
Zurzeit ist eine Unterarbeitsgruppe der DSK damit beschäftigt, den Fragebogen zum besseren Verständnis der deutschen Aufsichtsbehörden zu kommentieren.

8 Richtlinienbereich – Richtlinie (EU) 2016/680 – und sonstige Bereiche

8.1 Speicherungen des Landesamts für Verfassungsschutz nach dem Tag X im Jahr 2023 in Leipzig

↗ § 2 Abs. 1 SächsVSG, § 3 Abs. 1 SächsVSG, § 5 Abs. 1 SächsVSG

Noch im Jahr 2024 erhielt ich Kenntnis von einem Beschluss des Oberverwaltungsgerichts Bautzen vom 12. September 2024 – 5 B 94/24 –, mit dem das Landesamt für Verfassungsschutz Sachsen (LfV) verpflichtet wurde, der Plattform „Frag-den-Staat" Auskunft über verfassungsschutzbehördliche Speicherungen von Personen zu geben, die am sogenannten Tag X am 3./4. Juni 2023 in Leipzig von einer polizeilichen Einschließung betroffen und gegen die strafprozessuale Ermittlungsverfahren eingeleitet worden waren (zu polizeilichen Maßnahmen in diesem Zusammenhang siehe auch 8.2 und Tätigkeitsbericht Datenschutz 2023, 1.7, Seite 41 ff.).

Tätigkeitsbericht Datenschutz 2023:
↗ sdb.de/tb2023

Veröffentlichungen von „Frag-den-Staat" zufolge waren Daten aller über 1.300 von der polizeilichen Umschließung betroffenen Personen in Leipzig an das LfV übermittelt worden. Die erlaubte Demonstration vom 3. Juni 2023 – behördliche Schätzungen gingen von circa 500 gewaltsuchenden und gewaltbereiten Teilnehmerinnen und Teilnehmern an der Versammlung aus – hatte zu ihrem Ende hin einen gewalttätigen Verlauf genommen, wobei die Angriffe auf Polizeibedienstete von einer relativ kleinen Personengruppe aus der Menge heraus erfolgten. Die Versammlung wurde gegen 18.00 Uhr

beendet, wenig später begann die polizeiliche Umschließung. Polizeiliche, ausdrücklich an (ehemalige) Versammlungsteilnehmer/innen gerichtete Aufforderungen, die Örtlichkeit zu verlassen, ergingen per Lautsprecherdurchsagen erst, fünf Minuten bevor die Umschließung gegen 18.30 Uhr vollzogen war. Hinsichtlich aller über 1.300 Betroffener stand der Verdacht der Begehung eines Landfriedensbruchs im besonders schweren Fall im Raum, die Identität aller umschlossenen Personen wurde polizeilich festgestellt.

Auf Nachfrage nach den tatsächlichen und rechtlichen Umständen von Speicherungen durch das LfV teilte mir dieses mit, dass es zu 1.323 Betroffenen personenbezogene Daten vom Landeskriminalamt Sachsen übermittelt bekommen habe. Die Daten seien nach § 6 des Sächsischen Verfassungsschutzgesetzes (SächsVSG, alte Fassung; Anmerkung: am 16. August 2025 trat die aktuelle Fassung des SächsVSG in Kraft) daraufhin überprüft worden, ob sie für die Aufgabenerfüllung des LfV erforderlich waren. Im Ergebnis seien durch das LfV Daten von 590 Personen aus dem betroffenen Personenkreis im Nachrichtendienstlichen Informationssystem des Bundesamtes und der Landesbehörden für Verfassungsschutz (NADIS) gespeichert worden, die ihren Wohnsitz im Freistaat Sachsen hatten. Daten der Betroffenen, die ihren gewöhnlichen Aufenthalt nicht in Sachsen hatten, hat das LfV an die jeweils zuständige Verfassungsschutzbehörde weitergeleitet. Die Datenspeicherungen stützte das LfV auf § 6 Abs. 1 SächsVSG a. F., wonach das LfV zur Erfüllung seiner Aufgaben personenbezogene Daten speichern durfte, wenn tatsächliche Anhaltspunkte für Bestrebungen oder Tätigkeiten nach § 2 Abs. 1 SächsVSG a. F. vorlagen oder dies für die Erforschung und Bewertung von Bestrebungen oder Tätigkeiten nach § 2 Abs. 1 SächsVSG a. F. erforderlich war. Gemäß § 2 Abs. 1 Satz 1 SächsVSG a. F. sei die Sammlung und Auswertung von Informationen, insbesondere von sach- und personenbezogenen Auskünften, Nachrichten und Unterlagen über Bestrebungen, die gegen die freiheitliche demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes oder eines Landes gerichtet sind, Aufgabe des LfV ge-

wesen. Nach der Definition in § 3 Abs. 1 Nr. 3 SächsVSG a. F. waren Bestrebungen gegen die freiheitliche demokratische Grundordnung politisch bestimmte, ziel- und zweckgerichtete Verhaltensweisen in einem oder für einen Personenzusammenschluss, der darauf gerichtet ist, einen der in § 3 Abs. 2 SächsVSG a. F. genannten Verfassungsgrundsätze zu beseitigen oder außer Geltung zu setzen. Nach § 3 Abs. 1 Satz 2 SächsVSG a. F. handelte für einen Personenzusammenschluss, wer ihn in seinen Bestrebungen aktiv sowie ziel- und zweckgerichtet unterstützte.

Diese Voraussetzungen lagen nach Auffassung des LfV bei sämtlichen 590 Personen vor, die von der polizeilichen Umschließung am 3./4. Juni 2023 in Leipzig betroffen waren und ihren gewöhnlichen Aufenthalt in Sachsen hatten. Das LfV setzte die Speicherfrist zunächst auf fünf Jahre fest.

Daraufhin entspann sich eine längere schriftliche Diskussion zwischen meiner Behörde und dem LfV über die rechtlichen Voraussetzungen einer Speicherung personenbezogener Daten im NADIS und die Bewertung der tatsächlichen Umstände am 3./4. Juni 2023 in Leipzig. Dabei äußerte ich starke Bedenken gegen die Einschätzung des LfV. Einigkeit bestand darüber, dass auch Mitglieder einer durch das LfV beobachteten extremistischen Bestrebung an der Versammlung teilgenommen hatten und es zu teils massiven Gewalttätigkeiten gekommen war. Allerdings hatte und habe ich starke Zweifel daran, dass ein Verbleiben im örtlichen Bereich einer legalen Versammlung als aktive sowie ziel- und zweckgerichtete Unterstützung der an den Gewalttätigkeiten beteiligten extremistischen Bestrebung gewertet werden kann. Die Rechtsprechung verlangt im Hinblick auf das Merkmal einer „aktiven sowie ziel- und zweckgerichteten Unterstützung" einer verfassungsfeindlichen Bestrebung durchweg Unterstützungshandlungen „von bedeutendem Gewicht" (BVerwG, Urteil vom 14.12.2020 – 6 C 11.18 -, juris Rn. 31; VGH Baden-Württemberg, Urteil vom 31. Mai 2023 – 1 S 3351/21 –, Rn. 34, juris; VG Berlin, Beschluss vom 29. Oktober 2019 – 1 L 247.19 –, Rn. 33, juris; OVG Nordrhein-Westfalen, Urteil vom 7. August 2018 –

5 A 1698/15 –, Rn. 94 – 101, juris; VG München, Beschluss vom 27. November 2019 – M 30 E 19.1368 –, Rn. 35, juris). Auch ein gemeinsames Skandieren von Parolen durch über eintausend Personen, die gemeinsam von einer polizeilichen Umschließung betroffen sind, ist meines Erachtens schwerlich als Unterstützungshandlung von bedeutendem Gewicht für eine extremistische Bestrebung zu klassifizieren, an der Mitglieder an der Versammlung teilgenommen hatten. Selbst wenn man eine objektive Unterstützungshandlung annehmen wollte, fanden meines Erachtens vor der Entscheidung über eine fünfjährige Speicherung im NADIS maßgebliche Aspekte der Verhältnismäßigkeit, deren Beachtung für das LfV gemäß § 4 Abs. 4 SächsVSG a. F. gesetzlich verpflichtend war, kaum ausreichende Berücksichtigung. Für die Prüfung der Angemessenheit der Beobachtung einer Einzelperson wegen aktiver sowie ziel- und zweckgerichteter Unterstützung eines verfassungswidrigen Personenzusammenschlusses kommt es ebenso wie bei der Prüfung der Angemessenheit der Beobachtung einer Einzelperson wegen nachdrücklicher Unterstützung eines verfassungswidrigen Personenzusammenschlusses nämlich auf eine Abwägung aller berührten Interessen und Umstände an. In deren Rahmen ist eine Gesamtbeurteilung des Gewichts des Eingriffs, des Grades der von der Einzelperson ausgehenden Gefährdung der freiheitlichen demokratischen Grundordnung, der sich wesentlich danach bestimmt, ob die Einzelperson selbst verfassungsfeindliche Ziele verfolgte, sowie des Gewichts der durch ihre Beobachtung zu erwartenden Informationen für den Schutz der freiheitlichen demokratischen Grundordnung vorzunehmen (vgl. BVerwG, Urteil vom 14.12.2020 – 6 C 11.18 – juris Rn. 57; VGH Baden-Württemberg, Urteil vom 31. Mai 2023 – 1 S 3351/21 –, Rn. 92, juris). Ich konnte nicht erkennen, dass die Speicherung von fast 600 Personen, zu denen zum allergrößten Teil keinerlei weitere verfassungsschutzbehördlichen Erkenntnisse vorlagen, auch nur ansatzweise einen Gewinn an zusätzlichen relevanten Erkenntnissen für die Ermittlung eines umfassenden Bildes über die an der Versammlung beteiligte extremistische Bestrebung versprach.

Die Schwere des Eingriffs in das (Grund-)Recht auf informationelle Selbstbestimmung durch eine NADIS-Speicherung ist erheblich und erklärt sich im Wesentlichen aus der Sichtbarkeit der Speicherung für alle am NADIS teilnehmenden Verfassungsschutzbehörden (Länder und Bund) sowie der Einbeziehung von NADIS-Speicherungen in (gesetzlich vorgesehene) Sicherheits- und Zuverlässigkeitsüberprüfungen. Bei Letzteren liegt nahe, dass angesichts der Speichervoraussetzung einer Unterstützungshandlung von bedeutendem Gewicht für eine verfassungsfeindliche Bestrebung schon die Speicherung als solche zu negativen Auswirkungen für die betroffene Person führt. Besonderen Wert legte ich auf den Aspekt der Verhältnismäßigkeit daher bei NADIS-Speicherungen zu Versammlungsteilnehmern, zu denen die Speicherung wegen der Teilnahme an der Versammlung am 3. Juni 2023 in Leipzig die einzige verfassungsschutzbehördliche Erkenntnis war („Erstspeicherungen").

Im Ergebnis der Diskussion verkürzte das LfV die Speicherfrist auf zwei Jahre und nahm auch sukzessiv erfolgende Einstellungen der Strafverfahren nach § 170 Abs. 2 Strafprozessordnung (StPO) zum Anlass, ab Juni 2025 Speicherungen zu Personen, zu denen keine weiteren Erkenntnisse vorlagen, aus NADIS zu löschen. Weil damit ein wesentliches Ziel meiner Bemühungen – die Beendigung von Speicherungen im NADIS zu Personen, zu denen abgesehen von der Teilnahme an der Versammlung am 3. Juni 2023 in Leipzig keinerlei weiteren verfassungsschutzbehördlichen Erkenntnisse vorlagen – erreicht war, habe ich, auch mit Blick auf meine beschränkten Reaktionsmöglichkeiten auf festgestellte Datenschutzverstöße (vgl. § 18 Abs. 3 SächsVSG a. F.), auf eine weitere Klärung der Frage, ob die ursprünglichen „Erstspeicherungen" im NADIS rechtmäßig waren, verzichtet. Auf die aus meiner Sicht zwingenden Voraussetzungen für eine rechtmäßige Speicherung im NADIS, die ich oben genannt habe und die kumulativ vorliegen müssen, habe ich das LfV ausdrücklich aufmerksam gemacht. In einer gegen Ende des Berichtszeitraums anberaumten gemeinsamen Besprechung zur Praxis bei „Erstspeicherungen" im Allgemeinen gewann

Was ist zu tun?
Personenbezogene Speicherungen im NADIS sind erhebliche Grundrechtseingriffe mit potenziell gravierenden Auswirkungen für die Betroffenen. Bei festgestellten Unterstützungshandlungen für verfassungsfeindliche Bestrebungen setzen sie eine Handlung von bedeutendem Gewicht voraus. Weiter sind unter anderem die Motivation der Betroffenen und die Relevanz der einzelnen personenbezogenen Speicherung für die Beobachtung der Bestrebung zu berücksichtigen.

ich den Eindruck, dass das LfV die Relevanz von Daten Betroffener für seine Aufgabenerfüllung grundsätzlich sorgfältig prüft und dabei auch die Belange betroffener Personen nicht unberücksichtigt lässt.

8.2 Datenverarbeitung des Landeskriminalamts im Zusammenhang mit dem Tag X im Jahr 2023 in Leipzig

↗ §§ 21, 27 SächsVSG

Nachdem ich bereits im Herbst 2024 Kenntnis von einem Beschluss des Oberverwaltungsgerichts Bautzen vom 12. September 2024 – 5 B 94/24 – erhalten hatte, mit dem das Landesamt für Verfassungsschutz Sachsen (LfV) verpflichtet worden war, der Plattform „Frag-den-Staat" Auskunft über verfassungsschutzbehördliche Speicherungen von Personen zu geben, die am sogenannten Tag X am 3./4. Juni 2023 in Leipzig nach einer Versammlung von einer polizeilichen Einschließung betroffen und gegen die strafprozessuale Ermittlungsverfahren eingeleitet worden waren (vgl. hierzu 8.1 und Tätigkeitsbericht Datenschutz 2023, 1.7, Seite 41 ff.) und ich auf Nachfrage bei der zuständigen Staatsanwaltschaft erfahren hatte, dass entsprechende Datenübermittlungen durch das Landeskriminalamt Sachsen (LKA) ohne Kenntnis der Staatsanwaltschaft vorgenommen worden waren, wandte ich mich an das LKA. Von datenschutzrechtlichem Interesse waren zunächst die Frage der Rechtsgrundlage der Übermittlungen und der Umstand, dass das LKA die sachleitende Staatsanwaltschaft über seine Entscheidung zur Übermittlung zahlreicher personenbezogener Daten an das LfV nicht informiert hatte.

Tätigkeitsbericht Datenschutz 2023:
↗ sdb.de/tb2023

Das LKA teilte mit, dass die Übermittlung von 1.323 Datensätzen an das LfV auf der Grundlage von § 10 Abs. 2 Sächsisches Verfassungsschutzgesetz (SächsVSG) a. F. (Anmerkung: am 16. August 2025 trat die aktuelle Fassung des SächsVSG

in Kraft) erfolgt sei. Alle Personen, die zum Zwecke der Identitätsfeststellung am 3./4. Juni in Leipzig polizeilich umschlossen worden waren, hätten in dem eingeleiteten Ermittlungsverfahren Beschuldigtenstatus wegen des Verdachts des besonders schweren Falls des Landfriedensbruchs gemäß § 125a Strafgesetzbuch (StGB) aufgewiesen. Nach § 10 Abs. 2 SächsVSG a. F. übermittelten Polizeidienststellen auch alle anderen ihnen bekannt gewordenen personenbezogenen Daten und sonstigen Informationen über Bestrebungen oder Tätigkeiten nach § 2 Abs. 1 SächsVSG a. F., wenn tatsächliche Anhaltspunkte dafür bestünden, dass die Übermittlung für die Erfüllung der Aufgaben des LfV erforderlich sei.

Nachdem das Unterbleiben der Einbeziehung der sachleitenden Staatsanwaltschaft zunächst nicht begründet wurde – tatsächlich stellte § 10 Abs. 2 SächsVSG a. F. Übermittlungen der Polizei an das LfV in strafprozessualen Ermittlungsverfahren unter den Vorbehalt der Sachleitungsbefugnis der Staatsanwaltschaft –, verwies das LKA auf Nachfrage auf einen Erlass des Sächsischen Staatsministeriums des Innern (SMI) aus dem Jahr 2016. Danach hatten das SMI und das Sächsische Staatsministerium der Justiz vereinbart, dass die Polizei bei Informationsübermittlungen an den Verfassungsschutz von einem generellen Einverständnis der zuständigen Staatsanwaltschaft ausgehen darf. Dies soll ausweislich des Erlasses nicht bei herausragenden Einzelfällen von besonderer Bedeutung gelten, in denen, wie auch in Zweifelsfällen, vor der Übermittlung von über den Lagebericht hinausgehenden Informationen unverzüglich eine Entscheidung der zuständigen Staatsanwaltschaft herbeizuführen ist.

Auch wenn das Unterlassen einer Information an die für das Ermittlungsverfahren zuständige Staatsanwaltschaft vor der Übermittlung von Personendatensätzen und Tatvorwürfen mit Blick auf den erwähnten Erlass des SMI (noch) vertretbar erscheint, wäre es künftig wünschenswert, wenn in medienwirksamen Verfahren mit einer vierstelligen Zahl an Beschuldigten das LKA vor einer Mitteilung der Daten sämtlicher Beschuldigter „en bloc" an das LfV die Abstimmung mit der zuständigen Staatsanwaltschaft suchen würde. Erlasse der Exekutive sind

nicht geeignet, (bundes-)gesetzliche Zuständigkeitsbestimmungen zu umgehen. In strafprozessualen Ermittlungsverfahren entscheidet nach der Strafprozessordnung nicht die Polizei, sondern die Staatsanwaltschaft als zuständige und sachleitende Verfolgungsbehörde über Datenübermittlungen an Dritte, darunter auch an andere Behörden. Vor diesem Hintergrund ist eine zurückhaltende Anwendung des Erlasses geboten. Die Abstimmung mit der Staatsanwaltschaft förderte zudem die Einhaltung gesetzlicher Schutzvorkehrungen, wie zum Beispiel die Prüfung von Übermittlungsverboten nach § 13 SächsVSG a. F (jetzt: § 27 SächsVSG), und verringerte das Risiko unverhältnismäßiger Eingriffe in das Recht betroffener Personen auf informationelle Selbstbestimmung.

Anfang August wandte ich mich erneut an das LKA, weil ich zwischenzeitlich von der zuständigen Staatsanwaltschaft darüber informiert worden war, dass zum Stand Mitte Mai insgesamt 857 Ermittlungsverfahren gemäß § 170 Abs. 2 StPO eingestellt worden seien und in 20 Verfahren Anklage erhoben worden sei. Ich bat das LKA um Bestätigung, dass nach Erhalt der Einstellungsbenachrichtigungen der Staatsanwaltschaft die Information über die jeweilige Einstellung des Verfahrens nach § 170 Abs. 2 StPO unverzüglich an das LfV übermittelt wird. Darüber hinaus bat ich um Auskunft zu polizeilichen Speicherungen zu den von der Umschließung betroffenen Personen insbesondere in den Fällen, in denen zu der betroffenen Person keine weiteren polizeilichen Erkenntnisse oder Speicherungen vorlagen. Dabei bat ich um Berücksichtigung der jüngeren verfassungsgerichtlichen Rechtsprechung sowie der novellierten Richtlinien des SMI zur vorsorgenden Speicherung.

Das LKA bestätigte mir leider erst im Dezember, über vier Monate nach meiner Anfrage, dass nach Erhalt der Informationen zu jeweiligen Einstellungen des Verfahrens durch die Staatsanwaltschaft das LfV unverzüglich über die jeweilige Verfahrenseinstellung informiert werde. Bis Ende November seien zu über 1.100 Beschuldigten Mitteilungen über die Einstellung des Verfahrens nach § 170 Abs. 2 StPO eingegangen, die in der Folge dem LfV mitgeteilt worden seien.

Zu polizeilichen Speicherungen über Beschuldigte aus der Umschließung vom 3./4. Juni 2023 teilte das LKA mit, dass zunächst Speicherungen zum Zwecke der Strafverfolgung vorgenommen und diese nach Abschluss der jeweiligen Ermittlungsverfahren zum Zwecke der vorsorgenden Speicherung im Polizeilichen Auskunftssystem Sachsen (PASS) fortgeführt worden seien. Zusätzlich seien in einigen Fällen Speicherungen in Verbunddateien des Bundeskriminalamtes (BKA) vorgenommen worden. Das LKA wies darauf hin, dass mit der Einführung der Richtlinie des SMI zur vorsorgenden Speicherung am 15. Juni 2025 eingestellte Verfahren gegen „Ersttäter" (zu denen keine weiteren polizeilichen Erkenntnisse im Zusammenhang mit Ermittlungsverfahren vorliegen) nicht länger vorsorgend gespeichert würden. Vor Einführung der Richtlinie gespeicherte Verfahren seien mittlerweile im PASS bereinigt worden. Die Bereinigung der Daten, die das LKA in Verbunddateien des BKA gespeichert habe, sei noch nicht abgeschlossen.

Datenschutzrechtlich ist das Vorgehen des LKA bei Speicherungen, die aus Datenerhebungen im Zusammenhang mit der Umschließung der aufgelösten Versammlung am 3./4. Juni 2023 und den eingeleiteten Ermittlungsverfahren stammen, nicht zu beanstanden. Zu begrüßen ist insbesondere die retrograde Bereinigung der Speicherungen, die noch nach den Vorgaben der mittlerweile außer Kraft getretenen KpS-Richtlinie angelegt worden waren. Das Unterbleiben einer vorsorgenden Speicherung bei „Ersttäterinnen bzw. Ersttätern" nach Einstellung des Verfahrens bzw. das Löschen einer unter altem „untergesetzlichem Recht" angelegten Speicherung setzt die verfassungsrechtlichen Vorgaben für die vorsorgende Speicherung und die Anforderungen an eine notwendige Negativprognose – nun in der aktuellen Richtlinie des SMI zur vorsorgenden Speicherung – in begrüßenswerter Weise in die Praxis um.

Was ist zu beachten?

In strafprozessualen Ermittlungsverfahren, die etwa im Hinblick auf Ermittlungsmaßnahmen oder ihren Umfang Besonderheiten aufweisen, hat die Polizei vor der Übermittlung personenbezogener Daten an das LfV die verfahrensleitende Staatsanwaltschaft zu beteiligen. Bei vorsorgenden polizeilichen Speicherungen sind im Hinblick auf deren Verhältnismäßigkeit Verfahrenseinstellungen zu berücksichtigen.

8.3 Schutz von Angaben zu Geschädigten von Straftaten

↗ § 68 StPO

Im Berichtszeitraum erreichten mich Beschwerden von Geschädigten, die in strafprozessualen Ermittlungsverfahren durch die Polizei befragt worden waren. Die jeweiligen Ermittlungsverfahren betrafen Straftaten gegen die sexuelle Selbstbestimmung. Anlass für die Beschwerden gab jeweils der aus Sicht der Petenten unbefriedigende Umgang der Polizei mit ihren Anliegen, ihre aktuellen Wohnanschriften nicht in die Ermittlungsakte aufzunehmen, um deren Kenntnisnahme durch den jeweiligen Beschuldigten zu verhindern. In den betreffenden Vorgängen waren die aktuellen Adressen der Betroffenen allerdings schon im Zusammenhang mit anderen Ermittlungsmaßnahmen zeitlich bereits vor den Vernehmungen der Petenten in die jeweilige Ermittlungsakte gelangt, sodass dem mit den in beziehungsweise nach den Vernehmungen gegenüber der Polizei geäußerten Anliegen nicht mehr Rechnung getragen werden konnte.

Die Beschwerden geben Anlass, auf die rechtlichen Möglichkeiten und Voraussetzungen des Schutzes personenbezogener Daten von Geschädigten und/oder Zeugen im Strafverfahren hinzuweisen.

Aus rechtsstaatlichen Gründen ist es grundsätzlich zwingend notwendig, dass Beschuldigte hinsichtlich des ihnen gemachten Vorwurfs nicht mit intransparenten oder „geheimen" Beweismitteln konfrontiert werden, die eine gesetzmäßige Verteidigung erschweren oder gar vereiteln würden. Unter anderem für die Beurteilung der Glaubwürdigkeit von Zeugen ist daher nach ständiger Rechtsprechung von Bedeutung, dass diese konkret benannt werden; die Personalien dürfen deshalb grundsätzlich vor dem Angeklagten und seinem Verteidiger nicht geheim gehalten werden. Weil es aber Konstellationen gibt, in denen der Schutz von Zeuginnen bzw. Zeugen oder Geschädigten ein solches Gewicht erlangt, dass vom Grundsatz der Transparenz abgewichen werden muss, sieht das Gesetz in § 68 Abs. 2 bis 5 Strafprozess-

ordnung (StPO) Schutzvorkehrungen zugunsten gefährdeter Zeuginnen bzw. Zeugen vor. Voraussetzung für das Absehen von der Angabe der Wohnanschrift nach § 68 Abs. 2 StPO ist das Vorliegen einer erheblichen Gefährdung; bloße Belästigungen reichen hingegen nicht aus (KK-StPO/Slawik, 9. Aufl. 2023, StPO § 68 Rn. 7, beck-online). Anlass zur Besorgnis einer Gefährdung kann aufgrund allgemeiner Erkenntnisse oder Erfahrungen bestehen, ohne dass schon konkrete Anhaltspunkte dafür im Einzelfall hervorgetreten sind; eine Gefährdung der Zeugin bzw. des Zeugen ist in der Regel jedenfalls dann anzunehmen, wenn er schon vor der Vernehmung Ziel eines Anschlages oder einer entsprechenden Bedrohung war (vgl. BT-Drs. 16/12908, Seite 13).

Im Gesetz selbst ist eine „Unterstützungsregelung" verankert, die die Strafverfolgungsbehörden adressiert: „Liegen Anhaltspunkte dafür vor, dass die Voraussetzungen der Absätze 2 oder 3 vorliegen, ist der Zeuge auf die dort vorgesehenen Befugnisse hinzuweisen", § 68 Abs. 4 Satz 1 StPO. Liegen für das mit der Sache befasste Strafverfolgungsorgan oder das Gericht die Voraussetzungen des § 68 Abs. 2 S. 1 StPO ersichtlich vor, begründet die Vorschrift die Verpflichtung, die Zeugin bzw. den Zeugen darauf hinzuweisen, anstelle seiner vollständigen Anschrift eine andere ladungsfähige Anschrift angeben zu können oder – im Falle des § 68 Abs. 3 Satz 1 – Angaben zur Person verweigern oder nur Angaben über eine frühere Identität machen zu dürfen (KK-StPO/Slawik, 9. Aufl. 2023, StPO § 68 Rn. 10, beck-online). Die Vorschriften des § 68 Absätze 2 bis 4 StPO gelten auch nach Abschluss der Zeugenvernehmung, § 68 Abs. 5 Satz 1 StPO. Wenn eine erhebliche Gefährdung von Rechtsgütern der Zeugin bzw. des Zeugen anzunehmen ist, ist die Möglichkeit der Beschränkung der Verarbeitung von Personalien in jeder Lage des Verfahrens eröffnet. Die Entscheidung kann von Amts wegen ergehen, aber auch auf Antrag eines Prozessbeteiligten oder der Zeugin bzw. des Zeugen selbst (BeckOK StPO/Monka, 55. Ed. 1.4.2025, StPO § 68 Rn. 5, beck-online).

Grundsätzlich ist der Sächsischen Polizei die Problematik bewusst. In einer Broschüre zum Polizeilichen Opferschutz

(sdb.de/tb2510) erscheint folgender Hinweis: „Erläutern Sie der Polizei, die über den Adressdatenschutz entscheiden darf, Ihre Gründe oder Ihre Besorgnis. Die Polizei unterstützt Sie dann bei der Benennung einer sinnvollen ladungsfähigen Anschrift."

Die Beschwerden geben allerdings Anlass zur Besorgnis, dass entsprechenden Anliegen von Betroffenen nicht durchweg mit der gebotenen Sensibilität begegnet wird. Unabhängig davon, ob im Einzelfall die (relativ hohen) Anforderungen an eine hinreichende Gefährdung von Zeuginnen bzw. Zeugen oder Geschädigten erfüllt sind, sollten – wenn nicht schon, wie gesetzlich vorgesehen, initiativ, § 68 Abs. 4 Satz 1 StPO – von betroffenen Personen vorgebrachte Wünsche unverzüglich geprüft und die Möglichkeiten des Schutzes persönlicher Angaben erörtert werden. Dies gilt insbesondere in Ermittlungsverfahren zu Straftaten, die den Kern der Persönlichkeit von Geschädigten besonders berühren und gravierende Auswirkung auf deren Lebensführung haben können.

Was ist zu tun?
Liegen Anhaltspunkte für Gefährdungen von Zeuginnen bzw. Zeugen oder Geschädigten vor, hat bereits die Polizei im Rahmen der Vernehmung aktiv auf die Möglichkeiten zum Schutz der Wohnanschrift hinzuweisen. Entsprechende Anträge betroffener Personen sind unverzüglich zu bearbeiten.

8.4 Akteneinsichtsrecht von Gefangenen

↗ §§ 54, 55, 56, 58 SächsJVollzDSG

Im Berichtszeitraum wandte sich ein Gefangener einer sächsischen Justizvollzugsanstalt (JVA) an mich und teilte mit, er habe Akteneinsicht in all seine Person betreffenden Akten, die in der JVA geführt werden, beantragt. Er habe dies mit seinem berechtigten Interesse im Hinblick auf eine geplante gerichtliche Entscheidung begründet und zudem darauf hingewiesen, dass eine Auskunft gemäß § 54 Sächsisches Justizvollzugsdatenschutzgesetz (SächsJVollzDSG) für die Wahrnehmung seiner rechtlichen Interessen nicht ausreichend sei. Durch den Stationsdienst sei ihm mündlich mitgeteilt worden, dass sein Antrag auf Akteneinsicht mit der Begründung abgelehnt wurde, weil er zu pauschal und somit unzulässig sei. Der Petent verfüge über Kopien der Dokumente in den Akten und müsse angeben, welche konkreten

Dokumente er einsehen wolle. Der Gefangene bat mich um eine datenschutzrechtliche Prüfung.

Die um Stellungnahme gebetene JVA erläuterte, der Gefangene erhalte auf Antrag die Akteneinsicht gemäß § 55 Sächs JVollzDSG nur, soweit eine Auskunft für die Wahrnehmung seiner rechtlichen Interessen nicht ausreiche. Die JVA habe daher abzuwägen, ob eine Akteneinsicht gewährt werden müsse oder eine Auskunft ausreiche. Praktischer Hintergrund sei, dass die Verwaltung einer JVA die Akteneinsicht an mehrere hundert Gefangene, die dies beantragen würden, personell und organisatorisch nicht gewähren könnte, wenn eine Abwägung, ob eine Auskunft ausreiche, durch die JVA nicht erfolgen dürfte oder der Gefangene ein Akteneinsichtsgesuch nicht wenigstens entsprechend begründen müsste.

§ 55 SächsJVollzDSG regelt, dass betroffene Personen, denen Auskunft nach § 54 SächsJVollzDSG zu gewähren ist, auf Antrag Akteneinsicht erhalten, soweit eine Auskunft für die Wahrnehmung ihrer rechtlichen Interessen nicht ausreicht, sie hierfür auf die Einsichtnahme angewiesen sind und überwiegende berechtigte Interessen Dritter nicht entgegenstehen. Insoweit entspricht § 55 SächsJVollzDSG weitgehend wortgleich zum bundesgesetzlichen § 185 Strafvollzugsgesetz (StVollzG). Die herrschende Rechtsprechung zu § 185 StVollzG a. F. legte strenge Anforderungen an ein Akteneinsichtsrecht an, da schon das Recht auf Auskunft gemäß § 185 StVollzG a. F., § 19 Abs. 1 Sätze 2 und 3 Bundesdatenschutzgesetz a. F. nicht schrankenlos gewährt wurde. Die geänderte, aktuelle Rechtslage sieht allerdings ein schrankenloses (von Ausnahmen wie Rechtsmissbrauch abgesehen) Auskunftsrecht vor. Dem hat auch der seit einigen Jahren zuständige Landesgesetzgeber mit der Regelung des § 54 SächsJVollzDSG Rechnung getragen. Meiner Ansicht nach sollte sich dies auch in der Ermessensausübung der JVA, ob dem betroffenen Gefangenen auf Antrag Akteneinsicht gewährt wird, niederschlagen, um einer nicht gerechtfertigten Ungleichbehandlung von Auskunft gemäß § 54 und Akteneinsicht gemäß § 55 entgegenzuwirken. Als Mindestanfor-

derung für eine Akteneinsicht sehe jedoch auch ich, dass der Gefangene in seinem Antrag zumindest hinsichtlich des Vorliegens eines rechtlichen Interesses konkrete Angaben machen muss. Insoweit war die tatsächliche Antragstellung des Petenten, die mir die JVA vorlegte, entgegen der Behauptung des Petenten unzureichend. Aus datenschutzrechtlicher Sicht dürfte das Ermessen der JVA auf null reduziert sein, wenn der antragstellende Gefangene sein rechtliches Interesse an der Akteneinsicht nachvollziehbar darlegt. Weitergehender Begründungen bedarf es dann nicht. Auch in Fällen, in denen sich aus einer einfachen Auskunft nicht ergibt, welche personenbezogenen Unterlagen sich in der Akte befinden, wird die Einsicht in die Akte zur Wahrnehmung rechtlicher Interessen in der Regel erforderlich sein und durch die JVA gewährt werden müssen.

Vom Akteneinsichtsrecht gemäß § 55 SächsJVollzDSG ist das Recht auf Einsicht in Gesundheits- und Therapieakten gemäß § 56 SächsJVollzDSG zu unterscheiden. Letzteres ist – abgesehen von Aktenbestandteilen mit einem Sperrvermerk nach § 56 Satz 4 in Verbindung mit § 55 Abs. 1 Satz 2 SächsJVollzDSG – gesetzlich unbeschränkt, das heißt, es ist nicht an weitere Voraussetzungen als die Antragstellung geknüpft. Der Petent und Antragsteller hatte vorliegend Akteneinsicht in alle seine Person betreffenden Akten, die in der JVA geführt werden, beantragt. Die JVA teilte bezüglich der Einsicht in die Gesundheits- und Therapieakten mit, dass dieses Ersuchen bei den hierfür verantwortlichen Stellen wie Medizinischem Dienst und Fachdiensten geltend zu machen sei, die die entsprechenden Akten verwahren. Das ist nicht rechtmäßig. Der Einsichtsanspruch erfasst sämtliche vollzugliche Akten und Dateien, ganz gleich, ob diese vom allgemeinen Vollzugsdienst oder bei besonderen Fachdiensten geführt werden. Verantwortliche Stelle ist nicht der jeweilige Fachdienst, sondern die Justizvollzugsanstalt. Der Verweis auf eine andere speichernde Stelle innerhalb der JVA genügt nicht. Antragstellende Gefangene sind nicht an besondere Stellen zu verweisen, vielmehr obliegt es der JVA, Anträge intern an die konkreten Fachdienste weiterzuleiten.

Was ist zu tun?
Ein nicht näher spezifizierter Einsichtsanspruch einer oder eines Gefangenen erfasst sämtliche vollzugliche Akten und Dateien der JVA, unabhängig, ob diese vom allgemeinen Vollzugsdienst oder bei besonderen Fachdiensten geführt werden. Verantwortliche Stelle ist nicht der jeweilige Fachdienst, sondern die JVA. Der Verweis auf eine andere interne speichernde Stelle genügt nicht.

Letztlich habe ich die JVA auf § 58 Abs. 2 SächsJVollzDSG hingewiesen, wonach die Justizvollzugsbehörden die betroffenen Personen unverzüglich schriftlich darüber informieren müssen, wie mit ihrem Antrag verfahren wurde. Eine mündliche Eröffnung durch den Stationsdienst genügt nicht den gesetzlichen Anforderungen.
Das Sächsische Staatsministerium der Justiz habe ich informatorisch an dem Vorgang beteiligt.

8.5 Novellierung des Sächsischen Polizeivollzugsdienstgesetzes

↗ SächsPVDG

Nachdem mich das Sächsische Staatsministerium des Innern (SMI) dankenswerterweise frühzeitig über Pläne zur Überarbeitung des Sächsischen Polizeivollzugsdienstgesetzes (SächsPVDG) informiert hatte, gab es im Berichtszeitraum einen kontinuierlichen Austausch auf der Arbeitsebene unserer Häuser.
Konkreter Handlungsbedarf für eine Anpassung des Polizeigesetzes entstand bereits mit dem Urteil des Sächsischen Verfassungsgerichtshofs vom 25. Januar 2024 – Vf. 91-II-19 – zu einzelnen Bestimmungen des Sächsischen Polizeivollzugsdienstgesetzes (SächsPVDG). Das Verfassungsgericht hatte bestimmte Vorschriften für unvereinbar mit der Sächsischen Verfassung erklärt. Die Fortgeltung der betreffenden Vorschriften unter bestimmten Maßgaben wurde bis zum 30. Juni 2026 befristet. Parallel dazu liefen, auch aufgrund von Entscheidungen des Bundesverfassungsgerichts, in anderen Bundesländern Gesetzgebungsvorhaben bezüglich des jeweiligen Landespolizeirechts, in denen teils kontrovers diskutierte Befugnisse Eingang in Gesetze gefunden haben.
Anfang Oktober legte das SMI den Entwurf eines Gesetzes zur Änderung polizeirechtlicher Vorschriften vor, dessen wichtigster Teil Änderungen des SächsPVDG enthält. Der Entwurf wurde zeitweise auf dem Beteiligungsportal Sach-

sen veröffentlicht. Ich habe gegenüber dem SMI eine umfassende datenschutzrechtliche Stellungnahme zum Gesetzentwurf abgegeben.

Der Gesetzentwurf enthält begrüßenswerte Änderungen, insbesondere in Umsetzung der oben erwähnten verfassungsgerichtlichen Rechtsprechung. Dies betrifft etwa die Präzisierung des Begriffs der Vorfeldstraftat und die Bestimmung der Voraussetzungen für eine vorsorgliche Speicherung personenbezogener Daten für künftige Verfahren. Zu begrüßen sind auch die Schaffung von Rechtsgrundlagen für Maßnahmen, die bislang rechtsstaatlich bedenklich auf die polizeilichrechtliche Generalklausel zur Verarbeitung personenbezogener Daten gestützt wurden, zum Beispiel für die Speicherung von personengebundenen oder ermittlungsunterstützenden Hinweisen zu einer bestimmten Person. Ausdrücklich zu begrüßen ist auch die Streichung der Befugnis zur Ausschreibung von sogenannten Kontakt- und Begleitpersonen aus Gründen der Verhältnismäßigkeit.

Andererseits finden sich im Gesetzentwurf Bestimmungen zu Befugnissen, die eine enorme Eingriffstiefe aufweisen, ohne zugleich wirksame eingriffsmindernde Vorkehrungen zu treffen – beispielhaft seien die automatisierte Datenanalyse, die Nutzung personenbezogener Daten für das Trainieren und Testen selbstlernender KI-Systeme oder die Videoüberwachung des fließenden Straßenverkehrs mit Bildaufzeichnung des Fahrzeugführers zur Verhütung einer Ordnungswidrigkeit genannt. Vorgesehen ist auch, ohne Begründung der Erforderlichkeit, die Speicherfrist für Aufzeichnungen der Videoüberwachung des öffentlichen Raums und damit den Umfang der verarbeiteten personenbezogenen Daten zu verdoppeln. Sehr kritisch sehe ich eine Regelung, nach der Dritten (privaten Unternehmen) erlaubt werden kann, polizeilich gespeicherte personenbezogene Daten zur Weiterentwicklung ihrer Produkte zu nutzen (selbstlernende KI-Systeme).

In diesen Fällen muss ebenso wie bei geplanten Befugnissen, die die Einbeziehung von umfangreichen polizeifremden und nahezu unbegrenzten, auch privaten Datenbeständen vorsehen (automatisierte Datenanalyse und Bildabgleiche mit

dem Internet), besonders kritisch hinterfragt werden, ob entsprechende polizeiliche Maßnahmen geeignet und erforderlich wären, den angestrebten Zweck zu erreichen, und in ihrer Beeinträchtigung der Grundrechte der betroffenen Personen die gebotene Verhältnismäßigkeit wahrten. Aus datenschutzrechtlicher Sicht bestehen bezüglich einiger (neuer) Befugnisse erhebliche Zweifel daran, dass Sicherheit – im Sinne eines handlungsfähigen, Gefahren abwehrenden Staates – und Freiheit – im Sinne einer Ausübung von Grundrechten frei von staatlicher Einwirkung – in einem verfassungsrechtlich gebotenen ausgewogenen Verhältnis stehen.

In Anbetracht des Umstands, dass der Gesetzentwurf noch nicht dem Sächsischen Landtag zugeleitet wurde, sehe ich hier von einer detaillierten Betrachtung einzelner Entwurfsvorschriften ab.

Was ist zu tun?

Im Rahmen der Novellierung des Sächsischen Polizeivollzugsdienstgesetzes ist die Schaffung von Befugnissen vorgesehen, die zum Teil massiv in Grundrechte Betroffener eingreifen. Der Gesetzgeber muss bei der Abwägung widerstreitender Belange von Verfassungsrang besonders sorgfältig vorgehen.

8.6 Neue Richtlinie der Polizei zur vorsorgenden Speicherung

↗ SächsPVDG

Das Sächsische Staatsministerium des Innern (SMI) kam Anfang 2025 auf mich zu und informierte mich über die beabsichtigte Novellierung der „Richtlinien des Sächsischen Staatsministeriums des Innern für die Führung Kriminalpolizeilicher personenbezogener Sammlungen in den Polizeidienststellen des Freistaates Sachsen" (KpS-Richtlinie), die zuletzt im Jahr 2021 aktualisiert worden war. Bedarf für eine grundlegende Überarbeitung hatte sich vor allem aus dem Urteil des Sächsischen Verfassungsgerichtshofs vom 25. Januar 2024 – Vf. 91-II-19 – zu einzelnen Bestimmungen des Sächsischen Polizeivollzugsdienstgesetzes (SächsPVDG) sowie aus dem Urteil des Bundesverfassungsgerichts vom 1. Oktober 2024 – 1 BvR 1160/19 – zu bestimmten Normen des Gesetzes über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (BKAG). Beide Verfassungsgerichte urteilten unter anderem über die jeweiligen Vorschriften, auf deren Grundlage perso-

nenbezogene Daten aus polizeilichen Vorgängen vorsorgend für Zwecke der künftigen Gefahrenabwehr und zur künftigen Strafverfolgung gespeichert wurden bzw. werden. Die für die sächsische Polizei unmittelbar geltende Vorschrift des § 80 Abs. 2 SächsPVDG wurde für nicht mit der Sächsischen Verfassung vereinbar erklärt. Der Verfassungsgerichtshof gab dem Gesetzgeber eine Frist zur Neuregelung bis zum 30. Juni 2026. Die Entscheidung des Bundesverfassungsgerichts zum BKAG betraf die Sächsische Polizei zwar nicht unmittelbar, gleichwohl erlangten Vorgaben zur Verfassungskonformität von vorsorgenden Speicherungen und deren Vereinbarkeit mit dem Grundgesetz zumindest mittelbar Relevanz auch für die Polizei im Freistaat.

Das Bestreben des SMI, untergesetzliche Regelungen zur vorsorgenden Speicherung unabhängig von einem notwendigen Gesetzgebungsverfahren und im Vorgriff auf ein solches an die klar formulierten verfassungsgerichtlichen Vorgaben anzupassen, konnte ich nur ausdrücklich begrüßen. Der Austausch mit dem SMI gestaltete sich ausgesprochen kollegial und überaus konstruktiv. Besonders hervorheben möchte ich die Bereitschaft des SMI und der Polizei, die Vorgaben der Gerichte nicht (nur) als Einschränkungen polizeilicher Handlungsmöglichkeiten zu betrachten und bei der Erarbeitung der neuen Richtlinie polizeipraktische Bedürfnisse und Notwendigkeiten einerseits und Grundrechtsbeeinträchtigungen und praktische Auswirkungen für betroffene Personen andererseits in einen angemessenen Ausgleich zu bringen.

Die im Ergebnis durch das SMI erstellte „Richtlinie des Sächsischen Staatsministeriums des Innern über die Anforderungen an die vorsorgende Speicherung von personenbezogenen Daten in polizeilichen Dateisystemen (Richtlinie vorsorgende Speicherung)" regelt, unter welchen Voraussetzungen im Zusammenhang mit Strafermittlungs- oder Gefahrenabwehrvorgängen rechtmäßig erhobene oder erlangte personenbezogene Daten über den konkreten Anlassfall hinaus vorsorgend zu Zwecken der künftigen Abwehr von Gefahren und/oder zur Verhütung oder Verfolgung künftiger Straftaten in polizeilichen Dateisystemen gespeichert werden dürfen. Sie trifft da-

rüber hinaus Festlegungen über die Fristen, nach deren Ablauf die Zulässigkeit der weiteren vorsorgenden Speicherung personenbezogener Daten zu prüfen ist, über die Voraussetzungen der Löschung oder Vernichtung vorsorgend gespeicherter Daten und zu Dokumentationsanforderungen, die im Zusammenhang mit der Entscheidung zur vorsorgenden Speicherung und über Speicherfristen bestehen.

Von zentraler Bedeutung für die vorsorgende Speicherung personenbezogener Daten, die zum allergrößten Teil aus strafprozessualen Ermittlungsverfahren stammen dürften und Tatverdächtige, Beschuldigte und verurteilte Personen betreffen, ist die sogenannte Negativprognose, also die Bewertung der Wahrscheinlichkeit, mit der die betroffene Person künftig polizeilich in Erscheinung treten wird. Als Prognosekriterien sind unter anderem die Art, Schwere und Begehungsweise der Tat, die zur ursprünglichen Erfassung der betroffenen Person in polizeilichen Dateien führte, die Persönlichkeit der betroffenen Person und das bisherige strafrechtliche Erscheinungsbild heranzuziehen. Relevant kann regelmäßig auch sein, ob die betroffene Person wiederholt und in welchem Ausmaß sie straffällig geworden ist, aber auch der Zeitraum, währenddessen sie strafrechtlich nicht mehr in Erscheinung getreten ist.

Aufgrund des Umstandes, dass Speicherungen im Polizeilichen Auskunftssystem Sachsen (PASS) praktisch sämtlichen Bediensteten des sächsischen Polizeivollzugsdienstes zugänglich sind und polizeiliche Speicherungen bei gesetzlichen Zuverlässigkeitsüberprüfungen relevant sind (vergleiche etwa § 4 des Sächsischen Gesetzes zur Regelung polizeilicher Zuverlässigkeitsüberprüfungen, § 5 des Waffengesetzes, § 34a der Gewerbeordnung), ist die Einhaltung verfassungsrechtlicher und gesetzlicher Vorgaben bei derartigen Verarbeitungen personenbezogener Daten datenschutzrechtlich von höchster Bedeutung (vgl. Tätigkeitsbericht Datenschutz 2023, 8.3, Seite 254 ff.).

Die Richtlinie Vorsorgende Speicherung ist meines Erachtens eine sehr gut geeignete Grundlage für die Vornahme rechtskonformer vorsorgender Speicherungen in der polizeilichen Praxis. Die Richtlinie trat am 15. Juni 2025 in Kraft.

Tätigkeitsbericht Datenschutz 2023:
↗ sdb.de/tb2023

Was ist zu tun?
Die polizeiliche Speicherung personenbezogener Daten für künftige Zwecke ist ein Grundrechtseingriff, der nur unter bestimmten Voraussetzungen zulässig ist. Die neue Richtlinie der Polizei zur vorsorgenden Speicherung als untergesetzliche verbindliche Vorgabe setzt die verfassungsrechtlichen Vorgaben für eine solche Datenverarbeitung um.

9 Rechtsprechung zum Datenschutz

9.1 Fehlende Information kann zur Rechtswidrigkeit der Verarbeitung führen – EuGH-Urteil vom 9. Januar 2025, C-394/23

↗ Art. 6, 13 DSGVO

Sofern sich ein Verantwortlicher auf ein berechtigtes Interesse gemäß Art. 6 Abs. 1 Satz 1 Buchst. f DSGVO als Rechtsgrund stützt, ist er verpflichtet, die betroffene Person zum Zeitpunkt der Datenerhebung über dieses Interesse zu informieren (Art. 13 Abs. 1 Buchst. d DSGVO). Unterlässt der Verantwortliche diese Information, kann die Datenverarbeitung laut dem Urteil des Europäischen Gerichtshofs (EuGH) vom 9. Januar 2025 (C-394/23) nicht auf ein berechtigtes Interesse gestützt werden.

In früheren Urteilen wurde in diesem Zusammenhang ausgeführt, dass der Verantwortliche „zudem allen anderen ihm obliegenden Pflichten aus der DSGVO nachkommen" muss, um die Datenverarbeitung auf Art. 6 Abs. 1 Buchst. f DSGVO stützen zu können. Im gegenständlichen Urteil weist der EuGH einleitend in Bezug auf alle Rechtsgrundlagen darauf hin, dass es dem Verantwortlichen gemäß Art. 13 Abs. 1 Buchst. c DSGVO obliegt, den Betroffenen über Zweck und Rechtsgrundlage der Verarbeitung zu informieren. In einem früheren Urteil hat der EuGH zudem die Informationspflicht gemäß Art. 12, 13 DSGVO mit der Wirksamkeit einer Einwilligung gemäß Art. 6 Abs. 1 Buchst. a DSGVO verknüpft.

Folge einer derartigen generellen zwingenden Verbindung von Informationspflichten (Art. 13 DSGVO) mit der Rechtmäßigkeit gemäß Art. 6 Abs. 1 DSGVO wäre, dass auch bei Fehlen einzelner Informationen in einer Datenschutzerklärung (wie etwa Kontaktdaten der/des Datenschutzbeauftragten gemäß Art. 13 Abs. 1 Buchst. b DSGVO) die Datenverarbeitung insgesamt rechtswidrig wäre.

Da Urteile des EuGH eng auf den konkreten Fall begrenzt auszulegen sind, bleibt abzuwarten, ob die ergangenen Entscheidungen so verstanden werden müssen, dass jeder DSGVO-Verstoß auf die Rechtmäßigkeit der Verarbeitung durchschlagen könnte oder vielmehr nur bestimmte Fehler bei der Information auf die Rechtmäßigkeit durchschlagen und sich dies auch lediglich, beispielsweise in der Interessenabwägung im Rahmen von Art. 6 Abs. 1 Buchst. f DSGVO, auswirkt.

Was ist zu tun?
Verantwortliche sollten überprüfen, ob sie für alle Datenerhebungen ihren gesetzlichen Informationspflichten nachkommen.

9.2 Zurechenbarkeit von Informationen Dritter zur Herstellung eines Personenbezugs – EuGH-Urteil vom 4. September 2025, C-413/23 P

↗ DSGVO, KI-VO

Anlass war ein Rechtsstreit zwischen dem Europäischen Datenschutzbeauftragten (EDSB) und dem einheitlichen Abwicklungsausschuss (SRB), an dem auch der Europäische Datenschutzausschuss (EDSA) sowie die Europäische Kommission beteiligt waren. Unter Bezugnahme auf seine bisherige Rechtsprechung hat der Europäische Gerichtshof (EuGH) im Rahmen dieses Urteils die Bedeutung des Begriffs der personenbezogenen Daten im Zusammenhang mit der Übermittlung pseudonymisierter Daten an Dritte präzisiert.

Pseudonymisierte Daten sind demnach nicht in jedem Fall und für jede Person als personenbezogene Daten zu betrachten. Die Pseudonymisierung kann – je nach den Umständen

des Falles – andere Personen als den Verantwortlichen tatsächlich daran hindern, die betroffene Person zu identifizieren, sodass diese für sie nicht oder nicht mehr identifizierbar ist. Der EuGH hat im Wesentlichen entschieden, dass für einen Verantwortlichen personenbezogene, pseudonyme Daten zugleich für einen anderen Empfänger anonym sein können. Für die Identifizierbarkeit ist maßgeblich, ob der Verantwortliche oder eine andere Person über nach allgemeinem Ermessen wahrscheinlich verwendete Mittel für die Identifizierung verfügt. Die maßgebliche Sicht für die Beurteilung der Identifizierbarkeit betroffener Personen richtet sich demnach wesentlich nach den Umständen der Datenverarbeitung im Einzelfall.

Unabhängig davon ist aber die dem Verantwortlichen obliegende Pflicht zur Information von betroffenen Personen zum Zeitpunkt der Datenerhebung bei ihnen über die Empfänger bzw. Kategorien von Empfängern zu informieren, an die ihre personenbezogenen Daten übermittelt werden sollen. Zu dieser Informationspflicht weist der Gerichtshof darauf hin, dass sie im Rechtsverhältnis zwischen der betroffenen Person und dem Verantwortlichen besteht und ihr Gegenstand daher in den mit dieser Person zusammenhängenden Informationen in der Form besteht, wie sie dem Verantwortlichen übermittelt wurden, also vor einer möglichen Übermittlung an Dritte. Folglich sei die Identifizierbarkeit der betroffenen Person in einem solchen Fall aus der Sicht des Verantwortlichen und nicht aus der Sicht des Empfängers zu beurteilen. Der Verantwortliche muss in solchen Fällen demnach in Datenschutzhinweisen den Empfänger der pseudonymisierten Daten angeben, auch wenn die Daten für den Empfänger anonym sind.

Was ist zu tun?

Alle Verträge zur Datenweitergabe müssen dahingehend geprüft werden, ob sie die Verarbeitung pseudonymisierter Daten als personenbezogene Daten korrekt abbilden.

9.3 Auch berufliche Daten sind personenbezogen – EuGH-Urteil vom 3. April 2025, C-710/23

↗ Art. 4, 15 DSGVO

Der EuGH hat mit seinem Urteil vom 03.04.2025 in der Rechtssache C-710/23 eine wichtige Klärung im Datenschutzrecht geschaffen: Auch berufliche Kontaktdaten von Vertretern juristischer Personen sind personenbezogene Daten im Sinne der DSGVO.

Dem Urteil lag ein Fall aus Tschechien zugrunde: Ein Bürger verlangte vom Gesundheitsministerium Auskunft über die Vertreter von Unternehmen, die Verträge über die Beschaffung von COVID-19-Tests unterzeichnet hatten – auch von Unternehmen aus Drittstaaten. Das Ministerium verweigerte die vollständige Auskunft unter Verweis auf den Datenschutz und schwärzte Namen, Unterschriften und Funktionsbezeichnungen der unterzeichnenden Personen.

Der EuGH stellte klar, dass der Begriff der personenbezogenen Daten weit auszulegen ist. Erfasst werden alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen – ausdrücklich auch beruflich genutzte Daten wie Name, Unterschrift und dienstliche Kontaktdaten von Vertretern juristischer Personen. Der berufliche Kontext begründet keine Ausnahme vom Datenschutz. Erwägungsgrund 14 der DSGVO schließt nur juristische Personen aus, nicht aber deren menschliche Vertreter.

Was ist zu tun?
Für jede Verarbeitung, Weitergabe oder Veröffentlichung dieser Daten ist eine klare und valide Rechtsgrundlage erforderlich.

Notizen

Herausgeberin
Sächsische Datenschutz- und Transparenzbeauftragte
Dr. Juliane Hundert
Maternistraße 17
01067 Dresden
Postanschrift: Postfach 11 01 32, 01330 Dresden
Telefon: +49 351 85471-101
Telefax: +49 351 85471-109
post@sdtb.sachsen.de
www.datenschutz.sachsen.de

Fotos
Titelbild: © KENGKAT – iStockphoto.com
Weitere Fotos: ronaldbonss.com (Seite 5, 195), G. Albrecht (Seite 217 o.), SDTB (Seite 217), Leonard Bergmann (Seite 219)

Druck
siblog – Gesellschaft für Dialogmarketing, Fulfillment & Lettershop mbH

Auflage
1.000 Exemplare

Bezug
kostenlos
Zentraler Broschürenversand der Sächsischen Staatsregierung
Hammerweg 30, 01127 Dresden
Telefon: +49 351 210-3671/-3672
publikationen@sachsen.de
www.publikationen.sachsen.de

Verteilerhinweis
Dieser Tätigkeitsbericht wird aufgrund der Verpflichtung nach Artikel 59 Datenschutz-Grundverordnung herausgegeben. Er darf weder von politischen Parteien noch von deren Kandidatinnen und Kandidaten oder deren Helferinnen und Helfern zum Zwecke der Wahlwerbung verwendet werden. Dies gilt für alle Wahlen. Missbräuchlich ist insbesondere die Verteilung auf Wahlveranstaltungen, an Informationsständen der Parteien sowie das Einlegen, Aufdrucken oder Aufkleben parteipolitischer Informationen oder Werbemittel. Untersagt ist auch die Weitergabe an Dritte zur Verwendung bei der Wahlwerbung.