Sächsischer Landtag
8. Wahlperiode

DRUCKSACHE 8/288

Unterrichtung

durch die Sächsische Datenschutz- und Transparenzbeauftragte

Tätigkeitsbericht Datenschutz
Berichtszeitraum: 1. Januar bis 31. Dezember 2023

(Dem Sächsischen Landtag vorgelegt gemäß Artikel 59 der Datenschutz-Grundverordnung.)

Eingegangen am: 25.10.2024 Ausgegeben am: 25.10.2024

Tätigkeitsbericht Datenschutz

Berichtszeitraum:
1. Januar bis 31. Dezember 2023

Meine Daten.
Meine Freiheit.

SÄCHSISCHE
DATENSCHUTZ- UND
TRANSPARENZBEAUFTRAGTE

Freistaat
SACHSEN

Tätigkeitsbericht Datenschutz 2023 der Sächsischen Datenschutz- und Transparenzbeauftragten

Berichtszeitraum:
1. Januar bis 31. Dezember 2023

Rechtsstand: 31. Dezember 2023

Liebe Leserinnen und Leser,

wohin wir auch schauen, weltweit haben es Unternehmen, Organisationen und Staaten auf unsere Daten abgesehen. Der Hunger danach scheint unstillbar. Während die einen Informationen über Menschen lediglich als wirtschaftliche Ressource betrachten, sind sie für andere ein Mittel zur Manipulation, Machtausübung und Verhaltenskontrolle. In jedem Fall aber sind unsere Daten ein wertvolles Gut. Dass darüber das Individuum ein „informationelles Selbstbestimmungsrecht" hat, das ist bereits der Kern des berühmten Volkszählungsurteils des Bundesverfassungsgerichts. Im Berichtszeitraum jährte sich dieses historische Urteil zum 40. Mal. Verglichen mit heute steckte die elektronische Datenverarbeitung damals noch „in den Kinderschuhen". Dennoch bewiesen die Richterinnen und Richter eine beeindruckende Weitsicht, als sie das Recht auf informationelle Selbstbestimmung erkannten. Denn sie bezogen es nicht nur auf offenkundig bedeutsame Informationen über den einzelnen Menschen. Im Gegenteil: Sie hoben hervor, dass jedes scheinbar belanglose personenbezogene Datum abhängig von seinem Verwendungszusammenhang wichtig werden kann. Und sie wiesen schon damals auf die besondere Gefährdung durch eine automatisierte Verarbeitung hin.

Heute ist absehbar, dass es durch die Fortschritte bei der Künstlichen Intelligenz (KI) immer weniger „unbedeutende" Daten geben wird. Was vor zehn Jahren noch nutzlos erschien und in der täglichen Datenflut unterging, kann KI heute mit anderen Informationen verknüpfen und in sinnvolle Zusammenhänge stellen. Welches Potenzial und welche Risiken KI-Anwendungen bergen, darüber kam 2023 eine breitere gesellschaftliche Debatte auf – maßgeblich angetrieben durch die Entwicklungen bei ChatGPT von OpenAI. Deutsche und europäische Aufsichtsbehörden bezweifeln, dass das Unternehmen mit seinem Dienst die datenschutzrechtlichen Anforderungen erfüllt. Deshalb wurden entsprechende Verfahren zur Überprüfung der Rechtmäßigkeit ge-

startet. Meine Behörde beteiligt sich hierbei auf nationaler und europäischer Ebene.

Entscheidend für die Prüfung solcher Produkte sind die Vorgaben aus der Datenschutz-Grundverordnung, kurz DSGVO. Auch sie verzeichnete im Berichtszeitraum ein kleines Jubiläum. Seit fünf Jahren, seit dem 25. Mai 2018, ist sie unmittelbar anwendbares und EU-weit einheitlich geltendes Recht. Die Verordnung hat den Datenschutz in der EU und den Mitgliedsstaaten gestärkt. Sie sichert zudem die verfassungsmäßige Rechts- und Wirtschaftsordnung. Anfängliche Unsicherheiten bei der Auslegung und Anwendung der DSGVO gehören mittlerweile der Vergangenheit an. Dazu haben auch die deutschen Aufsichtsbehörden beigetragen, etwa durch die Veröffentlichung von Orientierungshilfen. Ebenso hat die Rechtsprechung des Europäischen Gerichtshofs für Klarheit gesorgt. Auf einige wichtige Entscheidungen des vergangenen Jahres gehe ich in meinem Bericht ein. Gern komme ich damit auch dem Wunsch aus dem Sächsischen Landtag nach, den EU-Bezug meiner Tätigkeit deutlicher darzustellen und herauszuheben. Dies gilt auch für die Beschreibung einer grenzüberschreitenden Zusammenarbeit mit der spanischen Aufsichtsbehörde.

In Verfahren, bei denen die Datenschutz-Grundverordnung unmittelbar gilt, ist der EU-Zusammenhang offenkundig. Das betrifft eine Vielzahl an Fällen, die ich in meinen Jahresbericht aufgenommen habe, zum Beispiel die Videoüberwachung in Tanzschulen, die Verarbeitung von Personalausweiskopien durch Carsharing-Anbieter, die Dokumentation von Krankheitstagen und Urlaubsansprüchen in Unternehmen oder die Übermittlung von Kundendaten an einen Online-Shop. Hinzu kommen weitere Fälle aus dem öffentlichen Bereich. Sie betreffen unter anderem die überzogene Datenerhebung in einer Kindertageseinrichtung, die Aufzeichnung von Telefongesprächen durch eine Behörde, das Cloud-Computing in der Schule, den Einsatz von Drohnen und Kameratechnik bei Fußballspielen durch die Polizei oder die Beschlagnahmung von Mobiltelefonen nach einer polizeilichen Einkesselung.

Dabei geht es stets um das Recht auf informationelle Selbstbestimmung. In diesem Sinne prägt das Volkszählungsurteil auch nach vier Jahrzehnten Staat und Gesellschaft. Die damalige Entscheidung des Bundesverfassungsgerichts ist wahrlich ein Meilenstein in der Geschichte der Freiheitsrechte. Das Urteil wird angesichts der Herausforderungen rund um die Digitalisierung auch in den kommenden Jahren nicht an Bedeutung verlieren.

Ihre

Dr. Juliane Hundert
Sächsische Datenschutz- und Transparenzbeauftragte

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

AGB	Allgemeine Geschäftsbedingungen
AO	Abgabenordnung
ASOG Bln	Allgemeines Sicherheits- und Ordnungsgesetz (Berlin)
BauGB	Baugesetzbuch
BDSG	Bundesdatenschutzgesetz
BetrVG	Betriebsverfassungsgesetz
BGB	Bürgerliches Gesetzbuch
BKAG	Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten
BMG	Bundesmeldegesetz
BurlG	Bundesurlaubsgesetz
BZRG	Bundeszentralregistergesetz
DSGVO	Datenschutz-Grundverordnung
EntgFG	Entgeltfortzahlungsgesetz
ePD	ePrivacy-Richtlinie
EstG	Einkommensteuergesetz
FZV	Fahrzeugzulassungsverordnung
GeschoSReg	Geschäftsordnung der Sächsischen Staatsregierung
GG	Grundgesetz für die Bundesrepublik Deutschland
GVG	Gerichtsverfassungsgesetz
HandwO	Handwerksordnung
HeizkostenV	Heizkostenverordnung
IfSG	Infektionsschutzgesetz
KHEntG	Krankenhaus-Entgeltgesetz
KunstUrhG	Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie

MBO-Ä	(Muster-)Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte
OWiG	Gesetz über Ordnungswidrigkeiten
PaßG	Paßgesetz
PAuswG	Personalausweisgesetz
SächsAGBMG	Sächsisches Gesetz zur Ausführung des Bundesmeldegesetzes
SächsAGSGB	Sächsisches Gesetz zur Ausführung des Sozialgesetzbuches
SächsBeWoG	Sächsisches Betreuungs- und Wohnqualitätsgesetz
SächsBO	Sächsische Bauordnung
SächsDSG	Sächsisches Datenschutzgesetz
SächsDSDG	Sächsisches Datenschutzdurchführungsgesetz
SächsDSUG	Sächsisches Datenschutz-Umsetzungsgesetz
SächsGAVO	Sächsische Gutachterausschussverordnung
SächsGemO	Sächsische Gemeindeordnung
SächsKHG	Sächsisches Krankenhausgesetz
SächsLKrO	Sächsische Landkreisordnung
SächsMeldVO	Sächsische Meldeverordnung
SächsPersVG	Sächsisches Personalvertretungsgesetz
SächsPolG	Polizeigesetz des Freistaates Sachsen
SächsPVDG	Sächsisches Polizeivollzugsdienstgesetz
SächsSchulG	Sächsisches Schulgesetz
SächsVermKatG	Sächsisches Vermessungs- und Katastergesetz
SächsVwVG	Verwaltungsvollstreckungsgesetz für den Freistaat Sachsen
SächsSchulGesPflVO	Sächsische Schulgesundheitspflegeverordnung
SGB	Sozialgesetzbuch
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
StVG	Straßenverkehrsgesetz
TTDSG	Telekommunikation-Telemedien-Datenschutz-Gesetz
VwGO	Verwaltungsgerichtsordnung
WEG	Wohnungseigentumsgesetz
ZPO	Zivilprozessordnung

Sonstiges

a. a. O.	am angegebenen Ort
Abs.	Absatz
AEPD	Agencia Española de Protección de Datos
Art.	Artikel
Az.	Aktenzeichen
BfDI	Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
BGH	Bundesgerichtshof
BMDV	Bundesministerium für Digitales und Verkehr
BMG	Bundesministerium für Gesundheit
BT-Drs.	Bundestags-Drucksache
Buchst.	Buchstabe
BVerfG	Bundesverfassungsgericht
BVerwGE	Bundesverwaltungsgerichtsentscheidung
DKSB	Deutscher Kinderschutzbund
DSK	Konferenz der unabhängigen Datenschutzbeauftragten des Bundes und der Länder – Datenschutzkonferenz
EDSA	Europäischer Datenschutzausschuss
EU	Europäische Union
EuG	Europäisches Gericht
EuGH	Europäischer Gerichtshof
FAER	Fahreignungsregister
FIN	Fahrzeugidentifikationsnummer
GKDZ	Gemeinsames Kompetenz- und Dienstleistungszentrum der Polizeien der Länder Berlin, Brandenburg, Sachsen, Sachsen-Anhalt und Thüringen
IMI	Internal Market Information System
KBA	Kraftfahrt-Bundesamt
LDS	Landesdirektion Sachsen
LG	Landgericht
LK	Landkreis
LT-Drs.	Landtags-Drucksache
OH	Orientierungshilfe
OLG	Oberlandesgericht
OVG	Oberverwaltungsgericht
PASS	Polizeiliches Auskunftssystem Sachsen

PD	Polizeidirektion
PVA	Polizeiverwaltungsamt
Rdnr.	Randnummer
Rn.	Randnummer
SAKD	Sächsische Anstalt für kommunale Datenverarbeitung
SächsGVBl	Sächsisches Gesetz und Verordnungsblatt
SächsOVG	Sächsisches Oberverwaltungsgericht
SID	Staatsbetrieb Sächsische Informatik Dienste
SK	Sächsische Staatskanzlei
SMI	Sächsisches Staatsministerium des Innern
SMR	Sächsisches Staatsministerium für Regionalentwicklung
SMS	Sächsisches Staatsministerium für Soziales und Gesellschaftlichen Zusammenhalt
SVN	Sächsisches Verwaltungsnetz
VG	Verwaltungsgericht
VwV	Verwaltungsvorschrift
UWG	Gesetz gegen den unlauteren Wettbewerb
WEG	Wohnungseigentumsgesetz
ZEVIS	Zentrales Verkehrsinformationssystem
Ziff.	Ziffer

Sachgebietsregister

mit »*« ausschließlich öffentlicher Bereich
ohne »*« nichtöffentlicher Bereich bzw.
öffentlicher und nichtöffentlicher Bereich

Videografie und Bildverarbeitung

- Behördliche Überwachung/Verarbeitung*
- Beschäftigte, vgl. ansonsten Beschäftigtendatenschutz
- Dashcam, Drohnen — 6.4.3, 8.1
- Handel, Gewerbe — 1.3, 2.2.3, 2.2.11, 2.2.12
- Wohnbereiche — 2.1.3, 6.4.5
- Sonstiges, Allgemeines — 2.2.1, 2.2.2, 6.1.1, 6.3.1, 6.4.4

Wahlrecht*

Zertifizierung, Akkreditierungen, Prüfsiegel

Richtlinie (EU) 2016/680

Polizei*	1.7, 1.8, 6.4.1, 8.1, 8.2, 8.3, 8.4
Ordnungswidrigkeitenbehörden*	2.2.13, 2.2.24
Strafverfolgung*	1.7, 8.5

Straf- und Justizvollzug*

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

Sächsischer Landtag als Parlament

Verfassungsschutz

Weitere datenverarbeitende Stellen

1 Datenschutz im Freistaat Sachsen

1.1 Prüfung von ChatGPT

↗ DSGVO

Lange Zeit war Künstliche Intelligenz – KI – die nächste große Revolution, die „bald" kommen würde. Man konnte durch den ausbleibenden durchschlagenden Erfolg neuartiger Anwendungen wie beispielsweise verschiedener Sprachassistenten, Heimautomation oder Support-Chatbots den Eindruck gewinnen, dass KI mehr Hype als Revolution ist. Dass dieser Eindruck täuschte, ist den meisten Beobachtern nach den jüngsten Entwicklungen nun deutlich geworden. Eingeläutet durch ChatGPT 3.5, dessen Leistungsfähigkeit uns alle überrascht hat, setzt sich nun eine zunehmende Akzeptanz durch, dass KI unser Leben nachhaltig verändern wird.
Dass dabei KI ein ganz besonderes Risiko für die Menschheit darstellt, wird an anderer Stelle bereits vielfältig diskutiert. Umso wichtiger ist es, dass in der frühen Phase dieser Entwicklung die Weichen in die richtige Richtung gestellt werden. Dazu gehört auch ein klares Bekenntnis zum Datenschutz. KI-Anwendungen verarbeiten Daten, und wenn diese Daten einen Personenbezug haben, müssen die Anforderungen der DSGVO erfüllt werden. Das gilt sowohl für die Nutzung der KI-Modelle als auch deren Training.
Bei einigen Anwendungen bestehen berechtigte Zweifel, dass diese Anforderungen derzeit erfüllt werden, weshalb verschiedene europäische Datenschutzaufsichtsbehörden Verfahren aufgenommen haben, unter anderem gegen ChatGPT von OpenAI. Meine Behörde beteiligt sich bei diesen Ver-

fahren sowohl auf nationaler als auch auf europäischer Ebene. Dies soll keinesfalls als fortschrittsfeindlich verstanden werden. Im Gegenteil, das Fortschrittsversprechen von KI ist, dass sie den Menschen dienen wird, nicht umgekehrt. Dieses Ziel kann man nur durch Einhaltung starker Grundrechte und Schutzrechte erreichen.

Da sich die Geschäftspraktiken von KI-Unternehmen bisher noch nicht bewähren konnten, sind Verantwortliche nun besonders aufgefordert, diese Anwendungen vor ihrem Einsatz gründlich zu prüfen. Es empfiehlt sich der Abschluss eines Auftragsverarbeitungsvertrags (AVV), welcher klar regelt, welche Daten verarbeitet werden, von wem, auf welche Weise und zu welchem Zweck. Insbesondere muss sichergestellt sein, dass für jede Verarbeitung personenbezogener Daten eine Rechtsgrundlage (Art. 6 oder Art. 9 DSGVO) vorliegt. Im Umkehrschluss bedeutet dies allerdings auch, dass eine Verwendung dann datenschutzrechtlich unkritisch sein kann, wenn sichergestellt ist, dass keine personenbezogenen Daten verarbeitet werden.

Was ist zu tun?
Die Verarbeitung von personenbezogenen Daten durch KI-Anwendungen unterliegt den Anforderungen der DSGVO. Verantwortliche müssen vor Einsatz entsprechender Lösungen sicherstellen, dass alle relevanten Rechtsnormen erfüllt werden.

1.2 Untersagung des Facebook-Auftritts der Sächsischen Staatskanzlei

↗ § 42 Abs. 2 VwGO, Art. 5 Abs. 2 DSGVO

Im vergangenen Jahr hatte ich mich in meinem Tätigkeitsbericht (1.1, Seite 22 ff.) umfangreich zur Unzulässigkeit eines Auftritts bzw. einer sogenannten „Fanpage" bei Facebook geäußert und meinen entsprechenden Schriftverkehr mit der Sächsischen Staatskanzlei (SK) geschildert. Leider konnte ich diese nicht davon überzeugen, ihren Auftritt einzustellen. Ich habe ihr daher mit Bescheid vom 5. Juli 2023 untersagt, den von ihr betriebenen Facebook-Auftritt weiter zu betreiben. Darüber informierte ich in einer Pressemitteilung und veröffentlichte meinen Untersagungsbescheid.

Tätigkeitsbericht Datenschutz 2022:
↗ sdb.de/tb2022

Untersagungsbescheid zur Facebook-Fanpage der Sächsischen Staatskanzlei:
↗ sdb.de/tb2301

Wie zu erwarten, erhob die SK hiergegen Klage. Unerwartet war hingegen, dass ich auch durch die Meta Platforms Ireland (Meta), zu der Facebook gehört, wegen meines Bescheids an die SK verklagt wurde. Ich halte diese sogenannte Drittanfechtungsklage wegen fehlender Klagebefugnis bereits für unzulässig. Eine solche wäre gemäß § 42 Abs. 2 VwGO gegeben, wenn ein Antragsteller hinreichend substanziiert Tatsachen vorträgt, die es zumindest als möglich erscheinen lassen, dass er durch den zur Prüfung gestellten Rechtssatz in einem eigenen subjektiven Recht verletzt wird. Aus meiner Sicht besteht keine Möglichkeit, dass mein Bescheid auf rechtliche Interessen von Meta einwirken kann. Bei Meta tritt weder eine Verbesserung noch eine Verschlechterung der Rechtsposition ein. Gegenstand des Verfahrens ist die Frage, ob die SK in der Lage ist, die Rechenschaftspflicht gemäß Art. 5 Abs. 2 DSGVO zu erfüllen – nicht, ob Meta es kann.

Eine Befugnis folgt nach meiner Auffassung auch nicht aus den Grundrechten von Meta. Ein unmittelbarer Eingriff in die Berufs- und Eigentumsfreiheit (Art. 12 Abs. 1 und Art. 14 Abs. 1 Grundgesetz [GG]) liegt schon deswegen nicht vor, weil sich die Untersagungsverfügung nicht an Meta richtet, sondern ausschließlich die Nutzung von Facebook durch die SK betrifft. Auch eine mittelbare Grundrechtsbeeinträchtigung ist nicht ersichtlich. Der Schutz des Art. 12 Abs. 1 GG richtet sich nicht gegen jedwede auch nur mittelbar wirkende Beeinträchtigung des Berufs. Aus Art. 12 Abs. 1 GG folgt in der freien Wettbewerbswirtschaft nach der Rechtsprechung des Bundesverwaltungsgerichts im Grundsatz kein subjektives Recht auf Erhaltung eines bestimmten Geschäftsumfangs und auf Sicherung weiterer Erwerbsmöglichkeiten.

Ich werde über den weiteren Fortgang der gerichtlichen Verfahren berichten.

Was ist zu tun?
Die Präsenz in Sozialen Netzwerken sollte durch Verantwortliche generell hinterfragt werden; jedenfalls sind Facebook-Fanpages nicht DSGVO-konform zu betreiben. Öffentlichen Stellen in Sachsen steht als datenschutzfreundliche Alternative die Mastodon-Instanz der SDTB zur Verfügung (siehe 6.5.1): social.sachsen.de

1.3 Querschnittskontrollen zur Videoüberwachung in Tanzschulen

↗ § 26 BDSG; Art. 6 Abs. 1 Buchst. b DSGVO; Art. 13, Art. 58 Abs. 2 Buchst. a und b DSGVO

Der Tanzsport ist wieder „in" und begeistert mehr und mehr Menschen, nicht zuletzt aufgrund entsprechender TV-Formate. So verzeichnen die Tanzschulen nach wie vor einen regen Zulauf. Und da wundert es nicht, dass von den Tanzschulen am Eingang, in Umkleideräumen/Garderoben oder gar in den Tanzsälen angebrachte Videokameras nicht lange unbemerkt bleiben. Dies erklärt auch, weshalb ich hin und wieder Beschwerden wegen einer Videoüberwachung in Tanzschulen erhalte. Auf Befragen erklärten mir die Tanzschulbetriebe, dass sie die Videoüberwachung vornehmlich zum Einbruchschutz sowie zum Schutz von Wertsachen der Gäste einsetzen würden. Bei näherer Betrachtung stellte ich fest, dass in Einzelfällen große Teile der Tanzfläche überwacht wurden, und zwar auch während der Geschäftszeiten.

Außerhalb der Geschäftszeiten ist eine Videoüberwachung der Tanzschulräume aus Datenschutzsicht unproblematisch. Anders verhält sich dies, wenn die Tanzschüler/innen bei der Teilnahme an Tanzkurzen oder auch zu sonstigen Veranstaltungen (Tanzabende oder Bälle) in Ausübung ihres Hobbys beobachtet werden. Sie bewegen sich dabei – abhängig vom tänzerischen Niveau und Können – mehr oder weniger sicher und gekonnt auf der Tanzfläche und wähnen sich dabei im Normalfall unbeobachtet, rechnen sie doch nicht damit, dass jede gelungene Tanzfigur oder jeder Fehlversuch auch auf einem Datenspeicher festgehalten wird.

Es darf dabei nicht vergessen werden, dass sich Tanzschulen in der Mehrzahl der Fälle nicht nur an erwachsene Tanzbegeisterte richten, sondern auch Angebote für Kinder und Jugendliche vorhalten. Von der Videoüberwachung in einer Tanzschule sind außerdem auch die dort tätigen Beschäftigten unmittelbar und in besonderem Maße betroffen, können

sie sich doch einer im Regelfall anlasslosen Dauerbeobachtung nicht entziehen, ohne ihre arbeitsvertraglichen Pflichten zu verletzen.

Was den Einsatz von Videoüberwachungsanlagen anbelangt, hielt ich es daher für angezeigt, eine stichprobenhafte Überprüfung der in Sachsen ansässigen Tanzschulen vorzunehmen. Nach meiner Recherche gibt es in Sachsen ungefähr 150 Tanzschulen und vergleichbare Angebote. Das Spektrum reicht dabei von der klassischen Tanzschule mit einem breiten Angebotsspektrum über Spartenanbieter (Tango, Latinotänze) bis hin zu Bauchtanzschulen.

Ich entschloss mich in Anbetracht der großen Anzahl der Schulen proaktiv zu einer repräsentativen Stichprobe. Ausschlaggebend dafür waren die mir für anlassfreie Kontrollen nur begrenzt zur Verfügung stehenden Ressourcen sowie die Annahme, dass ungeachtet der mir vorliegenden Beschwerden Videotechnik in Tanzschulen jedenfalls nicht standardmäßig zum Einsatz kommt. Außerdem ging ich davon aus, dass unter den Betrieben, die teilweise zudem in Dachverbänden organisiert sind, ein Austausch dergestalt stattfindet, dass auch die weiteren Anbieterinnen und Anbieter dahingehend sensibilisiert werden, sich mit datenschutzrechtlichen Fragen speziell bei der Videoüberwachung auseinanderzusetzen.

Datenschutzrechtlich fehlt es für eine Videoüberwachung der für Kundinnen und Kunden sowie Mitarbeiter/innen zugänglichen Bereiche – während der Geschäftszeiten – an einer gesetzlichen Rechtfertigung. Auch wenn die Tanzschulen gelegentlich vorgeben, im Interesse ihrer Kundinnen und Kunden zu handeln, um beispielsweise Diebstähle im Umkleide- und Garderobenbereich aufzuklären, kann dies eine Videoüberwachung letztlich nicht rechtfertigen. Es bleibt dabei nicht selten außer Betracht, dass es andere, noch dazu effektivere Möglichkeiten gibt, das Eigentum der Kundinnen und Kunden zu schützen (wie beispielsweise verschließbare Fächer oder eine Zutrittskontrolle über Chipkarte etc.). Einbrüche werden in aller Regel in den Abend-/Nachtstunden verübt, also außerhalb der (wöchentlichen) Betriebszeiten

von Tanzschulen. Ob eine Videoüberwachung dann überhaupt brauchbare Bilder liefert, die zur Tataufklärung und Täterfeststellung führen können, mag zu Recht in Zweifel gezogen werden. Vor der Tanzschule liegende öffentliche Bereiche dürfen nicht überwacht werden.

Zumindest einige Betriebe scheinen sich der datenschutzrechtlichen Problematik wenigstens bewusst gewesen zu sein. Anders lässt sich nicht erklären, dass sie über die Videoüberwachung auf der Tanzschulen-Homepage informiert haben oder in die Mitgliedschaftsverträge entsprechende Passi aufgenommen haben. Auch wenn naheliegt, dass sie damit eine Einwilligung in die Videoüberwachung erreichen wollten, lässt sich eine Videoüberwachung nicht darauf stützen. Vertragliche Einwilligungen würden dem gesetzlichen Koppelungsverbot nicht standhalten (Art. 7 Abs. 4 Datenschutz-Grundverordnung [DSGVO]). Im Übrigen lässt sich bei einer Tanzschule mit einem großen und sich ständig ändernden Kundinnen- und Kundenbestand eine von den vertraglichen Vereinbarungen losgelöste Einwilligung bereits aus rein praktischen Gründen nicht umsetzen. Sobald eine Kundin oder ein Kunde die Einwilligung verweigert oder widerruft, wäre für die Zeit seiner Anwesenheit die gesamte Videoüberwachung außer Betrieb zu nehmen. Abgesehen davon stellt sich natürlich die Frage, warum man – freiwillig – eine solche Einwilligung überhaupt erteilen sollte.

Nicht zu vernachlässigen ist, dass Beschäftigte, hier also insbesondere die Tanzlehrer/innen, beim Umgang mit ihren personenbezogenen Daten einen besonderen Schutz genießen, der eine Überwachung und damit einhergehende Verarbeitung personenbezogener Daten im Beschäftigungsverhältnis nur bei Vorliegen besonderer Voraussetzungen zulässt, § 26 Bundesdatenschutzgesetz (BDSG). Auch insoweit sehe ich in einer Einwilligungslösung keine tragfähige Lösung, zumal mit der Videoüberwachung für die Beschäftigten auch kein rechtlicher oder wirtschaftlicher Vorteil verbunden ist (vgl. § 26 Abs. 2 Satz 2 BDSG), sondern stattdessen ein erhöhter Überwachungsdruck einhergeht.

Bei der Auswahl der infrage kommenden Tanzschulen legte ich Wert darauf, eine sich möglichst an den Zahlen der Einwohnerinnen und Einwohner orientierende flächenmäßig gleichmäßige Verteilung der befragten Betriebe sicherzustellen. Heraus kam schließlich eine Liste mit insgesamt 30 Tanzschulen. Nach einer ersten Befragung stellte sich die Situation wie folgt dar:

Tanzschulen mit Kameras	9	30 %
Tanzschulen ohne Kameras	21	70 %

Bei den Tanzschulen, die Videokameras im Einsatz hatten, ergab sich letzten Endes folgendes Bild:

Zulässiger Betrieb (nur außerhalb der Geschäftszeiten oder keine Tanz-, Aufenthalts- und Sitzbereiche)	5
Videoüberwachung während der Geschäftszeiten	2
Kamerademontage	2

Drei Tanzschulen setzten die datenschutzrechtlichen Vorgaben vorbildlich um, indem sie den Kamerabetrieb (teilweise gekoppelt an eine Alarmanlage) auf die Zeiten außerhalb des Tanzschulbetriebs begrenzten. In einer anderen Tanzschule war die einzig vorhandene Videokamera nur auf die in der Garderobe angebrachten Kleiderständer gerichtet. Nachdem keine Umkleidebereiche direkt davon betroffen waren, war hiergegen nichts einzuwenden.
Eine Tanzschule nahm mein Schreiben sogleich zum Anlass, das ohnehin funktionsuntüchtige Videoüberwachungssystem zu deinstallieren. Auch in einem anderen Fall entschloss sich der Inhaber der Tanzschule letzten Endes dazu, die einzig vorhandene Videokamera zu entfernen. Allerdings war diese bis zu jenem Zeitpunkt so angebracht, dass damit für die Kunden vorgesehene Sitzbereiche und auch große Teile des Ausschanktresens im Blickfeld der Kamera lagen. Betroffen waren also nicht nur die Tanzbegeisterten, sondern

auch die dort tätigen Mitarbeiter und Mitarbeiterinnen, die einem ständigen Überwachungsdruck ausgesetzt gewesen sein dürften. Hinzu kam, dass aufgrund fehlender technischer Einstellmöglichkeiten ein jederzeitiger Zugriff auf die Livebilder via Smartphone möglich war. So kam ich letzten Endes nicht umhin, in diesem Fall eine Verwarnung (Art. 58 Abs. 2 Buchst. b DSGVO) auszusprechen.

Bei einem weiteren Anbieter stellte sich heraus, dass zwar mehrere Videokameras in den Räumen der Tanzschule installiert waren, entsprechende Livebilder jedoch aufgrund einer Änderung des Betriebssystems nicht (mehr) abrufbar waren. Da nur während der Schließzeiten der Tanzschule Aufzeichnungen angefertigt wurden, konnte ich dem aus Datenschutzsicht nichts entgegenhalten. In Anbetracht der jederzeitigen Möglichkeit allerdings, mittels Aufspielen eines neuen Betriebssystems wieder die Zugriffsmöglichkeit auf die Livebilder herzustellen, schloss ich den Vorgang mit einer Warnung nach Art. 58 Abs. 2 Buchst. a DSGVO ab.

Eine weitere Tanzschule hatte insgesamt vier Videokameras im Betrieb. Zwei Videokameras waren nur auf Notausgänge gerichtet, was nicht zu beanstanden war. Allerdings war eine andere Videokamera auf Tanzflächen gerichtet, eine weitere Kamera hatte auch Aufenthalts- und Sitzbereiche im Sichtfeld. Dementsprechend waren auch dort Kunden, Kundinnen sowie Mitarbeiter und Mitarbeiterinnen unter potenzieller Dauerbeobachtung. Auf mein Einwirken hin veranlasste der Betreiber der Tanzschule schließlich eine Änderung der Betriebszeiten für sämtliche Videokameras, sodass damit datenschutzkonforme Zustände hergestellt waren.

Im letzten Fall kamen insgesamt acht Videokameras zum Einsatz, verteilt über Treppenhausbereiche, Tanzsäle, den Tanzschuleingang sowie den Außenbereich. Aufgrund der wenig ausgeprägten Kooperationsbereitschaft des Tanzschulunternehmens und der fortwährend an den Tag gelegten Verschleppungstaktik konnte ich den Vorgang noch nicht abschließen. Problematisch ist dabei insbesondere, dass die Videokameras eine Vielzahl an Einstellmöglichkeiten bieten. Nachdem einzig die Geschäftsführung über Smartphone zu-

griffsberechtigt ist, lässt sich hierüber ortsunabhängig jederzeit ein Blick auf die Livebilder nehmen.

Schwierigkeiten bereitet es den Kamerabetreibern und -betreiberinnen offensichtlich nach wie vor, mittels geeigneter Schilder ihren datenschutzrechtlichen Informationspflichten nachzukommen (Art. 13 DSGVO). So verwundert es nicht, dass ich in vier der von mir überprüften Fälle die vorhandenen Hinweisschilder bemängeln musste. Entweder kamen nur die von der Herstellerin bzw. der Kamerahersteller beigelegten Hinweisschilder – diese erschöpfen sich in einem kurzen Warnhinweis, ergänzt um ein Kamerapiktogramm – zum Einsatz. Oder aber die verwendeten Hinweise waren unzureichend, oder es fehlten wesentliche Angaben.

Ich verweise hierzu stets auf die zwischen den Datenschutzaufsichtsbehörden abgestimmten Hinweise, die auch in meinem Internetauftritt zum Download bereitstehen. Diese sehen bei einer Videoüberwachung zunächst ein vorgelagertes Hinweisschild vor, auf dem sich alle wesentlichen Informationen befinden. Darin sollte auch ein Hinweis auf das vollständige Informationsblatt enthalten sein. Jenes enthält zusätzlich Angaben zu Empfängern sowie die in der Datenschutz-Grundverordnung enthaltenen Betroffenenrechte (Art. 15 ff. DSGVO). Das vollständige Informationsblatt muss an geeigneter Stelle angebracht werden, beispielsweise an der Eingangstüre, oder im Tresenbereich, im Internet oder anderweitig vorgehalten werden, um es bei Bedarf den betroffenen Personen zur Verfügung stellen zu können.

In der Gesamtbetrachtung lässt sich feststellen, dass sich meine anfängliche Befürchtung, Videokameras würden in großem Stil in Tanzschulen zum Einsatz kommen, nicht bestätigt hat. Damit wird einmal mehr deutlich, dass sich meiner Behörde in Anbetracht des Beschwerdeaufkommens oftmals ein anderes Bild der Wirklichkeit bietet, was in der Natur der Sache liegen dürfte.

Was ist zu tun?
Tanzschulenbetreiber/innen dürfen während der Geschäftszeiten keine Tanzflächen, Sitz- und Aufenthalts- und Umkleidebereiche sowie Dauerarbeitsplätze von Beschäftigten überwachen. Außerdem sind Informationspflichten zu beachten und entsprechende Hinweisschilder anzubringen.

1.4 Querschnittskontrollen bei Kommunen

↗ § 13 und § 14 Abs. 1 Satz 2 SachsDSDG, § 30 SachsPBG, Art. 58 Abs. 1 Buchst. b DSGVO

Auch im Jahr 2023 hat meine Behörde datenschutzrechtliche Querschnittskontrollen bei Kommunen gemäß Art. 58 Abs. 1 Buchst. b Datenschutz-Grundverordnung (DSGVO), § 14 Abs. 1 Satz 2 Sächsisches Datenschutzdurchführungsgesetz (SächsDSDG) fortgesetzt, nachdem diese pandemiebedingt mehrere Jahre lang ausfallen mussten.

Im Berichtszeitraum wurden eine große Kreisstadt und eine kleinere Kommune überprüft.

Vorrangig habe ich dabei wieder Bürger- und Ratsinformationssysteme, Bekanntmachungen und Veröffentlichungen im Internet und Amtsblatt, Einhaltung der Informationssicherheit sowie die Verarbeitung von Beschäftigtendaten und Personalaktenführung überprüft. Ich konnte auch in diesem Jahr keine (wesentlichen) Verstöße feststellen und bin mit der Einhaltung des Datenschutzes auf kommunaler Ebene im Großen und Ganzen zufrieden.

Erfreulich ist, dass das Thema Informationssicherheit in den Kommunen bis hin zur Leitungsebene ernst genommen wird. Die Vorfälle in anderen Bundesländern, bei denen Kommunen durch Schadsoftware teilweise wochenlang nicht arbeitsfähig waren, haben sicherlich dazu beigetragen, das Bewusstsein für Sicherheit zu stärken und entsprechende Investitionen zu tätigen.

Allerdings wurde bei den Kontrollen auch mein Eindruck bestätigt, dass die kommunale Videoüberwachung (in diesen Fällen an Schule und Museum) immer mehr an Bedeutung gewinnt, die datenschutzrechtlichen Anforderungen indes doch noch etwas stiefmütterlich behandelt werden. Hierzu habe ich die betreffenden Gemeinden beraten und auf bestehende Mängel hingewiesen.

Orientierungshilfe für die Videoüberwachung durch sächsische Kommunen:
↗ sdb.de/vue16

1.5 Schwärzung von Sitzungsunterlagen für Stadträte

↗ § 19 Abs. 1 Satz 1, § 36 Abs. 3, § 36 b SächsGemO; § 32 Abs. 3, § 32 b SächsLKrO; Art. 4 Nr. 2, Art. 6 Abs. 1 Buchst. e, Art. 6 Abs. 2 DSGVO

Tätigkeitsbericht Datenschutz 2022:
↗ sdb.de/tb2022

In meinem vorigen Tätigkeitsbericht (Tätigkeitsbericht 2022, 2.2.2, Seite 39 ff.) ging es um die Anfang 2022 verabschiedete Kommunalrechtsnovelle.

Einer der zentralen Punkte dieser Gesetzesänderung war die Einführung einer Veröffentlichungspflicht von Informationen und Unterlagen aus Sitzungen des Gemeinderats an die Bevölkerung, bereinigt um personenbezogene Daten oder Betriebs- und Geschäftsgeheimnisse, § 36 b Sächsische Gemeindeordnung (SächsGemO), parallel hierzu § 32 b Sächsische Landkreisordnung (SächsLKrO) für Unterlagen aus Kreisräten.

Nun erreichte mich die Eingabe zweier Gemeinderäte einer sächsischen Gemeinde zu dieser Thematik. Sie beklagten, dass der Bürgermeister unter Berufung auf die Norm des § 36 b SächsGemO bereits vor Ausgabe von Sitzungsunterlagen an Gemeinderäte Schwärzungen vornimmt. Konkret ging es um Unterlagen zu Firmendaten, die zur Vorbereitung des Zuschlagbeschlusses für eine kommunale Vergabe ausgereicht worden sind. Die jeweiligen Firmennamen und Anschriften wurden in den Sitzungsunterlagen geschwärzt. Da sich die Gemeinderäte mit den Schwärzungen nicht einverstanden zeigten, beim Bürgermeister aber nicht durchdringen konnten, wandten sie sich an mich.

Der Bürgermeister der Gemeinde begründete die Schwärzungen wie folgt: Die Bieterauswahl solle weitestgehend anonymisiert erfolgen, damit die Räte in ihrer Entscheidung von sachlichen Wertungskriterien ausgehen und keine subjektiven Entscheidungen anhand des Firmennamens treffen sollen. Dieser Auffassung kann ich nicht folgen, aus den folgenden Gründen:

> „Den Ratsmitgliedern sind alle Unterlagen, die für die Beratung zur Bildung einer (vorläufigen) Meinung […] benötigt werden, zur Verfügung zu stellen", Sächsisches Oberverwaltungsgericht (SächsOVG), Beschluss vom 28. Juli 2009, Aktenzeichen 4 B 406/9.

Werden nun durch die Bereitstellung der Sitzungsunterlagen an die Stadträte personenbezogene Daten verarbeitet, so richtet sich diese Datenverarbeitung nach Art. 6 Abs. 1 Buchst. e Datenschutz-Grundverordnung (DSGVO). Gemäß Art. 6 Abs. 2 DSGVO können die Mitgliedsstaaten spezifische Bestimmungen zur Anpassung und Präzisierung der Vorschriften dieser Verordnung erlassen. Die Norm des § 36 Abs. 3 Satz 1 SächsGemO (parallel dazu für die Landräte § 32 SächsLKrO) ist eine solche Norm. Demnach sind die Sitzungsunterlagen bei Einberufung der Sitzung beizufügen, soweit nicht das öffentliche Wohl oder berechtigte Interessen Einzelner entgegenstehen.
Das SächsOVG ergänzt diese Vorschrift in der oben zitierten Entscheidung noch wie folgt:

> „[…] Dabei ist auf den Informationsbedarf eines verständigen Ratsmitglieds abzustellen, das sich im Rahmen seiner auszuübenden ehrenamtlichen Tätigkeit in den wichtigen Angelegenheiten der Gemeinde auf dem Laufenden hält. Um welche Unterlagen es sich hierbei handelt, ist eine Frage des Einzelfalls und lässt sich nicht allgemein, sondern nur nach Art des jeweiligen Beratungs- bzw. Verhandlungsgegenstands, insbesondere seiner Komplexität und Tragweite bestimmen", vgl. hierzu SächsOVG, Beschluss vom 28. Juli 2009, Az. 4 B 406/9.

In einem anderen Urteil führt das SächsOVG aus:
Unterlagen, die vom Landrat (bzw. Bürgermeister) zur Vorbereitung der Sitzungen des Kreistags an die Kreisräte ausgereicht werden, seien **interne Dokumente** der Verwaltung,

deren Zweck allein in der Verwendung innerhalb des Kreisrats besteht. Sie dienen der Unterrichtung innerhalb des Gremiums und der Vorbereitung von Abstimmungen, Urteil vom 30. August 2019, Az.: 4 C 12/17.

Es besteht vor diesem Hintergrund grundsätzlich keine datenschutzrechtliche Notwendigkeit, personenbezogene Daten in amtlichen Unterlagen, die seitens des Bürgermeisters den einzelnen Stadträten zur Verfügung zu stellen sind, teilweise oder in personenbezogenen Inhalten zu schwärzen. Hier ist dem **umfassenden Informationsbedarf** der Räte Rechnung zu tragen. Es muss beachtet werden, dass die Gemeinderäte als Teil der Verwaltung anerkannt sind und zudem einer gesetzlichen Verschwiegenheitspflicht nach § 19 Abs. 1 Satz 1 SächsGemO unterliegen.

Zudem musste ich dem Bürgermeister noch einmal verdeutlichen, dass auch nach der neuen Rechtslage die Unterlagen nicht eins zu eins, so, wie sie an die Ratsmitglieder ausgereicht wurden, zu veröffentlichen sind. Vielmehr erfolgt (erst) bei Veröffentlichung der Unterlagen gemäß § 36 b Satz 3 SächsGemO die Bereinigung der personenbezogenen Daten (bzw. Betriebs- und Geschäftsgeheimnisse).

Zwar hat der Bürgermeister diese Ausführungen angenommen, schwärzte aber auch weiterhin ohne weitere Begründung die Sitzungsunterlagen. Der Bürgermeister berief sich nunmehr darauf, ihm würde ein Ermessen zustehen bei der Entscheidung, welche Tatsachen für die Behandlung im Gemeinderat maßgeblich seien und welche nicht.

Auch diese Wertung ist aber nicht rechtmäßig und widerspricht zudem der Auffassung des SächsOVG. In dem Urteil vom 30. August 2019, Az.: 4 C 12/17 heißt es nämlich weiterhin:

Bei den „für die Beratung erforderlichen Unterlagen" handelt es sich demnach um einen unbestimmten Rechtsbegriff, der einer vollständigen gerichtlichen Überprüfung unterliegt. Nach Sinn und Zweck des § 36 Abs. 3 Satz 1 Halbsatz 2 SächsGemO ist auf den Informationsbedarf eines verständigen Gemeinderats abzustellen, der sich im Rahmen seiner „uneigennützig und verantwortungsbewusst" (§ 19 Abs. 1 SächsGemO)

auszuübenden ehrenamtlichen Tätigkeit jedenfalls in den wichtigen Angelegenheiten der Gemeinde auf dem Laufenden hält, a. a. O.

Es ist somit ein (komplett gerichtlich überprüfbarer) Beurteilungsspielraum und kein Ermessen des Bürgermeisters an dieser Stelle gegeben. Hiermit sind Begründungs- und Dokumentationspflichten verbunden. Pauschale Behauptungen reichen an dieser Stelle nicht. Dies gilt auch für die Wertung, ob einer ungeschwärzten Ausreichung an die Räte das öffentliche Wohl oder berechtigte Interessen Einzelner gemäß § 36 Abs. 3 Satz 1 SächsGemO entgegenstehen.

Ein Verstoß gegen die DSGVO liegt meiner Ansicht hier darin, dass die praktizierte „unzulässige Datenminimierung" gegen Art. 6 DSGVO verstößt, da eine Rechtsgrundlage für die Schwärzung schlicht nicht vorliegt. Auch die Schwärzung (wie im Übrigen die Löschung von Daten) ist nämlich eine Form der Datenverarbeitung gemäß Art. 4 Nr. 2 DSGVO.

Ich kann nach alledem somit die auch im Tätigkeitsbericht 2022 dargelegte Wertung bekräftigen und festhalten, dass Sitzungsunterlagen bereits laut SächsOVG als **interne Dokumente der Verwaltung zu werten** sind und in erster Linie der Unterrichtung innerhalb des Gremiums und der Vorbereitung von Abstimmungen dienen.

Was ist zu tun?
Sitzungsunterlagen, die für Beratungen erforderlich sind, sind Stadt- und Gemeinderäten vollständig und ungeschwärzt vorzulegen. Als interne Dokumente der Verwaltung unterliegen sie der Verschwiegenheitspflicht. Die Schwärzung personenbezogener Daten ist auch ein Verarbeitungsvorgang nach DSGVO.

1.6 Zulässigkeit der Verarbeitung von Informationen aus erweiterten Führungszeugnissen

↗ § 30a Abs. 3 BZRG, § 72a Abs. 5 SGB VIII, Art. 5 Abs. 1 Buchst. c DSGVO

Immer wiederkehrend werde ich in bestimmten Einzelfällen mit der Frage konfrontiert, ob es seitens des Arbeitgebers, der Arbeitgeberin oder des Dienstherrn zulässig sei, erweiterte Führungszeugnisse einzuholen. Tatsächlich kommt es bei der Möglichkeit der Einholung von erweiterten Führungszeugnissen nicht selten zu fehlerhafter Rechtsanwendung, einhergehend mit der Verarbeitung nicht erforderlicher bzw.

überschießender Informationen. Und nicht nur ausnahmsweise erfolgt diese auch durch öffentliche Stellen.

Im letzten Berichtszeitraum wurde ich damit konfrontiert, dass eine Stadtverwaltung sämtliche Mitarbeiterinnen, Mitarbeiter und Bedienstete anwies, ein erweitertes Führungszeugnis zu beantragen und dieses beizubringen.

Gemäß § 30a Bundeszentralregistergesetz (BZRG) wird einer Person auf Antrag ein erweitertes Führungszeugnis erteilt, soweit dies in gesetzlichen Bestimmungen unter Bezugnahme auf § 30a vorgesehen ist oder eine berufliche oder ehrenamtliche Beaufsichtigung, Betreuung, Erziehung oder Ausbildung Minderjähriger oder vergleichbare Kontakte mit Minderjährigen stattfinden, Abs. 1 der Vorschrift. Arbeitgeber/in oder Dienstherr haben der antragstellenden Personen zu bestätigen, dass die vorgenannten Voraussetzungen und damit eine Notwendigkeit vorliegen, § 30a Abs. 2 BZRG.

Die entsprechende Anweisung gegenüber sämtlichen Beschäftigten und Beamtinnen und Beamten in dem Beispielsfall fand gemäß der vorgenannten Vorschrift also keine gesetzliche Stütze. Ich forderte die Stadtverwaltung daher auf, die entsprechende Anweisung zurückzunehmen und eine schon durchgeführte Verarbeitung nicht erforderlicher gespeicherter Daten umgehend einzustellen bzw. gegebenenfalls erhobene Informationen wieder zu löschen. Zum Ende des Berichtszeitraums war der Vorgang noch nicht vollständig abgeschlossen.

Eine ebenso häufig vorkommende Frage im inhaltlichen Zusammenhang ist, ob das erweiterte Führungszeugnis, sofern seine Beantragung geeignet und erforderlich ist, in die Personalakte aufzunehmen ist. Hierzu vertrete ich die Auffassung, dass die Einsichtnahme und der Vermerk über die erfolgte Einsicht bzw. über fehlende oder bestehende einschlägige Eintragungen von Vorstrafen zur Aufgabenerfüllung genügt, Art. 5 Abs. 1 Buchst. c Datenschutz-Grundverordnung. Nach Einsichtnahme durch die personalverwaltende Stelle können entsprechende Führungszeugnisse den betroffenen Beschäftigten, Beamtinnen und Beamten wieder zurückgegeben werden. Eine derartige Verfahrens-

Was ist zu tun?
Die Informationen aus erweiterten Führungszeugnissen sind nur in den gesetzlich bestimmten Fällen bzw. in den Zusammenhängen der Betreuung Minderjähriger durch Verantwortliche zu verarbeiten. Die Führungszeugnisse selbst sollen nicht in Personalakten Aufnahme finden. Die amtlichen Unterlagen sind zur Einsichtnahme vorzulegen. Die erneute Vorlage aktueller Zeugnisse ist in angemessen Zeitabständen durchführbar.

weise ist im Einklang mit § 72a Abs. 5 Sozialgesetzbuch VIII (SGB VIII). Zu verweisen ist der Vollständigkeit halber auch auf § 30a Abs. 3 BZRG, wonach „die Daten aus einem erweiterten Führungszeugnis" im Rahmen der Erforderlichkeit und zweckbezogen zu verarbeiten sind, vgl. dazu den konkreten Wortlaut der Vorschrift.
Soweit die Datenverarbeitung aus erweiterten Führungszeugnissen gesetzmäßig erfolgt, ist nach meiner Einschätzung auch eine erneute Vorlage eines aktuellen Führungszeugnisses zur Sicherstellung einer Betriebsfähigkeit mit geeignetem Personal in Abständen von drei bis fünf Jahren ohne Weiteres vertretbar.

1.7 Beschlagnahmen von Mobiltelefonen nach einer polizeilichen Einkesselung zahlreicher Personen

↗ §§ 94, 98, 110, 111n, 163b StPO; § 500 StPO in Verbindung mit § 75 Abs. 2 BDSG

Am Rande einer Demonstration Anfang Juni 2023 in einer sächsischen Großstadt kam es zu Angriffen auf Beamte und Sachbeschädigungen unter anderem an geparkten Autos, woraufhin Einsatzkräfte der Polizei eine große Personengruppe einschlossen. Sämtliche Personen aus dem „Polizeikessel" wurden einer Identitätsfeststellung unterzogen, Mobiltelefone der Betroffenen wurden beschlagnahmt. Von der Umschließung waren 1.323 Personen betroffen, darunter 104 Jugendliche und zwei strafunmündige Kinder. Insgesamt 383 Mobiltelefone wurden beschlagnahmt.
An den auf die Ereignisse folgenden Tagen erreichten mich mehrere Anfragen von Eltern Jugendlicher, die von den Maßnahmen betroffen waren. Aus den Anfragen sprach die Sorge über den Verbleib der Mobiltelefone und den Umgang mit den auf den Geräten befindlichen Daten.

Auf meine Bitte um Auskünfte teilten mir die zuständige Staatsanwaltschaft und die ermittelnde Polizeibehörde mit, dass die Identitätsfeststellungen gemäß § 163b Abs. 1 Strafprozessordnung erfolgt seien. Grundlage sei der gegen die von der Umschließung erfassten Personen gerichtete Anfangsverdacht des Landfriedensbruchs in einem besonders schweren Fall, des tätlichen Angriffs auf und des Widerstands gegen Vollstreckungsbeamte sowie der gefährlichen Körperverletzung gewesen. Die Beschlagnahme der Mobiltelefone sei wegen Gefahr im Verzug ohne vorherige richterliche Anordnung erfolgt. Soweit gegen die Beschlagnahme Widerspruch eingelegt und Antrag auf gerichtliche Entscheidung gestellt worden sei, seien die Akten dem zuständigen Ermittlungsrichter zur Entscheidung vorgelegt worden. Nach den zum Zeitpunkt der Auskunft vorliegenden Beschlüssen sei in allen Fällen die Beschlagnahme der Mobiltelefone richterlich bestätigt worden.

Daran war datenschutzrechtlich nichts auszusetzen.

Die Beschlagnahme von (großen) Datenträgern bringt es mit sich, dass die Strafverfolgungsbehörden immense Datenmengen erhalten, die nicht verfahrensrelevant und damit für die Erfüllung der gesetzlichen Aufgaben der Behörden nicht erforderlich sind. Bei der heute üblichen Nutzung von Mobiltelefonen dürften sich neben eigenen Daten der Telefonbesitzer auch große Mengen von Daten Dritter (Familienangehörige, Freunde, Bekannte, Kommunikationspartner) auf den Geräten befinden, es ist wahrscheinlich, dass auch Daten aus dem Kernbereich privater Lebensgestaltung gespeichert sind.

Ich habe die Strafverfolgungsbehörden darauf aufmerksam gemacht, dass angesichts dessen, dass der Anteil verfahrensrelevanter Daten auf den beschlagnahmten Mobiltelefonen – sofern sich überhaupt verfahrensrelevante Daten darauf befinden – verschwindend gering sein dürfte und eine Beschlagnahme des gesamten Datenbestandes (neben der Beschlagnahme des Mobiltelefons als Datenträger) ebenso unverhältnismäßig wäre wie dessen dauerhafte Speicherung trotz Verfahrensirrelevanz. In diesem Zusammenhang wies ich auch darauf hin, dass nach einer eventuellen Durchsicht

des Datenbestandes beschlagnahmter Mobiltelefone die gesetzlichen Anforderungen und die Vorgabe des Bundesverfassungsgerichts eingehalten und nicht verfahrensrelevante Daten unverzüglich gelöscht bzw. herausgegeben werden müssen (§ 75 Abs. 2 Bundesdatenschutzgesetz, unter anderem BVerfG vom 12. April 2005 - 2 BvR 1027/02).

Die Staatsanwaltschaft bestätigte, dass die einschlägige Rechtsprechung bekannt sei und dass die Ermittlungsbehörden dem Verhältnismäßigkeitsgrundsatz und dem Übermaßverbot durch geeignete Maßnahmen und Beschränkungen im Umfang der Ermittlungen im vorliegenden Verfahren Rechnung trügen.

Später erfolgte aufgrund einer Allgemeinverfügung der Staatsanwaltschaft eine Freigabe bzw. Herausgabe von im Juni beschlagnahmten Mobiltelefone, nachdem die Daten zuvor gesichert worden waren.

Ende Oktober war eine Auswertung der von den Mobiltelefonen gesicherten Daten noch nicht erfolgt. Die Löschung der nicht erforderlichen bzw. nicht verfahrensrelevanten Daten werde, wie die Polizei mitteilte, nach Abschluss der Auswertung in Abstimmung mit der Staatsanwaltschaft veranlasst.

Ich habe derzeit keine Anhaltspunkte dafür, dass die Datenverarbeitung durch die Strafverfolgungsbehörden in diesem Vorgang unverhältnismäßig ist. Die beschriebene Vorgehensweise der Behörden begegnet keinen durchgreifenden Bedenken; allerdings sollte eine Auswertung der gesicherten Datenbestände zeitnah erfolgen, um die massenhaften Daten, die erwartungsgemäß verfahrensirrelevant, aber höchstpersönlicher, teils vermutlich auch kernbereichsspezifischer Natur sind, löschen zu können und der Möglichkeit staatlicher Kenntnisnahme zu entziehen.

Was ist zu tun?

Bei der Sicherstellung/Beschlagnahme von Datenträgern erlangen Strafverfolgungsbehörden Zugriff auf Massen personenbezogener Daten ohne Verfahrensrelevanz, die teils höchstpersönlicher Natur sind und/oder Berufsgeheimnisse oder den Kernbereich privater Lebensgestaltung betreffen können. Das Gesetz verpflichtet die Behörden, Daten, die nicht für die Erfüllung ihrer gesetzlichen Aufgaben erforderlich sind, auszusondern und zu löschen.

1.8 Befugnisse der Polizei zur Überprüfung der Zuverlässigkeit von Personen vor Großereignissen

↗ § 88 SächsPVDG

Im vergangenen Jahr stand ich zur Erörterung von Fragen zum Akkreditierungsverfahren zur Fußball-Europameisterschaft 2024 über einen längeren Zeitraum im Kontakt mit dem Sächsischen Staatsministerium des Innern.

Ein Thema war dabei der Regelungsgehalt von § 88 Sächsisches Polizeivollzugsdienstgesetz (SächsPVDG), der die Polizei befugt, im Vorfeld besonders gefährdeter Veranstaltungen personenbezogene Daten an öffentliche und nichtöffentliche Stellen zu übermitteln, wenn die Übermittlung zu dem Zweck einer Zuverlässigkeitsüberprüfung erforderlich ist, mit schriftlicher Einwilligung des Betroffenen erfolgt und im Hinblick auf den Anlass dieser Überprüfung angemessen ist. Die Übermittlung an eine nichtöffentliche Stelle ist auf die Auskunft zum Vorliegen der Zuverlässigkeitsbedenken beschränkt.

Die Europameisterschaft 2024 findet in Deutschland statt, die Spielorte liegen in sieben Bundesländern, im Freistaat Sachsen wird Leipzig eine Gastgeberstadt sein.

Die polizeiliche Begleitung der Vorbereitung der Europameisterschaft und ihrer Austragung umfasst unter anderem die Zuverlässigkeitsprüfung bzw. die polizeiliche Zuarbeit zum Akkreditierungsverfahren, das Personen durchlaufen müssen, die – zumeist aus beruflichen Gründen – in sicherheitsrelevanten Bereichen der Austragungsstätten zum Einsatz kommen.

In der Abstimmung der betroffenen Landespolizeien zeigten sich für einen föderalistischen Staat nicht ungewöhnliche Unterschiede der jeweiligen polizeilichen Befugnisse und Möglichkeiten, zu Zwecken von Zuverlässigkeitsüberprüfungen vor Großereignissen personenbezogene Daten zu verarbeiten.

In Sachsen ist § 88 SächsPVDG die einschlägige Vorschrift. Sie wurde aufgrund der Erfahrungen bei der Austragung der Fußball-Weltmeisterschaft 2006 in Deutschland in das damalige Sächsische Polizeigesetz aufgenommen (§ 44 SächsPolG alte Fassung) und seitdem lediglich redaktionell geringfügig verändert. Die Regelung verdrängt als spezielle Vorschrift die allgemeine Datenerhebungsbefugnis des § 56 SächsPVDG (vgl. § 56 letzter Halbsatz SächsPVDG) und erlaubt der Polizei ausdrücklich (nur) die Übermittlung personenbezogener Daten, wobei die Übermittlung denklogisch auf die bei der Polizei vorhandenen bzw. ihrem direkten Zugriff unterliegenden personenbezogenen Daten begrenzt ist, da § 88 SächsPVDG nicht zu einer (vorherigen) Erhebung personenbezogener Daten bei Dritten, auch nicht bei Polizeibehörden anderer Länder oder bei Verfassungsschutzbehörden befugt. Der Gesetzgeber hat die Datenverarbeitung der Polizei bei Akkreditierungsverfahren anderer (öffentlicher oder privater) Stellen damit unmissverständlich auf die Übermittlung – vorhandener – Daten beschränkt, wobei die Übermittlung an private Stellen lediglich die Mitteilung umfasst, ob Zuverlässigkeitsbedenken bestehen.

Damit unterscheidet sich die sächsische Rechtslage durchaus von der in anderen Bundesländern, in denen die Polizei zum Zweck der Zuverlässigkeitsüberprüfungen vor gefährdeten Großveranstaltungen in unterschiedlichem Umfang auch Daten bei Dritten erheben darf. Allerdings ist eine enge Datenverarbeitungsbefugnis wie in Sachsen auch kein Alleinstellungsmerkmal des Freistaats (vgl. § 45a Allgemeines Sicherheits- und Ordnungsgesetz [ASOG Bln]).

Der Blick auf die Gesetzeslage oder die Praxis in anderen Ländern ist für die sächsische Polizei aber ohnehin irrelevant, da sie – als Staatsgewalt an Gesetz und Recht gebunden (Art. 20 Abs. 3 Grundgesetz, Art. 3 Abs. 3 Verfassung des Freistaates Sachsen) – allein die für sie geltenden Rechtsvorschriften zu beachten hat.

Unterschiedlich weite Befugnisse von Landespolizeien sind Ausdruck des Föderalismus, die Differenzen in der Gesetzeslage können und dürfen auch im Interesse möglichst gleich-

Was ist zu beachten?
Die verfassungsrechtlich verankerte Bindung der Verwaltung an Gesetz und Recht verlangt auch dann eine strenge Beachtung geltender gesetzlicher Vorschriften, wenn öffentlichen Stellen außerhalb des Freistaats in gleichen Sachverhalten mehr Befugnisse zustehen. Verfahrensabreden zwischen Stellen der Exekutive können gesetzliche Regelungen weder erweitern noch ersetzen.

laufender (und für private Veranstalter wie die UEFA bequemer) Verfahren nicht nivelliert werden. Das Recht und die vom Gesetzgeber beschlossenen Regelungen, mit denen in Grundrechte betroffener Personen eingegriffen wird, haben auch vor und während Fußball-Europameisterschaften Bestand.

Sollten Unterschiede in den Landesgesetzen zu nicht hinnehmbaren Lücken bei Überprüfungen von Personen führen, muss und kann im Vorfeld das zwischen dem (privaten) Veranstalter und den Behörden abzustimmende Verfahren für die Zuverlässigkeitsüberprüfungen angepasst werden.

2 Grundsätze der Datenverarbeitung

2.1 Datenverarbeitungsgrundsätze, Begriffsbestimmungen

2.1.1 Datenschutzrechtliche Verantwortlichkeit und Datenschutzbeauftragte/r in Eigenbetrieben

↗ §§ 95a SächsGemO, Art. 4 Nr. 7 DSGVO

Im Berichtszeitraum war zu klären, ob ein Eigenbetrieb als ein eigenständiger Verantwortlicher im Sinne der Datenschutz-Grundverordnung (DSGVO) zu qualifizieren ist und infolgedessen auch ein/e eigene/r Datenschutzbeauftragte/r zu bestellen ist bzw. bestellt werden kann.

Datenschutzrechtlicher Verantwortlicher ist gemäß der DSGVO jede „natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet", Art. 4 Nr. 7 DSGVO. Der Eigenbetrieb ist kommunalrechtlich keine eigenständige Rechtspersönlichkeit. Vielmehr kann die Gemeinde „Unternehmen ohne eigene Rechtspersönlichkeit als Eigenbetrieb führen, wenn Art und Umfang der Tätigkeit eine selbstständige Wirtschaftsführung rechtfertigen", § 95a Sächsische Gemeindeordnung (SächsGemO). Der Eigenbetrieb ist demnach unselbstständiger Teil der jeweiligen Gemeinde.

Im Kern der Frage ging es nun darum, ob aus der fehlenden kommunalrechtlichen Selbstständigkeit auch eine datenschutzrechtliche „Unselbstständigkeit" folgt und die oder der

Datenschutzbeauftragte der Stadt oder Kommune auch für Belange des Eigenbetriebs verantwortlich ist.

Beim Blick auf andere Bundesländer wird deutlich, dass bei dieser Frage unterschiedliche Ansichten bestehen. So wird einerseits unter meinen Kolleginnen und Kollegen vertreten, dass unabhängig von der fehlenden Rechtspersönlichkeit der Eigenbetrieb als datenschutzrechtlich selbstständig anzusehen sei, wenn dieser eigenverantwortlich über die Mittel und Zwecke der Datenverarbeitung entscheidet.

12. Tätigkeitsbericht (2005) für den öffentlichen Bereich:
↗ sdb.de/tb12oeb

Diese Ansicht teile ich indes so nicht, wie sie auch mein Amtsvorgänger bereits 2005 in seinem 12. Tätigkeitsbericht für den öffentlichen Bereich (1.7, Seite 41 f.) vertreten hat. Eigenbetriebe sind nach meiner Ansicht auch datenschutzrechtlich Teil der jeweiligen Gebietskörperschaft. Dieser ist schließlich auch nicht rechtsfähig, das heißt, er kann nicht selbstständiger Träger von Rechten und Pflichten sein, sondern diese sind immer abgeleitet von der Gebietskörperschaft. Dies gilt aus meiner Sicht auch unverändert für das Datenschutzrecht. Einen hinreichenden rechtlichen Grund, eine abweichende datenschutzrechtliche Wertung als in der übrigen Rechtsordnung vorzunehmen, besteht aus meiner Sicht nicht.

Dies ist aber wiederum aus meiner Sicht kein Hindernis für den Eigenbetrieb, eine/n eigene/n Datenschutzbeauftragte/n zu haben. Dies folgt aus dem Grundsatz, dass einem Verantwortlichen (hier der Gebietskörperschaft) nicht verwehrt ist, auch mehrere Datenschutzbeauftragte zu bestellen, jedenfalls dann, wenn – wie hier - organisatorisch eigenständige Teile bestehen. Es wäre deswegen nicht unzulässig, dass funktionell ein/e Datenschutzbeauftragte/r für den Eigenbetrieb tätig ist, der formell von der Gebietskörperschaft (als weiterer) Datenschutzbeauftragte/r bestellt wurde. Dies wird auch in den Erwägungsgründen zur DSGVO (Erwägungsgrund 97) so getragen.

Was ist zu beachten?
Eigenbetreibe sind keine eigenständigen Verantwortlichen, können aber (über ihre Gebietskörperschaft) eine/n eigene/n Datenschutzbeauftragte/n haben.

Da der anfragende Eigenbetrieb eine/n eigene/n Datenschutzbeauftragte/n bestellen wollte, konnte ich hierzu grünes Licht geben.

2.1.2 Relevantes aus dem Onlinehandel

↗ Art. 4. Nr. 7, Art. 5 Abs. 1 Buchst. a und c, Art. 13 DSGVO

Der Onlinehandel boomt und verzeichnet nach den Erhebungen des Statistischen Bundesamtes weiterhin steigende Umsatzzahlen.

Telefonnummer und Geburtsdatum als nicht zwingend notwendige Angaben

Bei jeder Bestellung im Internet sind Online-Händlern und -Händlerinnen einige persönliche Angaben zur Verfügung zu stellen. Zum Teil handelt es sich hier um Angaben, die in einem Pflichtfeld vorzunehmen sind und ohne die der Kauf nicht abgeschlossen werden kann, zum Teil nur um die freiwillige Angabe von Daten. Nicht jede Datenabfrage, die als Pflichtfeld gekennzeichnet ist, ist für den Abschluss und die Abwicklung eines Kaufs im Internet erforderlich.

Im Berichtszeitraum hat mich die Beschwerde eines Betroffenen erreicht, weil bei einem von ihm beabsichtigten Kauf im Internet im Rahmen des sogenannten Check-outs seine Telefonnummer sowie sein Geburtsdatum als Pflichtangaben abgefordert wurden.

Ich habe die Angaben geprüft; sie waren zutreffend.

Aus Sicht meiner Behörde steht die generelle und zwingend erforderliche Erhebung und Verarbeitung eines Geburtsdatums – unabhängig vom zu bestellenden Produkt – sowie einer Telefonnummer nicht im Einklang mit dem in Art. 5 Abs. 1 Buchst. a Datenschutz-Grundverordnung (DSGVO) normierten Prinzip der Rechtmäßigkeit einer Datenverarbeitung sowie mit dem in Art. 5. Abs. 1 Buchst. c DSGVO geregelten Grundsatz der Datenminimierung.

Eine Abfrage zum Alter oder sogar eines konkreten Geburtsdatums halte ich nur im Einzelfall für zulässig, so zum Beispiel dann, wenn der Vertragsschluss mit einem Minderjährigen gegen andere Rechtsnormen verstoßen würde.

Auch wird die Angabe einer Telefonnummer nur immer dann erforderlich sein, wenn größere Waren, wie zum Beispiel eine Waschmaschine, erworben werden sollen, die nur durch eine

Spedition geliefert werden können. In diesem Fall wird die Kenntnis der Telefonnummer tatsächlich notwendig sein, um den konkreten Liefertermin abzustimmen. Im Übrigen sollte es sich bei der Angabe der Telefonnummer um eine freiwillige Angabe handeln, da es dem Verkäufer unbenommen ist, über die ihm weiter bekannten Daten, wie zum Beispiel die E-Mail-Adresse, die bei Onlinekäufen regelmäßig anzugeben ist, einen ersten Kontakt zum Käufer herzustellen, um mit diesem dann die weiteren Kommunikationsmöglichkeiten abzustimmen.
Auf meine Bewertung habe ich den Verantwortlichen, der sehr einsichtig war, hingewiesen; seine Internetseite hat er daraufhin umgehend angepasst.

Der gewerbliche Verkäufer als Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO auf einer Verkaufsplattform wie eBay

Bei Verkaufsplattformen handelt es sich häufig um US-amerikanische Unternehmen, welche Online-Marktplätze betreiben, so auch eines der größten: eBay Inc. Auf der Internetplattform von eBay wird anderen Verkäufern und Verkäuferinnen sowie Händlern und Händlerinnen die Möglichkeit eingeräumt, ihre Waren/Leistungen anzubieten, die durch Endkunden bzw. -kundinnen erworben werden können. Der Vertragsschluss erfolgt zwischen dem/der Verkäufer/in und dem/der Händler/in und dem Endkunden bzw. der Kundin; eBay stellt hierfür lediglich die Plattform zur Verfügung.
Da der/die Verkäufer/in oder Händler/in Vertragspartner/in des Endkunden bzw. der Endkundin ist, ist er/sie nach Art. 4 Nr. 7 DSGVO datenschutzrechtlich verantwortlich für die Verarbeitung der personenbezogenen Daten der Endkunden bzw. Kundinnen im Rahmen des Zustandekommens und der Abwicklung der Bestellungen. In diesem Zusammenhang verarbeitet der/die Verkäufer/in oder Händler/in als datenschutzrechtlich Verantwortlicher regelmäßig die folgenden Datenkategorien: Name; Postadressdaten; E-Mail-Adresse; Informationen über die Ware oder Leistungen, die der Endkunde bzw. die Kundin erwerben möchte bzw. erwirbt.

Aus der datenschutzrechtlichen Verantwortlichkeit des Verkäufers oder der Verkäuferin bzw. des Händlers oder der Händlerin resultiert, dass dieser bzw. diese gemäß Art. 13 DSGVO über die Erhebung und Verarbeitung personenbezogener Daten zu informieren hat. Aber auch eBay Inc. ist datenschutzrechtlich verantwortlich und damit informationspflichtig nach Art. 13 DSGVO, da das Unternehmen als Betreiber der Plattform selbst Daten erhebt. Das ist unter anderem bei der Anlage eines Kontos der Nutzer/innen der Fall.

Im vergangenen Jahr habe ich eine Beschwerde erhalten, mit der mir angezeigt wurde, dass einer der gewerblichen Händler auf eBay mit Sitz im Freistaat Sachsen seiner Informationspflicht zur Erhebung und Verarbeitung personenbezogener Daten nicht nachkomme. Ich habe den Hinweis geprüft; er war zutreffend.

Den Händler habe ich auf seine Informationspflicht hingewiesen. Er hat gegenüber meiner Behörde zugesagt, die erforderliche Anpassung vorzunehmen.

Was ist zu beachten?
Nicht alle Daten, die bei einem Onlinekauf als Pflichtangaben abgefragt werden, sind für den Vertragsabschluss und die Durchführung des Vertrages erforderlich.
Händler/innen auf Online-Marktplätzen sind hinsichtlich der Verarbeitung von personenbezogenen Daten beim Verkauf Verantwortliche im Sinne von Art. 4 Nr. 7 DSGVO. Sie trifft auch die Informationspflichten gemäß Art. 13 DSGVO.

2.1.3 Videoüberwachung des Eingangsbereiches eines Wohnblocks – Nachtrag

↗ Art. 5 Abs. 2 DSGVO

Tätigkeitsbericht 2020:
↗ sdb.de/tb2020

Im Tätigkeitsbericht 2020 (2.2.26, Seite 78 ff.) hatte mein Amtsvorgänger von seiner Befassung mit der Videoüberwachungsanlage im Eingangsbereich eines Hochhauses berichtet. Er war dabei zu dem Ergebnis gekommen, dass diese Videoüberwachung zulässig und somit rechtmäßig erfolgt war, hatte aber auch betont, dass es sich dabei um eine Einzelfallentscheidung in einem besonderen Ausnahmefall gehandelt hat. Nachdem der Beschwerdeführer mit dieser Bewertung nicht einverstanden gewesen war und diesbezüglich beim Verwaltungsgericht Dresden Klage eingereicht hatte, ist darüber nunmehr im Berichtszeitraum entschieden worden.

Das Verwaltungsgericht hat sich im Rahmen seiner Entscheidung ausführlich mit den formellen und materiellen Anforderungen an die Prüfungstätigkeit der Aufsichtsbehörde befasst und dabei festgestellt, dass mir einerseits keine Ermessen-

fehler vorzuwerfen sind (vgl. dazu 6.3.2) und dass meine Behörde andererseits im Rahmen der in diesem Zusammenhang vorzunehmenden Interessenabwägung zu dem nicht zu beanstandenden Ergebnis gelangt ist, dass die betreffende Videoüberwachung in diesem Fall rechtmäßig ist.

Ungeachtet dieser für mich positiven Entscheidung habe ich im Berichtszeitraum meine Aufsichtstätigkeit in diesem konkreten Fall weitergeführt, denn bei einer Videoüberwachung im Wohnumfeld handelt es sich unbestritten um eine Kontrollmaßnahme mit großer Eingriffstiefe, die der regelmäßigen Evaluierung bedarf. Sind die ursprünglichen Voraussetzungen in dieser Form nicht mehr gegeben, kann dies durchaus dazu führen, dass die Videoüberwachung abzuändern oder teilweise bzw. auch komplett einzustellen ist. Ausgehend von der Rechenschaftspflicht des Art. 5 Abs. 2 Datenschutz-Grundverordnung (DSGVO), erfordert dies ein permanentes Monitoring der relevanten Vorkommnisse und Schadensfälle und eine Bewertung der Erheblichkeit dieser Ereignisse einschließlich einer diesbezüglichen Dokumentation.

Dabei reichen Übersichten über polizeiliche Anforderungen der Videoaufzeichnungen oder gebäudebezogene Aufstellungen von Versicherungsschäden keinesfalls aus, denn im Zuge der Eignungs-, Erforderlichkeits- und Verhältnismäßigkeitsprüfung sind vor allem auch Aussagen dazu zu treffen, ob mit den Videokameras überhaupt ein signifikanter Aufklärungsbeitrag geleistet werden kann und ob es sich tatsächlich um durch berechtigte Interessen des Verantwortlichen hinterlegte Vorkommnisse erheblicher Bedeutung, also nicht nur um Bagatellfälle, handelt. Vorkommnisse in den Etagenfluren oder im Kellerbereich sind daher – insbesondere in Wohngebäuden mit vielen Mietparteien – schon nicht geeignet, eine Videoüberwachung des Eingangsbereiches zu rechtfertigen. Auch bei (oftmals routinemäßig erfolgenden) polizeilichen Abfragen ist zu hinterfragen, wo sich die dort bearbeiteten Vorkommnisse zugetragen haben und welcher Art sie sind. Ereignisse lediglich im Umfeld des Gebäudes oder Delikte ohne unmittelbaren Bezug zum Verantwortlichen, etwa Körperverletzungsdelikte oder

Beleidigungen, sind für die Rechtfertigung einer Videoüberwachung des Eingangsbereiches irrelevant, selbst wenn sie im Einzelfall einen Beitrag zur Tataufklärung leisten könnten. Vermieter/innen sind keine Hilfspolizisten; die Strafverfolgung ist ausschließlich eine Aufgabe des Staates. Sich aus dem Mietvertrag ableitende rechtliche Verpflichtungen oder Obliegenheiten, die einen derartigen Schutz der Mieterinnen und Mieter zum Gegenstand haben, sind nicht ersichtlich.
Werden in erster Linie präventive Interessen verfolgt, kann dies schon keine Aufzeichnung rechtfertigen. In diesen Fällen sind Kameraattrappen völlig ausreichend.
Auch im Zuge bedeutsamer baulicher Änderungen, etwa Sanierungsmaßnahmen am Gebäude, insbesondere auch Änderungen der Wohnungszuschnitte und damit verbundener Änderungen beim Mietklientel, oder auch im gesamten Wohngebiet, ist eine Verifikation dahingehend notwendig, ob und in welchem Umfang die Voraussetzungen für eine Videoüberwachung weiterhin vorliegen.
Im konkreten Fall habe ich den Verantwortlichen mit Nachdruck auf seine diesbezüglichen Pflichten hingewiesen und eine Wiederholungsüberprüfung nicht ausgeschlossen.

Was ist zu beachten?
Im Zuge der sich aus der Datenschutz-Grundverordnung ergebenden Rechenschaftspflicht müssen Verantwortliche bei Videoüberwachungen regelmäßig prüfen, ob die Voraussetzungen für einen rechtmäßigen Betrieb noch gegeben sind.

2.2 Rechtmäßigkeitsvoraussetzungen der Datenverarbeitung

2.2.1 Anforderungen an eine Videoüberwachung von Eingangsbereichen in einer Gesundheitspraxis

↗ §§ 22, 33 KunstUrhG; Art. 6 Abs. 1, Art. 7, Art. 13 DSGVO

Ein kurioser Fall zeigte, dass der Betrieb einer Videokamera nicht immer ohne Risiken ist, gerade wenn der/die Betreiber/in bei der Installation und Inbetriebnahme nachlässig vorgeht. Sind die Kamera installiert und die Hersteller-App für das Smartphone heruntergeladen, dann steht der Inbetriebnahme nichts mehr im Weg – so denken viele. Doch ein unachtsamer Klick oder eine falsche Einstellung – und schon stellt die

Videokamera unbemerkt alle Bilder mitsamt Ton live ins Internet. Im Internetzeitalter bleiben solche Dinge im Regelfall nicht lange unbemerkt.

So war dies auch, als sich ein findiger Internetnutzer bei mir meldete. In einer sogenannten IoT-Suchmaschine (Internet-der-Dinge-Suchmaschine) wurde er darauf aufmerksam, dass eine in einer Physiotherapiepraxis angebrachte Videokamera Livebilder der ein- und ausgehenden Patientinnen und Patienten zeigte. Außerdem habe er über das aktivierte Mikrofon alle Gespräche mithören können. Zunächst sei nur der Eingangsbereich sichtbar gewesen. Nachdem er sich davon ausgehend an den Praxisinhaber gewandt und auf das „Sicherheitsproblem" aufmerksam gemacht hatte, habe dieser die Kamera kurzzeitig vom Netz genommen, nur um sie dann mit geändertem Blickwinkel abermals ins Internet zu stellen. Im Gegensatz zur vorherigen Ausrichtung waren aber nun auch der Wartebereich sowie ein Teil des Empfangstresens zu sehen. Der Internetnutzer belegte mir dies anhand mehrerer Bildschirmausdrucke. Dies nahm ich zum Anlass, mir den Fall genauer zu betrachten.

Zwar ergab der Aufruf der IoT-Suchmaschine, dass die Livebilder der Videokamera nicht mehr abrufbar waren. Jedoch stellte sich, ausgehend von den mir vorliegenden Bildschirmfotos, nach wie vor die Frage, ob denn die Videoüberwachung des Praxiseingangs rechtmäßig ist, auch wenn die Verbindung zum Internet zwischenzeitlich gekappt worden war. Deshalb bat ich den Praxisinhaber in einem ersten Schritt schriftlich um Auskunft. Nachdem dieser sich zunächst wenig kooperativ gezeigt hatte, suchte ich die Praxis schließlich bei einem Vor-Ort-Termin auf. Wie sich dabei herausstellte, waren die Livebilder inklusive Ton aufgrund einer falschen Konfiguration im Internet sichtbar gewesen.

Die Verbreitung nicht nur der Livebilder, sondern auch die Tonübertragung waren eindeutig ein Verstoß gegen Datenschutzvorschriften. Da jedoch zum Zeitpunkt meines Besuchs die Videokamera durch eine Änderung der Softwareeinstellungen nicht mehr mit dem Internet verbunden war, konzentrierte ich meine Prüfung darauf, wie sich die Situation der Video-

überwachung vor Ort genau darstellte. Denn was mit einmal ins Internet gestellten Videos passiert ist – völlig unabhängig davon, ob es sich um Livebilder und -ton oder die Wiedergabe von Aufzeichnungen handelte –, also beispielsweise welche Seitenbesucher/innen diese angeschaut haben, ob Bildschirmfotos oder gar Aufzeichnungen erstellt wurden, lässt sich im Nachhinein ohnehin nicht nachvollziehen.

Konkret hatte der Praxisinhaber nicht zuletzt wegen der Verbreitung der Livebilder im Internet bereits mit Ärgernissen zu tun. Denn der Internetnutzer, der sich mit seinem Hinweis an meine Behörde gewandt hatte, hatte wegen des Verdachts eines Verstoßes gegen § 33 in Verbindung mit § 22 Kunsturhebergesetz (KunstUrhG) auch einen Strafantrag gestellt. Diese Vorschriften regeln, dass es unter Strafe steht, Bilder ohne Einwilligung der abgebildeten Person zu verbreiten oder öffentlich zur Schau zu stellen. Allerdings kann nur die betroffene Person selbst einen Strafantrag stellen, da das Antragsrecht grundsätzlich höchstpersönlicher Natur und somit nicht auf andere übertragbar ist (§ 33 Abs. 2 KunstUrhG). Die Regelungen des KunstUrhG gelten im Übrigen auch nach Anwendbarkeit der Datenschutz-Grundverordnung unverändert fort.

Auf Befragen erklärte der Praxisinhaber die Videoüberwachung damit, dass er feststellen wolle, welche Personen die Praxis betreten. Hintergrund ist, dass gerade kleinere Praxen es sich nicht leisten können, einen ständig besetzten Empfang vorzuhalten, wie dies bei der Mehrzahl der niedergelassenen Ärztinnen und Ärzte noch der Fall ist. Deshalb kommen dort auch Videokameras zum Einsatz, mit denen sich auch aus den Behandlungsräumen schnell und einfach beobachten lässt, wer die Praxisräume betritt und ob der/die erwartete Patient/in schon eingetroffen ist.

Die datenschutzrechtliche Wertung der Videoüberwachung des Praxiseingangs vollzog sich nach Art. 6 Abs. 1 Buchst. f DSGVO. Dieser erlaubt die Videoüberwachung dann, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen erforderlich ist und die Interessen der betroffenen Personen nicht überwiegen.

Ein anzuerkennendes Interesse war dem Praxisinhaber nicht abzusprechen. Problematisch war hier allerdings, dass auch die Wartebereiche erfasst wurden. Die dortige Videoüberwachung hatte aber nichts mit dem eigentlichen Überwachungszweck, den Praxisinhaber über ein- und ausgehende Personen zu informieren, zu tun. Und auch die permanente Darstellung des Livebildes der Videokamera, in das auch im Behandlungszimmer befindliche Patienten bzw. Patientinnen Einblick nehmen konnten, brauchte es hierzu nicht. Dies hatte dementsprechend zur Folge, dass bereits aus diesem Grund die Videoüberwachung in der sich mir darstellenden Ausgestaltung mangels Erforderlichkeit unzulässig war.

Es hätte ausgereicht, die Videokamera nur in der Art einer Klingelkamera zu betreiben, also die Bilddarstellung mit der Betätigung der Türklingel oder dem Betreten der Praxisräume zu koppeln (automatische Aktivierung) und die Videokamera nach kurzer Zeit wieder zu deaktivieren. Stattdessen fand sich in dem mir bei der Vor-Ort-Kontrolle gezeigten Behandlungszimmer ein aufgeklapptes Notebook, welches permanent das Livebild der Videokamera darstellte. Hierüber konnte der Praxisinhaber jederzeit Einblick in den Eingangs- und Wartebereich nehmen. Er erklärte dies damit, dass er sich so nicht vom Patienten/von der Patientin abwenden und selbst zum Eingangs-/Empfangsbereich gehen müsse, um zu sehen, wer die Praxisräume betrete.

Auch die – aufgrund fehlender Erforderlichkeit bereits – nicht mehr notwendige Interessenabwägung hätte zum gleichen Ergebnis geführt. Das Interesse der wartenden Patienten/Patientinnen wog ungleich schwerer als die Belange des Praxisinhabers, zumal der Videokamera nicht anzusehen war, dass sie sich auch auf den Wartebereich bezog. Schließlich war noch zu berücksichtigen, dass, wer eine Gesundheitspraxis besucht, schlicht nicht mit einer dortigen Beobachtung rechnet.

Ich stellte gegenüber dem Praxisbetreiber unter Verweis auf das Urteil des Bundesverwaltungsgerichts vom 27. März 2019 (Az. 6 C 2.18, juris) infolgedessen unmissverständlich klar, dass die Überwachung von Wartebereichen datenschutzrechtlich nicht zulässig ist.

Was eine Videoüberwachung der Eingangsbereiche von Praxisräumlichkeiten anbelangt, sehe ich diese ähnlich wie eine Klingelkamera oder einen digitalen Türspion. Findet nur eine Übertragung des Livebildes statt und schaltet sich der Kamerabetreiber lediglich kurzzeitig auf die Videokamera auf, um damit die Person an der Praxistür oder beim Betreten der Praxisräume zu sichten, gibt es hiergegen nichts einzuwenden. Praxiszugänge werden üblicherweise schnell passiert, im Gegensatz zu Sitzbereichen, die gerade einem längeren Aufenthalt dienen, etwa zur Überbrückung von Wartezeiten.

Auch wenn der Praxisinhaber an der Eingangstür in Form eines Aufklebers mit Kamerasymbol und kurzem schriftlichem Hinweis auf die Videoüberwachung aufmerksam gemacht hatte, stellt das bloße Passieren eines Hinweises keine den datenschutzrechtlichen Vorschriften gerecht werdende Einwilligung in die Videoüberwachung dar; eine konkludente Einwilligung scheidet aus. Für einen legalen Kamerabetrieb muss vielmehr eine freiwillige und eindeutig bestätigende Handlung des/r Einwilligenden vorliegen, vgl. auch Erwägungsgrund 12 Satz 1. Ohnehin lässt sich eine Videoüberwachung bei einem unbestimmten oder wechselnden Personenkreis, wie bei einer Physiotherapiepraxis, allein aus praktischen Gründen nicht auf die Einwilligungslösung stützen. Art. 6 Abs. 1 Buchst. a in Verbindung mit Art. 7 DSGVO scheidet daher als Rechtsgrundlage aus.

Hinzu kam im dargestellten Fall, dass die verwendeten Hinweise auf die Videoüberwachung unvollständig waren, da Pflichtinformationen des Art. 13 DSGVO fehlten. Obgleich die Videokamera als solche gut sichtbar war, konnte der/die Patient/in daraus nicht auf den räumlichen Umfang der Videoüberwachung sowie die genaue Ausgestaltung des Kamerabetriebs (Livebeobachtung und/oder Videoaufzeichnung) schließen. Gerade auch hierzu dient der Zugang zu den Informationen des Art. 13 DSGVO, ohne deren Kenntnis außerdem eine Inanspruchnahme von Betroffenenrechten unverhältnismäßig erschwert oder gar unmöglich wäre.

Die in Art. 13 DSGVO genannten Informationen müssen „zum Zeitpunkt der Erhebung" vorliegen. Bei einer Videoüberwa-

Beispiel für ein vorgelagertes Hinweisschild nach Art. 13 DSGVO bei Videoüberwachung:
↗ sdb.de/vue06

Beispiel eines vollständigen Informationsblatts nach Art. 13 DSGVO bei Videoüberwachung:
↗ sdb.de/vue07

chung lässt sich dies nur dergestalt umsetzen, dass Hinweisschilder vor dem Betreten des Erfassungsbereichs angebracht werden.
Nur dann haben die betroffenen Personen die Möglichkeit, die Verarbeitungszwecke und die weiteren in Art. 13 DSGVO aufgeführten Informationen zu erfassen. Auf eine tatsächliche Kenntnisnahme kommt es indes nicht an.
Auf mein Zutun hin stellte der Praxisinhaber die Videokamera schlussendlich so ein, dass deren Blickwinkel wieder auf die Eingangstür gerichtet war. Alle anderen Bereiche wurden geschwärzt. Auch das Hinweisschild hat er in diesem Zuge an die gesetzlichen Vorgaben angepasst. Da in der Vergangenheit keine Aufzeichnungen erstellt wurden, dies auch künftig nicht beabsichtigt war und sich der Verantwortliche ab dem Zeitpunkt meines Kontrollbesuchs kooperativ zeigte, beließ ich es bei einer mündlichen Verwarnung, Art. 58 Abs. 2 Buchst. b DSGVO.

Was ist zu tun?
Eine Videokamera im Eingangsbereich einer Gesundheitspraxis darf nur kurzzeitig aktiviert werden, um festzustellen, wer die Praxisräume betritt. Im Bild befindliche Wartebereiche sind auszublenden. Weder ist eine Dauerbeobachtung zulässig, noch dürfen Videoaufzeichnungen erstellt werden. In jedem Fall sind die datenschutzrechtlichen Informationspflichten zu beachten und am Praxiszugang geeignete Hinweise anzubringen.

2.2.2 Zur Zulässigkeit der Überwachung öffentlich zugänglicher Räume zum Schutz vor Sachbeschädigungen

↗ Art. 6 Abs. 1 Buchst. f DSGVO; Art. 1 Abs. 1, Art. 2 Abs. 1, Art. 14 Abs. 1 GG

Auch nach Einführung der Datenschutz-Grundverordnung gilt weiterhin, dass es privaten Stellen grundsätzlich nicht zusteht, öffentliche Verkehrsräume zu beobachten oder in diesen Bereichen Videoaufzeichnungen anzufertigen. Unter öffentlichem Verkehrsraum sind alle Flächen zu verstehen, die der Allgemeinheit wegerechtlich oder tatsächlich zu Verkehrszwecken offenstehen bzw. gewidmet sind, unabhängig von bestehenden Eigentumsverhältnissen. Damit stellt sich die Frage, wie sich ein/e Grundstücksinhaber/in ansonsten gegen außerhalb des privaten Grundstücks agierende Täter/innen schützen kann, wenn diese etwa die Hauswand oder den um das Grundstück führenden Zaun besprühen oder andere Schäden am Grundeigentum anrichten.
Maßgeblich auch unter der seit 25. Mai 2018 anzuwendenden Datenschutz-Grundverordnung (DSGVO) ist noch immer

das Urteil des Bundesgerichtshofs vom 25. April 1995 (Az. VI Z 272/94), in dem sich dieses mit der Videoüberwachung öffentlicher Verkehrsbereiche befasst hat. Zwar hat diese Entscheidung eine privatrechtliche Klage auf Unterlassung von Bildaufzeichnungen mit einer Videokamera zum Gegenstand. Der Ausgangspunkt für die Videoüberwachung war aber mit der dargestellten Konstellation vergleichbar. Es ging darin um von einem öffentlichen Weg aus auf das Grundstück des Kamerabetreibers geworfenen Unrat, also gleichfalls um eine von außen auf das Betreibergrundstück erfolgte Einwirkung. Hiergegen wollte sich der Grundstückseigentümer mit einer gezielt auf ein Stück des öffentlichen Wegs gerichteten Videoüberwachung zur Wehr setzen – über längere Zeiträume und mit einer gewissen Regelmäßigkeit.

Somit hatte sich der Bundesgerichtshof auch mit der Frage zu befassen, welchen Voraussetzungen eine Videoüberwachung in öffentlichen Verkehrsbereichen unterliegt. Seine rechtliche Beurteilung basierte auf einer Güter- und Interessenabwägung unter Würdigung aller Umstände des Einzelfalls und Berücksichtigung aller (verfassungs-)rechtlich geschützten Positionen der beteiligten Parteien. Eine Abwägungsentscheidung ist auch nach der seit 25. Mai 2018 geltenden neuen Rechtslage zu treffen. Denn die datenschutzrechtliche Zulässigkeitsbeurteilung lässt sich einzig auf der Grundlage des Art. 6 Abs. 1 Buchst. f DSGVO vornehmen. Danach ist eine Verarbeitung (Videoüberwachung) dann erlaubt, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen erforderlich ist und die Interessen der betroffenen Personen nicht überwiegen.

Zwar hat ein/e Grundstückseigentümer/in das verfassungsrechtlich garantierte Recht (Art. 14 Abs. 1 Grundgesetz [GG]), geeignete Maßnahmen zum Schutz ihres/seines Grundeigentums zu ergreifen. Seine Grenze findet das Schutzrecht aber darin, wenn mit den ergriffenen Maßnahmen in unverhältnismäßiger Weise in hochrangige Rechtsgüter unbeteiligter Dritter eingriffen wird. Das vom Bundesverfassungsgericht anerkannte Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG) ist ein hochrangiges

Rechtsgut in diesem Sinne, welches einer Videoüberwachung des öffentlichen Verkehrsraums durch private Kamerabetreiber/innen grundsätzlich entgegensteht. Auch ungesehen gelöschte Videoaufzeichnungen ändern nichts daran, dass die Videoüberwachung unzulässig ist. Denn ansonsten läge es im Belieben des/der Kamerabetreiber/in, wie mit derart hergestellten Bild- und Videoaufzeichnungen verfahren wird. Eine dahingehende Kontrolle wäre den betroffenen Personen jedenfalls nicht möglich.

Nach den Wertungen des Bundesgerichtshofs ist es einzig bei Vorliegen einer notwehrähnlichen Situation denkbar, den videoüberwachten Bereich auch auf den öffentlichen Verkehrsraum auszudehnen. Denkbar wäre dies bei einer schwerwiegenden Beeinträchtigung des privaten Kamerabetreibers bzw. der privaten Kamerabetreiberin, etwa bei Angriffen auf ihre oder seine Person oder die unmittelbare häusliche Wohnsphäre, ohne dass andere zumutbare Abwehrmaßnahmen bestehen. Es handelt sich demgemäß um einen absoluten Ausnahmefall, der das Vorliegen spezieller Voraussetzungen notwendig macht. Die Gefahr einer Sachbeschädigung stellt aus Sicht des Bundesgerichtshofs allerdings keine schwerwiegende Beeinträchtigung dar. Damit gilt, dass auch bei von Dritten verursachten Sachschäden, die ihren Ursprung außerhalb des privaten Grundstücks haben, eine Videoüberwachung des öffentlichen Raums nicht möglich ist. Auch in diesem Fall hat die Videoüberwachung an der privaten Grundstücksgrenze zu enden.

Dementsprechend hat der Bundesgerichtshof den beklagten Grundstückseigentümer dazu verurteilt, die Videoüberwachung des öffentlichen Wegs zu unterlassen.

Es ist nicht nur ärgerlich, wenn fremde Personen Hauswände oder Zäune mit Graffiti besprühen, das vor dem eigenen Grundstück geparkte Kraftfahrzeug beschädigen, Zaunpfähle umknicken oder den Briefkasten in die Luft sprengen. Auch den daraus resultierenden finanziellen Schaden haben die Geschädigten nicht selten allein zu stemmen, wenn er nicht über eine Versicherung abgedeckt ist. Jedoch macht der Bundesgerichtshof als höchstes Zivilgericht in Deutschland unmissverständ-

lich klar, dass in derartigen Fällen eine Videoüberwachung des öffentlichen Verkehrsraums nicht zulässig ist. Aufgrund des Rechtsstaatsprinzips ist die Verwaltung an diese Entscheidung gebunden, sodass auch dann, wenn geschädigte Hauseigentümer/innen eine individuelle Härte geltend machen, keine davon abweichende rechtliche Bewertung möglich ist.

Ungeachtet dessen stelle ich regelmäßig fest, dass die Erwartungen der Kamerabetreiber/innen sich mit den landläufig eingesetzten Videokameras kaum erfüllen lassen. Obgleich Videokameras bei der Identifikation der Täter/innen helfen sollen, lässt eine Sichtung der Videoaufzeichnungen zumeist lediglich eine Rekonstruktion des Tathergangs zu. In den seltensten Fällen gelingt es auch, unerlaubt handelnde Personen zu ermitteln, da diese mit krimineller Absicht Aagierenden oft im Schutz der Dunkelheit und maskiert vorgehen. Damit steht bereits die grundsätzliche Eignung einer Videoüberwachung für Strafverfolgungszwecke in Zweifel. In Vergessenheit gerät außerdem, dass jedes frei zugängliche Grundstück potenziell gefährdet ist, also dort Straftaten wie Sachbeschädigungen oder Diebstahl auftreten können. Ließe man vor diesem Hintergrund eine Videoüberwachung öffentlichen Verkehrsraums zu, würde dies in der Endkonsequenz zu einer Komplettüberwachung in bebauten Gebieten führen.

Selbstverständlich steht das Datenschutzrecht nicht einer Videoüberwachung des eigenen selbstbewohnten Privatgrundstücks entgegen. Oftmals ist die Videoüberwachung auch fester Bestandteil einer (professionellen) Alarmanlage und ergänzt die weiteren Sicherheitskomponenten.

Was ist zu beachten?
Bei Sachschäden liegt keine notwehrähnliche Situation vor, die ausnahmsweise eine Überwachung öffentlicher Verkehrsbereiche rechtlich zuließe. Deshalb dürfen öffentliche Verkehrsbereiche auch zur Verfolgung von Straftaten (Sachbeschädigung), die das eigene Grundstück betreffen und von außerhalb ausgehen oder verübt werden, nicht überwacht werden.

2.2.3 Zur Einordnung optisch-elektronischer Datenverarbeitung – Kfz-Kennzeichenerfassungssysteme

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

Parkplätze und Parkhäuser hat der Handel in den letzten Jahren zunehmend mit Kennzeichenerfassungssystemen ausgestattet. Vereinzelt erhalte ich auch hierzu Beschwerden, da die Beschwerdeführer/innen unerlaubte Videoüber-

wachung vermuten, wie auch in einem Fall im Berichtszeitraum.

Die automatisierte Kennzeichenerfassung ist allerdings von einer herkömmlichen Videoüberwachung zu unterscheiden. Um eine „Beobachtung" betroffener Personen, wie bei der Videografie, handelt es sich aber eben nicht. Zwar kommen auch Kamerasysteme zum Einsatz, jedoch werden durch die Systeme nur einzelne Standbilder generiert, aus denen wiederum automatisiert die Kennzeichen ausgelesen werden. Die zertifizierten Verfahren erfassen die Fahrzeuginsassen regelmäßig nicht. Lediglich die (Roh-)Bildaufnahme, Kfz-Kennzeichen, Einfahrzeit mit Datum und Uhrzeit bzw. Parkbeginn sowie die Ausfahrzeit mit Datum und Uhrzeit werden bei der Ein- und Ausfahrt gespeichert. Beginnend mit der Erhebung der Informationen, werden personenbezogene Daten verarbeitet, da die Kfz-Kennzeichen als pseudonyme Information über den Halter und damit auch sämtliche weiteren damit verbundenen Informationen eine Personenbeziehbarkeit aufweisen, Art. 4 Nr. 1 Datenschutz-Grundverordnung (DSGVO).

Die Ausgabe und Abrechnung von Tickets wird bei dem Verfahren entbehrlich bzw. die Einhaltung von Höchstparkzeiten können durch das Verfahren automatisiert überwacht und unterstützt werden. Die Datenverarbeitung ist regelmäßig geeignet, auf eine vertragliche Grundlage, auch mittels allgemeiner Geschäftsbedingungen, gestützt zu werden, Art. 6 Abs. 1 Buchst. b DSGVO. So erhebe ich grundsätzlich gegen entsprechende Verfahren rechtlich keine Einwände, soweit auch eine den gesetzlichen Vorgaben entsprechende technische Umsetzung erfolgt ist, insbesondere nach Art. 5 Abs. 1 Buchst. e, 25 und 32 DSGVO.

Was ist zu beachten?
Kfz-Kennzeichenerfassungssysteme stellen in der Regel keine Videoüberwachungen dar. Verantwortlichen ist zu raten, eine suffiziente und transparente Information betroffener Personen mittels Beschilderung und Aushängen sicherzustellen.

Verantwortlichen bleibt allerdings zu raten, die Informationen gemäß Datenschutz-Grundverordnung bzw. eine Beschilderung über die Kennzeichenerfassung in einer für die betroffenen Personen inhaltlich strukturierten und örtlich wahrnehmbaren Art und Weise vorzunehmen, Art. 13 DSGVO. Die Verwendung von Videopiktogrammen erscheint mir nicht geeignet. Vereinzelt werden anschaulichere Piktogramme, die

von einer Bildkamera erfasste Kraftfahrzeuge mit Kfz-Kennzeichen darstellen, verwendet.
Den Beschwerdeführer informierte ich über das zum Einsatz gekommene Verfahren und meine rechtliche Einschätzung.

2.2.4 Datenübermittlung an das Jobcenter

↗ § 31, § 57 SGB II; § 67a SGB X; Art. 6 Abs. 1 Buchst. c DSGVO

Regelmäßig erhält meine Behörde Beschwerden oder Anfragen von Bewerberinnen und Bewerbern, ob Datenübermittlungen (potenzieller) Arbeitgeber/innen an das Jobcenter bzw. die Agentur für Arbeit zulässig sind.
Ich weise die betroffenen Personen dann darauf hin, dass die Agentur für Arbeit – im Falle einer Bewerbung auf ein Stellenangebot der Agentur für Arbeit – Daten über das Vermittlungsergebnis erheben darf, § 67a Abs. 2 Nr. 2 Buchst. b) aa) Zehntes Buch Sozialgesetzbuch (SGB X) in Verbindung mit § 31 Abs. 1 Nr. 2 SGB II.
Die Agentur für Arbeit hat gemäß § 31 Abs. 1 Nr. 2 SGB II auch die Aufgabe zu überprüfen, ob der/die Leistungsberechtigte durch sein/ihr Verhalten gegebenenfalls die Anbahnung eines Arbeitsverhältnisses – zum Beispiel durch unzureichende oder gar fehlende Bewerbungen oder sein/ihr Verhalten im Vorstellungsgespräch – verhindert und wofür die Agentur für Arbeit die Beweislast trägt. Dafür darf sie diese Daten auch bei den (potenziellen) Arbeitgebern bzw. Arbeitgeberinnen ohne Mitwirkung der Betroffenen erheben.
Die Rechtsgrundlage für die Auskunftserteilung und mithin für eine Datenübermittlung durch das Unternehmen, bei dem sich die/der Leistungsbezieher/in bewerben soll, an die Agentur für Arbeit ergibt sich wiederum aus § 57 SGB II. Der Umfang der Auskunftspflicht ist nach dem Wortlaut der Vorschrift weit gefasst. Der/Die Arbeitgeber/in muss der Agentur für Arbeit alle Tatsachen mitteilen, die für den Anspruch auf Leistungen nach dem SGB II erheblich sein können. Es ist dann Aufgabe des SGB-II-Trägers, die von dem/der Arbeitgeber/in mitgeteilten Tatsachen zu bewerten und im Hinblick auf das Leistungsbegehren des/der Hilfebedürftigen zu würdigen. Mitgeteilt

werden müssen vom Arbeitgeber bzw. von der Arbeitgeberin nur solche Tatsachen, die für den Leistungsanspruch erheblich sein können. Entscheidungserheblich sind solche Tatsachen, die Einfluss auf den Beginn, die Dauer oder die Höhe des Leistungsanspruchs haben können. Dazu gehören zum einen alle anspruchsbegründenden Tatsachen, zum anderen auch die Tatsachen nach § 31 SGB II, die zu einer Absenkung oder zum Wegfall des Anspruchs führen.

Was ist zu beachten?
Die Weitergabe vermittlungsbezogener Informationen von potenziellen Arbeitgebern/Arbeitgeberinnen an die Agentur für Arbeit zu konkreten Bewerbern/Bewerberinnen können auf Art. 6 Abs. 1 Buchst. c DSGVO gestützt werden.

Insoweit darf das betroffene Unternehmen nicht nur Angaben darüber machen, dass es zu keiner Einstellung gekommen ist, sondern auch zu den Gründen der fehlgeschlagenen Anstellung. Da es sich um eine gesetzliche Übermittlungsbefugnis im Sinne des Art. 6 Abs. 1 Buchst. c DSGVO handelt, kommt es weder auf ein Einverständnis noch auf einen Widerspruch gegen die Datenübermittlung an.

2.2.5 Einsichtnahme seitens der Beschäftigtenvertretung in Entgeltlisten

↗ § 79a Satz 2, § 80 Abs. 2 Satz 2 Halbsatz 2 BetrVG; Art. 6, Art. 21 Abs. 1 DSGVO

Wiederholt wurde meine Behörde seitens Arbeitgeberinnen/Arbeitgebern bzw. Dienstherrn um Rat gefragt, wie mit dem Widerspruch von Beschäftigten bzw. Bediensteten umzugehen sei, die einer Einsichtnahme durch die Beschäftigtenvertretung aufgrund ihrer besonderen Betroffenheit in Entgeltlisten (Bruttolohn- und Gehaltslisten) widersprechen würden, so auch im letzten Berichtszeitraum erneut. Fernmündlich wurde auf meine Nachfrage hin nachgeschoben, dass seitens der widersprechenden Beschäftigten in Anbetracht des Personenbezugs und der nicht anonym bereitzustellenden Listen auf Datenschutzgründe verwiesen und auch die Einhaltung der Geheimhaltung vonseiten des Betriebsrats in Zweifel gezogen werde. Letzteres blieb vage und konnte mir gegenüber nicht weiter konkretisiert werden.

Nach § 80 Abs. 2 Satz 2 Halbsatz 2 Betriebsverfassungsgesetz (BetrVG) ist der Betriebsrat bzw. genauer der Betriebsausschuss berechtigt, in die Bruttolohn- und Gehaltslisten

„Einblick zu nehmen". Mit Wirksamwerden der Datenschutz-Grundverordnung hat sich die Rechtslage nicht verändert, insbesondere stehen Datenschutz- und Persönlichkeitsrechte nicht entgegen, vgl. auch Landesarbeitsgericht Niedersachsen, Beschluss vom 22.10.2018 – 12 TaBV 23/18; vgl. zudem § 13 Abs. 2 Entgelttransparenzgesetz und den Beschluss des Bundesarbeitsgerichts vom 29. September 2020,1 ABR 32/19 wegen zu beachtender Einschränkungen bei der Gewährung der Einsichtnahme. Danach kann in der Praxis bei dargetaner Notwendigkeit zur Aufgabenwahrnehmung weiterhin Einblick genommen werden, allerdings ohne dass die Entgeltlisten der Beschäftigtenvertretung überlassen werden.

Im Sächsischen Personalvertretungsgesetz (SächsPersVG) findet sich keine § 80 Abs. 2 Satz 2 BetrVG vergleichbare enumerative Norm. Allerdings hatte das Bundesverwaltungsgericht zurückliegend schon die Rechtsfrage entschieden und dem Personalrat ein Recht zur Einsichtnahme im erforderlichen Umfang unter Bezugnahme auf die allgemeinen gesetzlichen Überwachungsaufgaben der Personalvertretung zugesprochen, Beschluss vom 16. Mai 2012, 6 PB 2.12. Die Entscheidung ist daher genauso in Bezug auf die sächsische personalvertretungsgesetzliche Lage einschlägig, vgl. § 73 SächsPersVG.

Zum besseren Verständnis und zur Einordnung der in Rede stehenden Datenweitergabe ist zu erinnern, dass Betriebsräte und Personalvertretungen nach Rechtsmeinung meiner Dienststelle als funktionale Stellen innerhalb des Verantwortlichen anzusehen sind und selbst keine eigenen Verantwortlichen darstellen, mithin keine Datenübermittlung an einen Dritten erfolgt, siehe dazu auch Tätigkeitsbericht 2019 (9.3, Seite 165 ff.).

Tätigkeitsbericht 2019:
↗ sdb.de/tb2103

Bei der letzten Änderung des Betriebsverfassungsgesetzes wurde nach zuletzt nicht einheitlicher Rechtsprechung seitens des Bundesgesetzgebers mit der Einfügung der Datenschutzvorschrift im Betriebsverfassungsgesetz klargestellt, dass der Betriebsrat bei der personenbezogenen Datenverarbeitung zur Erfüllung seiner gesetzmäßigen Aufgaben als

Teil des Verantwortlichen anzusehen ist, vgl. den Wortlaut von § 79a Satz 2 BetrVG, was die Sichtweise meiner Behörde nachträglich bestätigte. Zusätzlich ist, bezogen auf die bestehende Interessenlage in dem Ausgangsfall, auf die Geheimhaltungspflicht der Beschäftigtenvertretung hinzuweisen, § 79 BetrVG.

Nach alledem hat die Gewährung der Einsichtnahme bzw. Offenbarung der Entgeltlisten gegenüber Mitgliedern der Beschäftigtenvertretung gemäß § 26 Abs. 1 Bundesdatenschutzgesetz (BDSG) bzw. § 11 Abs. 1 Sächsisches Datenschutzdurchführungsgesetz (SächsDSDG) und im Einklang mit Art. 6 Datenschutz-Grundverordnung (DSGVO) im Arbeits- bzw. Dienstverhältnis unter Bezugnahme auf eine gesetzliche Pflicht hin zu erfolgen.

Ich habe dem anfragenden Unternehmen daher mitgeteilt, dass das Widerspruchsrecht des Art. 21 Abs. 1 DSGVO (tatbestandlich) nicht anwendbar, dass ein Widerspruchsrecht von Beschäftigten anderweitig gesetzlich nicht vorgesehen und der Informationsfluss trotz entgegenstehenden Willens betroffener Personen datenschutzrechtlich nicht zu beanstanden sei. Das Betriebsverfassungsgesetz enthält lediglich insoweit Ausnahmen, dass im Hinblick auf bestimmte Beschäftigte keine Arbeitnehmereigenschaft vorliegen soll, vgl. § 5 Abs. 2, 3 BetrVG.

Zuweilen mag es auch andere weitere Hintergründe geben, als die genannten, die dazu führen, dass Verantwortliche der Beschäftigten- bzw. Personalvertretung die dieser zustehenden Informationen nicht zur Kenntnis zu geben gewillt sind. Die Beachtung der gesetzlichen Rechte der Vertretungen jedenfalls entspricht dem Grundsatz des vertrauensvollen Zusammenwirkens zwischen Arbeitgeber und Betriebsrat im Sinne von § 2 Abs. 1 BetrVG; vgl. die Entsprechung im sächsischen Personalvertretungsrecht unter § 2 Abs. 1 SächsPersVG. Aufgrund nicht weiter substanziierter Verstöße gegen die Geheimhaltungspflicht des Betriebsrats bzw. bloßer darauf gerichteter Mutmaßungen sehe ich meine Behörde nicht gehalter, tätig zu werden.

Was ist zu beachten?
Die Mitbestimmungs- und Überwachungsrechte des Betriebs- und Personalrats bedingen einen Anspruch auf die erforderliche Einsichtnahme in die Entgeltlisten. Ein Widerspruchsrecht betroffener Personen, Beschäftigter oder Bediensteter, besteht nicht.

2.2.6 Dokumentation der Krankheitstage und Urlaubsansprüche zur Kenntnis aller Beschäftigten in einem Unternehmen

↗ § 1 BurlG, § 3 EntgFG, § 26 Abs. 3 Satz 1 BDSG, Art. 9 Abs. 1 DSGVO

Meine Behörde hatte den Hinweis erhalten, dass in einem Forschungsunternehmen die Krankheits- und Urlaubstage von allen Mitarbeiterinnen und Mitarbeitern – auch von ehemaligen Beschäftigten – in einer Excel-Datei erfasst werden; alle Beschäftigten haben Zugriff auf die Datei. In der Datei ausgewiesen wurde unter anderem, welche Beschäftigten wann und damit wie viele Tage selbst krank waren oder ob diese wegen der Erkrankung eines Kindes nicht anwesend waren. Dokumentiert wurde auch, welcher Mitarbeiter bzw. welche Mitarbeiterin wann Urlaub hatte und welcher Urlaubsanspruch ihm/ihr zusteht.

Bei der Erfassung von Krankheitstagen von Beschäftigten handelt es sich um eine Verarbeitung von Gesundheitsdaten im Sinne von Art. 4 Nr. 15 Datenschutz-Grundverordnung (DSGVO), welche gemäß Art. 9 Abs. 1 DSGVO untersagt ist, es sei denn, die Verarbeitung ist zur Erfüllung von rechtlichen Verpflichtungen aus dem Arbeitsrecht erforderlich, und es besteht kein Grund zu der Annahme, dass das schutzwürdige Interesse der betroffenen Personen an dem Ausschluss der Verarbeitung überwiegt (vgl. § 26 Abs. 3 Satz 1 Bundesdatenschutzgesetz). Die interne Erfassung von Krankheitstagen durch Personen, die mit Personalangelegenheiten betraut sind, halte ich mit Blick auf die sechswöchige Entgeltfortzahlungspflicht bei Krankheit durch einen Arbeitgeber bzw. eine Arbeitgeberin (vgl. § 3 Entgeltfortzahlungsgesetz) für rechtlich zulässig. Für eine Bekanntmachung im gesamten Kreis der Mitarbeiterinnen und Mitarbeiter habe ich aber kein Erfordernis gesehen.

Auch das Führen einer Urlaubsliste durch einen Arbeitgeber bzw. eine Arbeitgeberin halte ich grundsätzlich für praktikabel, um die Urlaubsansprüche gegenüber den Arbeitnehmerinnen und Arbeitnehmern gemäß § 1 Bundesurlaubsgesetz erfüllen zu können. Allerdings sehe ich auch hier kein Erfor-

dernis dafür, dass alle Beschäftigten Kenntnis darüber haben müssen, wer wie viel Urlaub beanspruchen kann.
Sofern der Sinn und Zweck der in einem Unternehmen geführten Datei darin besteht, für alle Mitarbeiter/innen die Information zu ermöglichen, welche Kollegin bzw. welcher Kollege anwesend bzw. abwesend ist, reicht es aus meiner Sicht aus, wenn allein dies in einer Datei erfasst wird. Auf meinen Hinweis hat mir das betroffene Unternehmen mitgeteilt, dass es die bei ihm geführte Datei entsprechend angepasst hat.

Was ist zu tun?
An- und Abwesenheitslisten in einem Unternehmen, die allen Beschäftigten zugänglich sein sollen, sollen auch nur zur An- und Abwesenheit eine Aussage treffen, nicht aber zu den Gründen einer Abwesenheit.

2.2.7 Verarbeitung privater Kontaktdaten (E-Mail-Adressen und Telefonnummern) von Beschäftigten durch Dienstherren bzw. Arbeitgeber/innen

↗ § 26 Abs. 2 BDSG; Art. 5, 7 DSGVO

Regelmäßig erhält meine Behörde Beschwerden und Anfragen von Beschäftigten, Beamtinnen und Beamten (im Folgenden als „Beschäftigte" bezeichnet), ob der/die Arbeitgeber/in bzw. der Dienstherr ihre privaten Kontaktdaten, wie zum Beispiel die E-Mail-Adresse oder die Telefonnummer, erfragen darf bzw. ob sie verpflichtet sind, diese dem Dienstherrn, dem/der Arbeitgeber/in, den Verantwortlichen, mitzuteilen.
Als Zweck der Datenverarbeitung wird seitens der Verantwortlichen zum Beispiel angeführt, dass mit der Datenverarbeitung eine kurzfristige Erreichbarkeit im Falle von Dienstplanänderungen oder im Vertretungsfall gewährleistet werden soll. Teilweise wird als Zweck die Sicherstellung der Kommunikation mit dem Personal, soweit auf dienstliche Kommunikationsmittel nicht zurückgegriffen werden kann, angegeben. Aber auch die Führung von sogenannten „Alarmlisten", in welchen die privaten Kontaktdaten der betroffenen Personen vorgehalten werden sollen, wird von Verantwortlichen als Verarbeitungszweck angegeben. Auch diese sollen der Erreichbarkeit durch den Verantwortlichen und damit der (kurzfristigen/ungeplanten) Dienst- und Beschäftigungsaufnahme dienen.
Die Verarbeitung von privaten Telefonnummern oder E-Mail-Adressen im Rahmen des Dienst- und Beschäftigungsver-

hältnisses durch den Dienstherrn und den/die Arbeitgeber/in ist nach meiner Auffassung grundsätzlich unzulässig, da es regelmäßig an der Erforderlichkeit fehlt. Dies ist allerdings im Einzelfall zu prüfen.

Im Rahmen von Beschäftigungs- und Dienstverhältnissen – sowohl im öffentlichen als auch nichtöffentlichen Bereich – wird regelmäßig von verschiedenen Arbeitszeitmodellen, insbesondere aber auch Rufbereitschaft/Bereitschaftsdienst, Gebrauch gemacht. Inwieweit neben diesen flexiblen Modellen zur Arbeitszeitgestaltung zusätzlich noch ein Erfordernis besteht, weitere Beschäftigte während ihrer Freizeit telefonisch erreichen zu können, um diese kurzfristig dienstlich einzusetzen, erschließt sich nicht. Im Hinblick auf den Umfang der Datenverarbeitung ist eine Erforderlichkeit zumeist ebenfalls nicht gegeben. Häufig wird die Abfrage der privaten Kontaktdaten durch die Arbeitgeber/innen nicht auf einzelne Führungskräfte beschränkt, sondern betrifft sämtliche Beschäftigte. In diesem Zusammenhang wäre auch die Bereitstellung von Diensthandys durch Dienstherrn und den/die Arbeitgeber/innen zu thematisieren, da ohne Weiteres und mangels einer individuellen individual oder kollektivrechtlichen Vereinbarung bzw. einer Rufbereitschaft nicht von einer dienstrechtlichen bzw. arbeitsvertraglichen (Neben-) Pflicht zur Vorhaltung eines Telefons durch Beschäftigte ausgegangen werden kann.

Auch eine Einwilligung als Rechtsgrundlage der Datenverarbeitung kann regelmäßig nicht in Betracht kommen, da diese, wie Art. 7 Abs. 4 Datenschutz-Grundverordnung (DSGVO) zeigt, ebenso eine Erforderlichkeit voraussetzt und von einer Freiwilligkeit regelmäßig nicht ausgegangen werden kann. 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. Ein hoher Konformitätsdruck mag hinzukommen. Anders wäre es ausnahmsweise, wenn die Beschäftigten eine echte oder freie Wahl hätten und in der Lage wären, die Einwilli-

gung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden (siehe Erwägungsgrund 42 der DSGVO). Bei einem klaren Ungleichgewicht soll die Einwilligung nicht in allen Fällen eine gültige Rechtsgrundlage liefern (Erwägungsgrund 43 der DSGVO). Ein klares Ungleichgewicht liegt aufgrund der strukturellen Unterlegenheit der Beschäftigten in einem Dienst- beziehungsweise Arbeitsverhältnis typischerweise vor. Hierzu wäre vom Verantwortlichen darzulegen, welchen Vorteil die/der Beschäftigte erlangt oder welche gleichgelagerten Interessen der Dienstherr und die/der Beschäftigte verfolgen. So genügt zum Beispiel die generelle Aussage, dass mit dieser Datenverarbeitung die Funktionsfähigkeit der Verwaltung gewährleistet wird oder auf die Möglichkeit einer mit der Corona-Pandemie vergleichbaren Ausnahmesituation Bezug genommen wird, diesen Anforderungen nicht.

In der Anwendungshilfe der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Stand: 20. Dezember 2021) „Häufige Fragestellungen nebst Antworten zur Verarbeitung von Beschäftigtendaten im Zusammenhang mit der Corona-Pandemie" wird unter Ziffer 3, auf Seite 4 und 5 ausgeführt, dass im Rahmen einer Einwilligung die privaten Erreichbarkeitsdaten der Beschäftigten verarbeitet werden dürfen, um im Falle einer Infektion eines oder einer Beschäftigten an dessen oder deren Kontaktpersonen heranzutreten und Letztere über die Risikobegegnung zu unterrichten. In diesem Fall wird angenommen, dass ausnahmsweise eine Freiwilligkeit der Einwilligung angenommen werden könne, da die Nutzung der privaten Kontaktdaten der Pandemiebekämpfung diene, welche sowohl die Interessen des Arbeitgebers bzw. der Arbeitgeberin als auch der Beschäftigten verfolgt, vgl. § 26 Absatz 2 Satz 2 BDSG. Allerdings wird in diesem Zusammenhang ausdrücklich darauf hingewiesen, dass die privaten Kontaktdaten nur zweckgebunden – das bedeutet nur für die Pandemiebekämpfung – verarbeitet werden dürfen. Ein pauschaler Verweis auf die vergangene Pandemiesituation genügt daher den Anforderungen an die Zweckbindung nach Art. 5 Abs. 1 Buchst. c DSGVO nicht.

Was ist zu tun?
Dienstherren oder Arbeitgeber/innen, die zur Erhaltung der Betriebsfähigkeit die Erreichbarkeit der Beschäftigten außerhalb von Dienst- und Arbeitszeiten zu verbessern beabsichtigen, ist zu raten, zur Vermeidung der Verarbeitung nicht erforderlicher Daten, dienstliche Endgeräte oder Rufnummern zur Verfügung zu stellen.

2.2.8 „Pre-Employment-Screening" – Recherchen zu Bewerberinnen und Bewerbern im Internet und in sozialen Netzwerken

↗ § 11 SachsDSDG; § 26 BDSG; Art. 5 Abs. 1 Buchst. c, Art. 6, Art. 7 Abs. 4, Art. 14 DSGVO

Die Personalauswahl ist für nichtöffentliche und öffentliche Stellen ein anspruchsvolles Feld. Es gilt, die geeignetsten unter den potenziellen Beschäftigten und Bediensteten zu erkennen, Nachweise einzuordnen und sich teuer und belastend auswirkende Fehlgriffe bei Einstellungsentscheidungen zu vermeiden. Arbeitgeber/innen und Dienstherren sind daher in Anbetracht der verfügbaren medialen Informationsquellen durchaus versucht, bei Auswahlprozessen mittels Suchmaschinen und sozialer Netzwerke so viel wie möglich über Bewerberinnen und Bewerber in Erfahrung zu bringen.

So wird meine Dienststelle auch mit der Zulässigkeit von „Background-Checks" konfrontiert. Zumeist handelt es sich um spezifische Anfragen. Im letzten Berichtszeitraum war ich aber auch mit einem Gesetzentwurf der Staatsregierung befasst, der die Befugnis einer nicht weiter eingeschränkten Internetrecherche zu Bewerberinnen und Bewerbern im Polizeibereich vorsah. Im Kern der Überlegungen stützten sich die Verfasser des Entwurfs auf den sicherheitsrelevanten Aufgabenbereich, dessen Bedeutung, die Erwartung gegenüber Bewerberinnen und Bewerbern für ein öffentlich-rechtliches Dienstverhältnis und eine wahrzunehmende Verantwortung gegenüber der Öffentlichkeit, was schlicht zu einfach und zu kurz gedacht ist.

Weder für ein Arbeitsverhältnis noch für ein öffentlich-rechtliches Dienstverhältnis rechtfertigt der Auswahlprozess eine uneingeschränkte Verarbeitung von im Internet zugänglichen Informationen zu Bewerberinnen und Bewerbern. Auch diese sind personenbezogene Daten, die automatisiert durch den Verantwortlichen verarbeitet werden, Art. 4 Nr. 1 DSGVO.

Allgemein gilt, dass eine Einwilligung in eine weitergehende Recherche mangels nicht bestehender Freiwilligkeit wegen

eines bestehenden Ungleichgewichts unwirksam sein sollte, vgl. Art. 7 Abs. 4 Datenschutz-Grundverordnung (DSGVO), § 26 Abs. 2 Bundesdatenschutzgesetz (BDSG) und auch Erwägungsgrund 43 Satz 1 der Verordnung im Kontext der Beteiligung öffentlicher Stellen.

Arbeitsrechtlich sind Arbeitgeberinnen und Arbeitgebern bereits Schranken gesetzt. Informationen, die noch vom Fragerecht umfasst sind, könnten erhoben werden, nicht jedoch darüber hinausgehende Angaben, auch nicht solche, die über allgemein zugängliche Internet-Informationsquellen im Zuge einer Eigenrecherche erworben wurden. Umgekehrt könnten noch von den Betroffenen zur beruflichen Selbstdarstellung eingerichtete Netzwerkpräsenzen bzw. ihre eigenen Internetseiten, auf die sie Verantwortliche entsprechend hinweisen, in eine Betrachtung eingehen. Ein schutzwürdiges Interesse der Bewerberinnen und Bewerber sollte dabei regelmäßig zu verneinen sein. Weitergehende Recherchen in sozialen Netzwerken, die nicht der beruflichen Darstellung dienen, sondern zumeist freizeitlich genutzt werden, gehen über das Fragerecht hinaus und sind unzulässig, Implikationen in Bezug auf Tatbestände des Allgemeinen Gleichbehandlungsgesetzes (AGG) lassen sich nicht ausschließen.

Datenschutzrechtlich besteht nach der Datenschutz-Grundverordnung kein Direkterhebungsgrundsatz mehr, wie bei der nationalen Rechtsetzung BDSG alte Fassung, Sächsisches Datenschutzgesetz (SächsDSG), aber die Geeignetheit und Erforderlichkeit bzw. Datenminimierung gemäß Art. 5 Abs. 1 Buchst. c DSGVO werden verlangt, vgl. auch Art. 6 Abs. 1 DSGVO, § 26 Abs. 1 BDSG sowie § 11 Abs. 1 SächsDSDG, die die Erforderlichkeit tatbestandlich voraussetzen. Die vorgenannten, die Datenschutz-Grundverordnung ergänzenden Vorschriften gelten ausdrücklich auch für Bewerberinnen und Bewerber.

Schon an der Geeignetheit sollte es für die meisten anzubahnenden Rechtsverhältnisse mangeln, sind die Internet-Informationen doch nicht selten invalide, überschießend, beziehen sie sich auf private Verhältnisse, die für das Arbeits- oder Dienstverhältnis keine Rolle spielen. Hinzu kommt ein die

Gleichmäßigkeit der Datenverarbeitung beeinträchtigender tatsächlicher Umstand. Zu Bewerberinnen und Bewerbern lassen sich aufgrund der Namenshäufigkeit sowie der sich unterscheidenden Präsenz nur uneinheitlich, unsicher und ungleichmäßig Informationen zusammentragen.

Zu verneinen ist die Erforderlichkeit im Hinblick auf eine uneingeschränkte Ausforschung der betroffenen Personen im Internet aufgrund der vielfältigen weiteren Optionen der Informationsgewinnung (Nachfragemöglichkeiten, Nachweisdokumente, Vorstellungsgespräche, Assessment-Center), der nicht zweckorientierten Sachfremdheit bezogener Inhalte, der überschießenden Informationen, des Verstoßes gegen das Gebot der Datenminimierung im Sinne von Art. 5 Abs. 1 Buchst. c DSGVO, der Unverhältnismäßigkeit im Hinblick auf Umfang, Tiefe und Ausmaß der Datenverarbeitung regelmäßig und auch, was den dargestellten Vorstoß der Staatsregierung im Kontext mit Polizeiberwerberinnen und -bewerbern anbelangt. Soweit dennoch, ob zulässig oder unzulässig, nicht direkt bei Bewerberinnen und Bewerbern, sondern im Internet personenbezogene Informationen zusammengetragen werden sollen, greifen die weitergehenden Informationspflichten des Art. 14 DSGVO. Nichtöffentliche Stellen haben zudem ihr berechtigtes Interesse inhaltlich darzutun, Art. 14 Abs. 2 Buchst. b DSGVO. Wegen Art. 15 Abs. 3 DSGVO ist die automatisierte Verarbeitung seitens des Verantwortlichen zu dokumentieren, Suchfolgen und -schema sowie Suchergebnisse zu den Recherchen sind revisionsfähig bereitzuhalten. Ansonsten gilt Art. 13 DSGVO.

Seitens meiner Behörde erging eine entsprechende Stellungnahme zum Gesetzentwurf der Staatsregierung im Zusammenhang mit dem Unterfangen, die Ausforschung von Bewerberinnen und Bewerbern bei Sicherheitsbehörden mittels uneingeschränkter Internetrecherche gesetzlich zu legitimieren, vgl. Art. 3, § 4 Satz 3 Sächsisches Gesetz zur Regelung polizeilicher Zuverlässigkeitsüberprüfungen (SächsPolZÜG), LT-Drs. 7/13905. Ein mit vorgenannter Vorschrift zur Datenauswertung verbundener legitimer gesetzgeberischer Zweck hat dem verfassungsrechtlichen Grundsatz der Verhältnis-

Was ist zu tun?
Die Erforderlichkeit der Durchführung von Background-Checks sowie deren Umfang, Tiefe und Ausmaß ist im Hinblick auf Erforderlichkeit und Datenminimierung zu hinterfragen. Verantwortlichen stehen Nachweisdokumente, Vorstellungsgespräche und Assessment-Center um Personalentscheidungen zu treffen.
Arbeitgeberinnen, Arbeitgebern und Dienstherrn ist zu raten, Erkundigungen zu betroffenen Bewerberinnen und Bewerbern von diesen direkt einzuholen bzw. mit deren Wissen vorzunehmen. Tun sie dies nicht, hat das zur Konsequenz, dass sie ihre Recherchen zu dokumentieren und der weitreichenden Informationspflicht aus Art. 14 DSGVO nachzukommen haben.

mäßigkeit zu genügen. Die mittels Gesetzentwurf eröffnete informationstechnisch unterstützte ungeregelte Erlangung und Sammlung – in Bezug auf Bewerberinnen und Bewerber – nicht valider (geeigneter) und nicht erforderlicher grundrechtsrelevanter Informationen aus dem privaten Kommunikationsbereich konstituiert ein erhebliches Eingriffsgewicht in das Grundrecht auf informationelle Selbstbestimmung. In Anbetracht der übrigen Überprüfungsbefugnisse rechtfertigt das meiner Überzeugung nach nur noch als gering zu bemessende Risiko des Nichterkennens von Gefahrenverdachtsfällen die angesonnene Befugnis zur Internetdatenauswertung und -analyse nicht. Das Gesetzgebungsverfahren ist zum Ende des Berichtszeitraums noch nicht abgeschlossen gewesen. Es bleibt zu hoffen, dass die Staatsregierung noch erkennt, dass ihr Gesetzesvorhaben in dieser Frage nicht europarechtskonform, verfassungs- und gerichtsfest sein kann.

2.2.9 Übermittlung von Adressdaten des Arbeitgebers wegen Lohnpfändung

↗ AO, SächsVwVG, SGB X

Ein Unternehmer, der eine Pfändungs- und Einziehungsverfügung (§ 15 SächsVwVG in Verbindung mit §§ 309 ff. Abgabenordnung) erhalten hatte, wandte sich an mich. Ausweislich des ihm zugegangenen Schreibens einer sächsischen Kommune schuldete ein Mitarbeiter des Unternehmers der betreffenden Stadt eine öffentlich-rechtliche Forderung, zu deren Begleichung nun Lohnforderungen des Mitarbeiters gegen den Unternehmer als sogenannter Drittschuldner gepfändet werden sollten. Der Arbeitgeber brachte dabei in Erfahrung, dass die Kommune seine Adressdaten bei der Rentenversicherung erfragt hatte, und bat mich um Klärung, ob dies denn rechtens sei.
Bei der Rentenversicherung handelt es sich um einen Sozialleistungsträger, sodass die Vorschriften nach dem SGB beachtet werden müssen.
Zur Durchsetzung von öffentlich-rechtlichen Ansprüchen dürfen indes nach § 74 a SGB X im Einzelfall auf Ersuchen

Name, Vorname, Geburtsdatum, Geburtsort, derzeitige Anschrift der betroffenen Person, ihr derzeitiger oder zukünftiger Aufenthaltsort sowie Namen, Vornamen oder Firma und Anschriften ihrer derzeitigen Arbeitgeber übermittelt werden, soweit kein Grund zu der Annahme besteht, dass dadurch schutzwürdige Interessen der betroffenen Person beeinträchtigt werden, und wenn das Ersuchen nicht länger als sechs Monate zurückliegt. Die ersuchte Stelle ist über § 4 Absatz 3 hinaus zur Übermittlung auch dann nicht verpflichtet, wenn sich die ersuchende Stelle die Angaben auf andere Weise beschaffen kann. Satz 2 findet keine Anwendung, wenn das Amtshilfeersuchen zur Durchführung einer Vollstreckung nach § 66 erforderlich ist.

§ 74 a Abs. 1 SGB X lässt die Übermittlung von Sozialdaten zur Durchsetzung von öffentlich-rechtlichen Ansprüchen also zu. Der Empfängerkreis der zu übermittelnden Sozialdaten ist hier nicht eingeschränkt; es kommt allein darauf an, dass öffentlich-rechtliche Ansprüche durchgesetzt werden sollen. § 74 a Abs. 1 SGB X enthält – anders als Absatz 2 der Vorschrift – keine benannten Adressaten, das heißt, er begrenzt die Datenübermittlung nicht durch Aufzählung von Datenempfängern, sondern allein durch die Art der Forderung. Öffentlich-rechtlich sind solche Ansprüche, die sich aus dem Verhältnis zwischen Bürger/in und Staat ergeben. Eine öffentlich-rechtliche Geldforderung muss ihre Rechtsgrundlage im öffentlichen Recht haben, zum Beispiel Steuern, Beiträge, Gebühren, Gemeindeabgaben. Dies war vorliegend offensichtlich der Fall.

Einen datenschutzrechtlichen Verstoß konnte ich mithin nicht erkennen und habe dies dem betroffenen Arbeitgeber so mitgeteilt. Eine Reaktion hierauf erfolgte nicht.

Was ist zu tun?
Bei der Lohnpfändung eines Arbeitnehmers dürfen Adressdaten seines Arbeitgebers unter den Voraussetzungen des § 74 a SGB X durch den Rentenversicherungsträger weitergegeben werden.

2.2.10 Angemessenheit der Überprüfung der Zahlungsfähigkeit – Selbstauskünfte von Vereinsmitgliedern

↗ § 26 BGB; Art. 6 Abs. 1 Buchst. b, Art. 58 Abs. 1 Buchst. d DSGVO

Der Vorsitzende eines Kleingartenvereins wandte sich mit einer Beratungsanfrage an mich. Es gab Gerüchte, dass bei

einem der Interessenten für einen Pachtgarten Schulden aus einem anderen Pachtverhältnis bestehen. Den mutmaßlich geschädigten Verein kannte er nicht, sondern nur eine „ungefähre Richtung". Dies reichte ihm aus, um drei andere Kleingartenvereine, auf die die vage Standortbeschreibung zutraf, mit dem Sachverhalt zu konfrontieren.
Enttäuscht darüber, dass keiner der angeschriebenen Vereine antwortete, stellte er sich die Frage, ob es wohl daran läge, dass seine Anfrage datenschutzrechtlich bedenklich sei. Weiter trieb ihn die Frage um, wie sich ein Kleingartenverein vor (finanziellen) Schäden durch insolvente oder säumige Unterpächter/innen schützen kann. Er sah eine Parallele bei von Wohnungssuchenden zumeist verlangten Selbstauskünften. Ausgehend davon wollte er von meiner Behörde wissen, welche Selbstauskünfte generell datenschutzkonform sind.

Abfrage bei anderen Kleingartenvereinen

Dem Vereinsvorsitzenden war offensichtlich nicht bewusst, dass seine Erkundigung bei den anderen Vereinen unter Nennung des Namens des Unterpächters sowie dessen potenzieller Schulden personenbezogene Daten im Sinne von Art. 4 Nr. 1 Datenschutz-Grundverordnung (DSGVO) enthielt, er also selbst eine Verarbeitung personenbezogener Daten vornahm, Art. 4 Nr. 2 DSGVO. Allerdings konnte ich hierfür keine datenschutzrechtliche Grundlage – eine abschließende Auflistung an Rechtsgründen ist in Art. 6 Abs. 1 DSGVO enthalten – ausmachen, welche dieses Vorgehen gerechtfertigt hätte.
Bei der Pacht einer Kleingartenparzelle wird ein Unterpachtvertrag zwischen der/dem Parzelleninhaber/in (Unterpächter/in) und dem Regionalverband als Pächter geschlossen. Der Kleingartenverein agiert dabei als Stellvertreter und treuhänderisch für den zuständigen Regionalverband. Auch der Mitgliedschaft in einem Kleingartenverein liegt ein zivilrechtliches vertragsähnliches Verhältnis zugrunde, der mit dem Vereinsbeitritt zustande kommt. Damit sind im Regelfall alle erforderlichen Verarbeitungen, die sich innerhalb dieser privatrechtlichen Verträge vollziehen, von der Erforderlichkeit zur Vertragserfüllung gedeckt, Art. 6 Abs. 1 Buchst. b DSGVO.

Die Geltung der Vorschrift reicht dabei von der Vertragsanbahnung über die Durchführung bis zur Abwicklung eines Vertragsverhältnisses.

Allerdings bewegte sich der Vereinsvorsitzende mit der Weitergabe der das individuelle Pacht- oder Mitgliedschaftsverhältnis – dies war der Anfrage des Vereinsvorsitzenden nicht unmittelbar zu entnehmen – betreffenden Informationen außerhalb des von der Vorschrift gedeckten Verarbeitungszwecks, wobei die in Rede stehenden Schulden auf bloßen Gerüchten basierten. Weder für die Abwicklung des Unterpachtnoch zur Durchführung des Mitgliedschaftsverhältnisses im Verein war es notwendig, gegenüber anderen Kleingartenvereinen die das Innenverhältnis Unterpächter zu Kleingartenverein und Regionalverband betreffenden Sachverhalte offenzulegen. Es wäre aus Sicht des betroffenen Kleingartenvereins angemessener und zielführender gewesen, sich stattdessen direkt fragend an den zuständigen Regionalverband zu wenden. Hiergegen wäre auch datenschutzrechtlich nichts einzuwenden gewesen, nachdem der Kleingartenverein insoweit treuhänderisch für den Dachverband tätig ist.

Letzten Endes wies mich der Vereinsvorsitzende also selbst auf einen möglichen von ihm begangenen und dem Verein zuzurechnenden Datenschutzverstoß, vgl. § 26 Bürgerliches Gesetzbuch, hin. In diesem Fall verzichtete ich ausnahmsweise auf eine weitergehende Erforschung des Sachverhalts, sondern beließ es bei einem schlichten Hinweis (Art. 58 Abs. 1 Buchst. d DSGVO).

Selbstauskünfte

Der von dem Vereinsvorsitzenden angestellte Vergleich mit Selbstauskünften bei Wohnraummietverträgen scheiterte aus mehreren Gründen. Zunächst ist die Höhe eines finanziellen Schadens im Fall eines Zahlungsausfalls respektive bei Mietschulden in einem (Wohnungs-)Mietverhältnis ungleich höher als bei ausstehenden Pachtzinszahlungen oder Vereinsbeiträgen. Ungeachtet dessen liegt der potenzielle finanzielle Schaden, insbesondere in Anbetracht der möglichen Dauer einer Räumungsklage wegen Mietschulden, im Wohnmietbereich

deutlich höher. Nicht zuletzt ist eine Selbstauskunft angesichts der geringen Höhe des Streitwertes (Pachtzins/Vereinsbeitrag) schlicht unverhältnismäßig.

Nicht zu vergessen ist auch, dass es der Kleingartenverein selbst in der Hand hat, im Vorfeld bzw. zu Beginn des Unterpachtverhältnisses von dem/r (potenziellen) Vertragspartner/in eine Kaution oder Vorauszahlung auf den Pachtzins zu verlangen. Steht die Zahlung des Pachtzinses aus, greifen zudem die bürgerlich-rechtlichen Vorschriften, die bis zu einer Kündigung des Unterpachtvertrags reichen können. Fernerhin hat der Kleingartenverein die Möglichkeit, Interessierte bei Bedenken bezüglich der Zahlungsfähigkeit jederzeit abzulehnen. Trotz aller Vorsicht und entsprechender Vorkehrungen ist es allerdings nicht ausgeschlossen, dass es auch bei laufenden Pachtverhältnissen zu finanziellen Schwierigkeiten bis zur Zahlungsunfähigkeit eines Unterpächters kommt, beispielsweise im Fall einer Privatinsolvenz.

Somit steht jedem Kleingartenverein ein Bündel an Möglichkeiten zur Verfügung, um bei Zweifeln an der Zahlungsfähigkeit von Interessierten das finanzielle Risiko zu minimieren oder gänzlich abzuwenden.

Was ist zu beachten?
Hat ein Kleingartenverein den Verdacht, dass ein/e Interessent/in für eine Parzelle bei anderen Vereinen Schulden angehäuft hat, darf er sich nicht einfach dort hierüber erkundigen. Im Regelfall ist der zuständige Dachverband über säumige Zahler/innen informiert. Selbstauskünfte wie im Wohnmietbereich hingegen sind unzulässig. Für den Verein bestehen andere Möglichkeiten, sein finanzielles Risiko zu minimieren.

2.2.11 Bezug von Kfz-Halterdaten zur Geltendmachung von Vertragsstrafen bei nicht bestimmungsgemäßer Parkraumnutzung

↗ § 39 Abs. 1 StVG, Art. 6 Abs. 1 Buchst. b DSGVO

Eines Tages stellt man fest, dass sich unter den eingegangenen Postsendungen der Brief eines unbekannten Unternehmens befindet. Nach dem Öffnen wird schnell klar, dass der Umschlag eine Zahlungsaufforderung enthält. Diese soll im Zusammenhang mit einem Parkvorgang stehen und beinhaltet eine Vertragsstrafe. Neben Ort und Uhrzeit des Verstoßes enthält das Schreiben außerdem das eigene Kfz-Kennzeichen. Hat sich der erste Schreck gelegt, taucht unweigerlich die Frage auf, wer das unbekannte Unternehmen ist und wie dieses überhaupt an die Halterdaten gelangt ist.

Genauso erging es offensichtlich dem Kunden eines Supermarktplatzes, was dieser zum Anlass nahm, sich bei meiner Behörde nach der Rechtslage zu erkundigen und eine Datenschutzbeschwerde zu erheben.

Grundstücke der Supermärkte befinden sich in Privateigentum. Eigentümer/innen können ihre Kundenparkplätze kostenfrei, kostenpflichtig anbieten bzw. die Parkordnung selbst festlegen. Dem geschilderten Lebenssachverhalt liegt zugrunde, dass mehr und mehr Einzelhändler/innen dazu übergehen, die Nutzung ihrer Parkflächen und deren Dauer von privaten Unternehmen überwachen zu lassen, um diese von fremdparkenden Fahrzeugen (Parkraumbewirtschaftung) frei zu halten. Dabei haben die Eigentümer/innen die Möglichkeit, das Grundstück zu verpachten bzw. die Ansprüche aus der Bewirtschaftung abzutreten, sodass der/die Pächter/in Ansprüche hieraus geltend machen kann. Auch diese können ihre Nutzungsregeln für den Supermarkt-Parkplatz selbst festlegen. Park- bzw. Nutzungsbedingungen müssen angeschlagen bzw. wahrnehmbar angebracht sein, sodass die Bedingungen von den Kundinnen und Kunden auch wissentlich akzeptiert werden können.

Stellt ein Kunde oder eine Kundin unter den sichtbaren Bedingungen einer Nutzungsordnung bzw. Geschäftsbedingungen sein/ihr Fahrzeug ab, geht er/sie einen privatrechtlichen Vertrag ein. Der Vertrag kommt konkludent zustande, je nach Ausgestaltung entweder mit dem/der Eigentümer/in oder Besitzer/in des Grundstücks oder dem Parkraumbewirtschaftungsunternehmen. Bei Verstößen sehen die Bedingungen regelmäßig Vertragsstrafen vor. Überschreitet der/die Parkplatznutzer/in etwa die zulässige Höchstparkdauer bzw. nutzt er keine verlangte Parkscheibe, begeht er damit jeweils einen Vertragsverstoß, der den AGB folgend eine Vertragsstrafe nach sich zieht. Mithilfe des Kennzeichens hat das mit der Parkraumbewirtschaftung beauftragte Unternehmen dann die Möglichkeit, sich an das Kraftfahrt-Bundesamt zu wenden, um von dort die Übermittlung von Halterdaten (auch der Postanschrift) zu verlangen. Die gesetzliche Grundlage hierfür findet sich in § 39 Abs. 1 Straßenverkehrsgesetz.

Voraussetzung für eine Datenübermittlung vonseiten des Kraftfahrt-Bundesamtes ist allerdings, dass die begehrten Informationen der Geltendmachung von Rechtsansprüchen im Zusammenhang mit der Teilnahme am Straßenverkehr oder der Erhebung einer Privatklage wegen im Straßenverkehr begangener Verstöße dienen. Die gesetzliche Voraussetzung der „Teilnahme am Straßenverkehr" ist dabei weit zu verstehen und umfasst auch auf einem Privatparkplatz abgestellte Fahrzeuge. Hinzukommen muss noch, dass dort durch den Gebrauch der Parkfläche Rechte anderer verletzt wurden. Bei Verstößen gegen die festgelegten Bedingungen ist das Eigentums- oder Besitzrecht berührt. Rechtlich wird von einer „Besitzstörung" gesprochen.

Aus datenschutzrechtlicher Sicht kann sich also das Parkraumbewirtschaftungsunternehmen – ebenso wie im Übrigen auch der/die Eigentümer/in der Parkflächen, wenn kein privates Unternehmen beauftragt ist – bei der Erhebung und weiteren Verarbeitung der personenbezogenen Halterdaten auf Art. 6 Abs. 1 Buchst. b DSGVO stützen. Danach ist die Verarbeitung dann zulässig, wenn sie zur Erfüllung eines mit der betroffenen Person abgeschlossenen Vertrags erforderlich ist.

Was ist zu beachten?
Befährt ein/e Kfz-Halter/in eine private Parkfläche und stellt er/sie dort sein/ihr Fahrzeug ab, schließt er/sie einen privatrechtlichen Vertrag. Im Regelfall sehen die geltenden AGB Vertragsstrafen vor. Liegt ein Vertragsverstoß vor, kann der/die Eigentümer/in oder ein beauftragtes Parkraumbewirtschaftungsunternehmen vom Kraftfahrt-Bundesamt Angaben zum/zur Halter/in verlangen, um diesem/dieser gegenüber die geforderte Zahlung geltend zu machen.

2.2.12 Carsharing – Verarbeitung von Personalausweiskopien bei der Online-Identifizierung

↗ § 18 Abs. 3 PaßG; § 20 Abs. 1 und 2 PAuswG; § 21 Abs. 1 Nr. 2 StVG; Art. 5 Abs. 1 und 2, Art. 6 Abs. 1, Art. 9 DSGVO

Nachdem die Online-Reservierung von Mietwagen inzwischen praktisch zum Standard geworden ist, verlagern Mietwagenfirmen zunehmend auch die Fahrzeuganmietung ins Internet, das heißt, eine Vorsprache in einer Vermietungsstation ist dazu nicht mehr zwingend notwendig; im Carsharing-Segment werden kaum noch solche Abholstationen unterhalten, sondern lediglich Parkflächen angemietet, von denen die Mietfahrzeuge dann abgeholt oder wohin sie zurückgebracht werden können. Die erstmalige Fahrzeug-

öffnung erfolgt dann online und damit kontaktlos über das Smartphone oder per Anruf im Call-Center des Vermieters; danach kann das Fahrzeug wie gewohnt mit dem (im Fahrzeuginneren hinterlegten) Schlüssel verschlossen und geöffnet werden. Der erstmaligen Anmietung vorgelagert ist notwendigerweise eine Identifizierung des Kunden bzw. der Kundin. Mit diesem Prozess hatte ich mich im Rahmen der Beschwerdebearbeitung zu befassen.

Gegenstand der Beschwerde war, dass der Vermieter im Rahmen der Vertragsanbahnung von seiner Kundin alternativlos und somit als Bedingung für einen Vertragsabschluss eine ungeschwärzte Personalausweiskopie verlangt hätte. Darüber hinaus ging aus der Datenschutzerklärung auf der Website des Fahrzeugvermieters auch hervor, dass er davon unabhängig explizit auch die Personalausweisnummer seiner Kundinnen bzw. Kunden für Identifikationszwecke verarbeitet. Im Mittelpunkt meiner Prüfung standen daher die Verarbeitung von Personalausweiskopien einerseits und die Zulässigkeit der Verarbeitung der Personalausweisnummer andererseits.

Die dem Anmietvorgang vorgeschaltete Identitätsprüfung (Personalausweis) dient der Verhinderung eines Identitätsmissbrauchs bzw. auf dieser Grundlage beabsichtigter Fahrzeugdiebstähle oder unter Zuhilfenahme des gemieteten Fahrzeugs geplanter Straftaten. Eine solche Identitätsprüfung wird – nicht zuletzt auch wegen der hier vermieteten hochwertigen Wirtschaftsgüter – grundsätzlich als zulässig angesehen, ist aber eben auch datenschutzkonform auszugestalten. Zusätzlich wird seitens der Vermieterin bzw. des Vermieters regelmäßig auch die Kopie des Führerscheins abgefordert, um Überwachungspflichten zu genügen und gegebenenfalls der strafrechtlichen Halterhaftung zu entgehen, etwa dass jemand das überlassene Fahrzeug führt, der nicht über die dazu erforderliche Fahrerlaubnis verfügt, vgl. § 21 Abs. 1 Nr. 2 Straßenverkehrsgesetz. Dies ist insgesamt weniger kritisch zu sehen und war vorliegend durch die Beschwerdeführerin insoweit auch nicht thematisiert worden.

Zur Identitätsprüfung waren im konkreten Fall zwei Möglichkeiten vorgesehen. Kundinnen und Kunden hatten entweder die Möglichkeit, einwilligungsbasiert einen automatischen Bildabgleich (Livebild und Ausweisfoto) zu durchlaufen; zum anderen wurde alternativ ein manueller Bildabgleich durch Beschäftigte des Unternehmens angeboten, bei dem die Kundinnen bzw. Kunden zuvor eine Kopie ihres Personalausweises hochzuladen hatten. Genau dabei hatte es bei der Beschwerdeführerin wohl geklemmt, das heißt, die Schwärzungsmöglichkeit war anfangs weder intern eigenen Mitarbeitenden noch extern Kundinnen und Kunden kommuniziert worden, sodass es hier in einigen Fällen zu Missverständnissen und Fehlinterpretationen und damit auch zur Nichtakzeptanz teilgeschwärzter Ausweiskopien gekommen war. Im Zuge der aufsichtlichen Befassung meinerseits sind diese Verfahrensmängel aber dann entsprechend beseitigt worden. Insbesondere wird nunmehr an entsprechenden Beispielbildern auch verdeutlicht, welche Angaben im Personalausweis geschwärzt werden können. Dies betrifft insbesondere auch die Personalausweisnummer.

Rechtliche Bewertung

Rechtsgrundlage für die Verarbeitung personenbezogener Daten im Rahmen eines Vertragsverhältnisses ist Art. 6 Abs. 1 Buchst. b DSGVO. Danach muss die Verarbeitung für die Erfüllung des Vertrages oder zur Durchführung vorvertraglicher Maßnahmen erforderlich sein. Unstreitig sein dürfte die Feststellung, dass solche Personalausweisdaten wie Augenfarbe, Körpergröße und Zugangsnummer keine Bedeutung für den Vertragsabschluss (einschließlich Identitätsprüfung) und dessen Durchführung haben und somit nach dieser Vorschrift nicht verarbeitet werden dürfen. Dies gilt nach meiner Überzeugung auch für Personalausweisnummer, Ausstellungsdatum und Meldebehörde. Darüber hinaus und dessen ungeachtet ist die Anfertigung von Personalausweiskopien immer dann nicht notwendig, wenn sich die Vertragsparteien beim Vertragsabschluss persönlich gegenüberstehen und eine Identifizierung des Vertragspartners durch bloße Einsichtnah-

me in den Personalausweis möglich ist, § 20 Abs. 1 Personalausweisgesetz (PAuswG). Sofern Fahrzeugvermieter/innen ihren Kundinnen und Kunden auch einen Vertragsabschluss an deren Standorten anbieten, wäre diese Verfahrensweise zumindest in diesen Fällen möglich und daher auch anzubieten.
Im Rahmen der automatisierten Identitätsprüfung wird vorliegend das im Personalausweis enthaltene (biometrische) Foto mit einem aktuellen Livebild der Fahrerin bzw. des Fahrers abgeglichen. Bei diesem Verfahren werden damit biometrische Daten der Kundinnen und Kunden verarbeitet, womit zusätzlich eine Rechtfertigung, personenbezogene Daten gemäß Art. 9 DSGVO zu verarbeiten, benötigt wird. Tatsächlich kommt dafür nur eine Einwilligung betroffener Personen in Betracht, Art. 9 Abs. 2 Buchst. a DSGVO. Im Zuge der manuellen Identitätsprüfung besteht dieses Einwilligungserfordernis nicht, denn dann erfolgt der Gesichtsvergleich durch einen Mitarbeiter und nicht durch ein spezielles IT-Verfahren. (Nach Erwägungsgrund 51 der Datenschutz-Grundverordnung sollen Lichtbilder nur dann von der Definition des Begriffs „biometrische Daten" erfasst werden, wenn sie mit speziellen technischen Mitteln verarbeitet werden, die die eindeutige Identifizierung oder Authentifizierung einer natürlichen Person ermöglichen.)
Im Übrigen eröffnet § 20 Abs. 2 PAuswG auch die Möglichkeit der Anfertigung von Personalausweiskopien, vgl. die entsprechende Vorschrift des § 18 Abs. 3 Paßgesetz (PaßG). Dies ist für das manuelle Identitätsprüfungsverfahren relevant. Dabei darf der Ausweis nur von der Ausweisinhaberin bzw. vom Ausweisinhaber oder von anderen Personen mit Zustimmung des Ausweisinhabers in der Weise abgelichtet werden, dass die Ablichtung eindeutig und dauerhaft als Kopie erkennbar ist. Werden durch Ablichtung personenbezogene Daten aus dem Personalausweis erhoben oder verarbeitet, so darf die datenerhebende oder -verarbeitende Stelle dies nur mit Einwilligung der Ausweisinhaberin bzw. des Ausweisinhabers tun. Die Vorschriften des allgemeinen Datenschutzrechts über die Erhebung und Verwendung personenbezogener Daten bleiben unberührt.

Dem hier benannten – personalausweisrechtlichen – Einwilligungserfordernis wird damit Genüge getan, dass die Kundin oder der Kunde die Kopie in Kenntnis des Erhebungs- und Verarbeitungszweckes selbst bereitstellt. Die datenschutzrechtliche Zulässigkeit der Verarbeitung der (teilgeschwärzten) Ausweiskopie ergibt sich wie bereits dargestellt aus Art. 6 Abs. 1 Buchst. b DSGVO, hier der Identitätsprüfung, die online anders kaum umgesetzt werden kann. Zwar wäre die Identitätsprüfung mithilfe der Online-Ausweisfunktion des Personalausweises deutlich datensparsamer, weniger aufwendig und zugleich zuverlässiger durchzuführen, jedoch steht dem derzeit jedenfalls noch die mangelnde Akzeptanz und Verbreitung in der Bevölkerung entgegen. Zudem könnte dies – um nicht Personen ohne deutschen Personalausweis als Vertragspartner auszuschließen – natürlich nur als weitere, nichtsdestoweniger aber den datenschutzrechtlichen Anforderungen am besten gerecht werdende Alternative in Betracht kommen.

Aus dem Erforderlichkeitsgebot des Art. 6 Abs. 1 Buchst. b DSGVO einerseits wie auch dem Gebot der Datenminimierung nach Art. 5 Abs. 1 Buchst. c DSGVO andererseits ergibt sich die Forderung, dass den Kundinnen und Kunden dabei bezüglich der für die Identifizierung nicht benötigten Datenarten die Möglichkeit einer Teilschwärzung der Ausweiskopie eingeräumt und diese Möglichkeit auch gut kommuniziert wird.

Nichts anderes ergibt sich auch aus den diesbezüglichen Ausführungen des Bundesministeriums des Innern und Heimat im Personalausweisportal. Dort heißt es:

„Ausweisdaten, die nicht zur Identifizierung benötigt werden, können und sollen auf der Kopie von der Ausweisinhaberin oder von dem Ausweisinhaber geschwärzt werden. Das gilt insbesondere für die auf dem Ausweis aufgedruckte Zugangsnummer sowie für die Dokumentennummer, sofern nicht gesetzliche Regelungen diese Angaben erfordern, zum Beispiel das Geldwäschegesetz. Ausweisinhaberinnen und Ausweisinhaber sind auf die Möglichkeit und Notwendigkeit der Schwärzung hinzuweisen."

Was ist zu tun?

Soweit Vertragsabschlüsse ausschließlich online erfolgen und erhöhte Anforderungen an die Identitätsprüfung bestehen, kann dies die Verarbeitung von Personalausweiskopien rechtfertigen, wobei den Kundinnen und Kunden aufgezeigt werden muss, dass und welche Daten sie dabei schwärzen können.

2.2.13 Abruf von personenbezogenen Daten aus dem Fahreignungsregister im Bußgeldverfahren

↗ § 30 Abs. 1 und § 28 Absatz 2 StVG

Im Berichtszeitraum erreichte mich die Beschwerde eines Fahrzeughalters, dass im Rahmen einer gegen ihn gerichteten Verkehrsordnungswidrigkeit das zuständige Ordnungsamt des Landkreises zeitgleich mit der postalischen Versendung der Anhörung eine seine Person betreffende Anfrage beim Fahreignungsregister (FAER) gestellt und somit eine vorsorgliche Auskunft eingeholt habe, ohne dass seine Betroffeneneigenschaft im Bußgeldverfahren festgestanden habe.

Auf meine Nachfrage hin bestätigte das verantwortliche Landratsamt dieses Vorgehen und begründete es damit, dass für die Entscheidung über die Höhe der Geldbuße und über die Verhängung eines Fahrverbotes im Einzelfall eine Auskunft aus dem FAER einzuholen sei. Das Ordnungsamt arbeite mit einer Software, in der unterschiedliche Funktionen/Automatismen (Abfragen zum Kraftfahrt-Bundesamt, FAER etc.) hinterlegt seien. Sobald der/die Fahrzeughalter/in anhand eines positiven Plausibilitätsabgleichs von erhobenen Beweismitteln und Halterdaten als Betroffener einer Verkehrsordnungswidrigkeit eingestuft worden sei, sei automatisch die Funktion „FAER-Abfrage" gestartet worden. Dies sei auch in anderen sächsischen Ordnungsämtern die übliche Vorgehensweise.

Im FAER werden Informationen über Verkehrsteilnehmer, die im Straßenverkehr auffällig geworden sind, gespeichert, soweit die begangene Zuwiderhandlung nach dem Fahreignungs-Bewertungssystem mit Punkten zu bewerten ist. Auskünfte aus diesem Register erhalten nur berechtigte Stellen und der Betroffene selbst. Eine behördliche Abfrage im FAER, die zeitgleich bzw. zeitnah ohne Feststellung einer überwiegenden Wahrscheinlichkeit der Betroffeneneigenschaft der abgefragten Person durchgeführt wird, bewerte ich als datenschutzwidrig. Gemäß § 30 Abs. 1 Straßenverkehrsgesetz (StVG) dürfen die Eintragungen im Fahreignungsregis-

ter unter anderem an die Stellen, die für die Verfolgung von Ordnungswidrigkeiten und die Vollstreckung von Bußgeldbescheiden zuständig sind, übermittelt werden, soweit dies für die Erfüllung der diesen Stellen obliegenden Aufgaben zu den in § 28 Abs. 2 genannten Zwecken jeweils erforderlich ist. Nach § 28 Abs. 2 StVG wird das FAER geführt zur Speicherung von Daten, die unter anderem erforderlich sind für die Ahndung der Verstöße von Personen, die wiederholt Straftaten oder Ordnungswidrigkeiten, die im Zusammenhang mit dem Straßenverkehr stehen, begehen. Im Hinblick auf die Erforderlichkeit der Abfrage bzw. Übermittlung zum Zweck der Ahndung von Verstößen – nicht aber für die Sachverhaltsaufklärung zum Verstoß – ist insoweit eine zumindest überwiegende Wahrscheinlichkeit der Betroffeneneigenschaft der abgefragten Person Voraussetzung für die Abfrage (zum Beispiel Anhörungsfrist verstreicht ohne Einlassung). Diese Voraussetzung hat bei der Anfrage beim FAER zum Petenten nicht vorgelegen.

Das verantwortliche Landratsamt hat den Vorgang zum Anlass genommen, die automatischen Arbeitsabläufe dahingehend abzuändern, dass die „FAER-Abfrage" erst ausgeführt wird, sobald der/die Fahrzeugführer/in als Betroffene/r feststeht oder die Anhörungsfrist verstrichen ist und die Fahrereigenschaft nicht bestritten wird. Zudem habe ich das Sächsische Staatsministerium des Innern als oberste Rechtsaufsichtsbehörde über die Gemeinden und Landkreise im Freistaat Sachsen über den Vorgang unterrichtet und gebeten, in ihrem Geschäftsbereich dafür zu sorgen, dass alle sächsischen Ordnungsämter entsprechend informiert werden und gegebenenfalls ihre Arbeitsabläufe umstellen.

Was ist zu beachten?
Eine behördliche Abfrage im FAER, die zeitgleich bzw. zeitnah mit der Anhörung der Halterin oder des Halters ohne Feststellung einer überwiegenden Wahrscheinlichkeit der Betroffeneneigenschaft der abgefragten Person durchgeführt wird, ist datenschutzwidrig.

2.2.14 Einsatz von Funk-Rauchwarnmeldern

↗ § 47 Abs. 4 SächsBO, Art. 6 Abs. 1 Buchst. c DSGVO

Eine besorgte Mieterin hatte sich an mich gewandt und mir mitgeteilt, dass kürzlich in ihrer Wohnung Funk-Rauchwarnmelder installiert worden seien. Sie befürchtete, dass die dadurch mögliche Ferninspektion eine Überwachung ihres Verhal-

tens als Mieterin ermögliche. Ihrer Auffassung nach liege hier eine automatisierte Verarbeitung personenbezogener Daten vor, in die sie hätte einwilligen müssen. Eine Einwilligung sei aber nicht von ihr eingeholt worden; sie sei durch ihren Vermieter noch nicht einmal über den Einsatz der Geräte und die damit verbundenen Datenübertragungen informiert worden. Vor diesem Hintergrund vermutete sie einen Datenschutzverstoß.

Zunächst einmal hatte die Mieterin zutreffend eingeschätzt, dass mit den Funk-Rauchwarnmeldern personenbezogene Daten verarbeitet werden und damit deren Betrieb in den Anwendungsbereich der Datenschutz-Grundverordnung (DSGVO) fällt. Gleichwohl ist die mit dem Betrieb solcher Rauchmelder verbundene Datenverarbeitung zulässig, da sie auf eine gesetzliche Grundlage, hier Art. 6 Abs. 1 Buchst. c DSGVO gestützt werden kann. Diese Vorschrift regelt, dass eine Verarbeitung personenbezogener Daten dann rechtmäßig ist, wenn sie zur Erfüllung einer rechtlichen Verpflichtung, der ein Vermieter als datenschutzrechtlich Verantwortlicher unterliegt, erforderlich ist. Diese rechtliche Verpflichtung ergibt sich vorliegend aus der Sächsischen Bauordnung (SächsBO), und zwar konkret aus § 47 Abs. 4 SächsBO (Installationspflicht von Rauchwarnmeldern). Sowohl das Bundesverfassungsgericht (Beschluss vom 08.12.15, 1 BvR 2921/15, juris) als auch der Bundesgerichtshof (Urteil vom 16.06.15, VIII ZR 216/14, juris) haben bereits entschieden, dass Mieter/innen auch den Einbau von Funk-Rauchwarnmeldern dulden müssen. Vor diesem Hintergrund ist für eine Einwilligung an dieser Stelle kein Raum; ein Datenschutzverstoß liegt insoweit nicht vor.

Aus der Anwendbarkeit der Datenschutz-Grundverordnung folgt nichtsdestoweniger aber auch, dass der Vermieter seine Mieterin über die damit verbundene Verarbeitung personenbezogener Daten hätte unterrichten müssen, Art. 13 DSGO. Soweit dies bislang nicht erfolgt ist – wovon ich angesichts der Sachverhaltsdarstellung ausgehen musste –, wäre dies umgehend nachzuholen. Da die Mieterin aber dessen Kontaktdaten nicht mitgeteilt hatte, konnte ich es an dieser Stelle bei einem hilfestellenden rechtlichen Hinweis der Beschwerdeführerin gegenüber belassen.

Was ist zu tun?

Der Betrieb von Funk-Rauchwarnmeldern in Mietwohnungen bedarf keiner datenschutzrechtlichen Einwilligung; allerdings sind Mieter und Mieterinnen im Rahmen des Art. 13 DSGVO über die damit verbundene Verarbeitung personenbezogener Daten zu informieren.

2.2.15 Datenübertragung durch fernablesbare Messgeräte

↗ § 6a und 6b HeizkostenV; Art. 2 Abs. 1, Art. 4 Nr. 1, Art. 6 Abs. 1 Buchst. c und Abs. 2 DSGVO

Eines Tages bemerkten Bewohner/innen eines Mehrfamilienhauses, wie im Treppenhaus ein „weißer Kasten" installiert wurde. Sie dachten zunächst, es würde sich um die gesetzlich vorgeschriebenen Rauchmelder handeln. Bei näherer Betrachtung des dubiosen Kästchens fiel ihnen dann jedoch auf, dass darauf die Bezeichnung eines Messdienstleisters angebracht war. Eine Internetrecherche ergab schließlich, dass es sich um ein Gerät handelt, das per Funknetz (WLAN) die Heizungsstände ausliest. Daraus schlossen die besorgen Bewohner/innen schließlich, dass das angebrachte Gerät auch in der Lage sein könnte, Daten aus dem heimischen WLAN, insbesondere der darin eingebundenen Unterhaltungs- und Telekommunikationsgeräte auszulesen.

Mit dieser Sorge wandten sie sich an meine Behörde, sahen sie sich damit doch in ihren Persönlichkeitsrechten verletzt. Verstärkt wurde ihr Unbehagen zusätzlich dadurch, dass weder Messdienst noch die zuständige Hausverwaltung zuvor über Installation und Zweck des Gerätes informiert hatte.

In der Tat handelte es sich bei dem festgestellten Gerät um den Datensammler eines Messdienstleisters. An diesen werden, ausgehend von den funkbasierten fernablesbaren Messgeräten in den einzelnen Wohnungen, die Verbrauchswerte übermittelt. Im Anschluss daran kann der Messdienstleister die im Datensammler kumulierten Messwerte auslesen und weiterverarbeiten. Vorgaben zur Fernablesbarkeit von Verbrauchwerten finden sich in der EU-Energieeffizienz-Richtlinie (EED) sowie der ab 1. Dezember 2021 geltenden Heizkostenverordnung (HeizkostenV). Hierzu ist ein Austausch der Zähler innerhalb der betroffenen Wohneinheiten notwendig. Die Verbrauchserfassung der fernablesbaren Geräte selbst darf nur durch den Gebäudeeigentümer oder einen beauftragten Dritten vorgenommen werden (§ 6b HeizkostenV).

Freilich finden auf den eigentlichen Datenübertragungsvorgang an den Datensammler sowie den Zugriff auf die Messwerte die Vorschriften der Datenschutz-Grundverordnung (DSGVO) Anwendung, Art. 2 Abs. 1 DSGVO. Schließlich werden die Zählerstände mit einer entsprechenden personenbeziehbaren Kennung übertragen, die die Zuordnung der Verbrauchswerte ermöglicht, vgl. Art. 4 Nr. 1 DSGVO. Damit finden sie schließlich Eingang in die Verbrauchsabrechnung der betreffenden Wohneinheit. Sind fernablesbare Messgeräte für die Erfassung der Heizenergie installiert, regelt die Heizkostenverordnung, dass den Nutzern die Verbrauchsinformation monatlich mitzuteilen ist, § 6a Abs. 1 Nr. 2 HeizkostenV. Die monatliche Erfassung und Mitteilung des Verbrauchs findet damit ihre gesetzliche Stütze und ist datenschutzrechtlich nicht zu beanstanden, Art. 6 Abs. 1 Buchst. c und Abs. 2 DSGVO.

Unerheblich ist dabei, ob der/die Gebäudeeigentümer/in selbst die Ablesung und Mitteilung vornimmt oder ein beauftragter Messdienstleister. Letzterer ist rechtlich Auftragsverarbeiter, Art. 4 Nr. 8 DSGVO, mit der Folge, dass der/die Gebäudeeigentümer/in mit diesem noch einen Vertrag zur Auftragsvereinbarung abschließen muss, Art. 28 Abs. 3 DSGVO.

Doch zurück zum konkreten Fall. Nachdem ich mir anhand der Angaben der Hausbewohner/innen ein Bild machen konnte, welches Gerät diese meinten, konnte ich diese dahingehend beruhigen, dass für das beauftragte Ableseunternehmen ein Zugriff auf technische Geräte innerhalb ihres lokalen Funknetzwerks nicht möglich war. Es handelte sich um zwei voneinander unabhängige Funknetze. Ein Zugriff von außen auf in einem lokalen WLAN eingebundene Geräte oder gar das Auslesen dort gespeicherter Daten wird durch die standardmäßige Verschlüsselung innerhalb des lokalen WLAN vereitelt. Die Befürchtungen der Bewohner waren damit im Ergebnis unbegründet.

Allgemein gilt: Lagert ein/e Gebäudeeigentümer/in die Ablesung und Abrechnung von (verbrauchsabhängigen) Nebenkosten an ein damit beauftragtes Unternehmen aus, hat er/sie in dieser Hinsicht eine Pflicht zur Information (Art. 13 Abs. 1

Was ist zu tun?
Lagert der/die Hauseigentümer/in eines Mietobjekts die Erfassung und Abrechnung von Verbrauchswerten an einen Dritten (Messdienstleister) aus, sind die Mieter/innen hierüber zu informieren. Wird in diesem Zuge ein sogenannter „Datensammler" im Treppenhaus angebracht, sollte auch in diesem Fall eine Information an die Mieter/innen ergehen, obgleich insoweit keine Informationspflicht besteht.

Buchst. e DSGVO). Wird dabei von einem Messdienstleister zur Vereinfachung des Auslesevorgangs ein Datensammler angebracht, besteht hingegen insoweit keine (separate) Informationspflicht. Freilich hätte es sich im konkreten Fall angeboten, allein schon zur Vermeidung von Diskussionen innerhalb der Bewohnerschaft, mit einer kurzen Mitteilung auf die Installation sowie den Zweck des „weißen Kastens" hinzuweisen.

2.2.16 Führung der Eigentümerliste durch den Verwalter nach WEG und Herausgabe von Kontaktdaten gegenüber Miteigentümern

↗ § 18 Abs. 4, § 23 Abs. 3 Satz 1, § 24 Abs. 2 WEG; Art. 4 Nr. 11, Art. 6 Abs. 1 Buchst. a, Buchst. c in Verbindung mit Abs. 2, Art. 7 DSGVO

Ich erlebe es in meinem Behördenalltag immer wieder, dass die Mitglieder einer Wohnungseigentümergemeinschaft nach Wohnungseigentumsgesetz (WEG) der irrigen Annahme sind, dass sie innerhalb der Gemeinschaft unerkannt bleiben können. Das lässt sich nur so erklären, dass sie sich damit offensichtlich vor „lästigen" Mitteilungen der anderen Beteiligten schützen möchten. Zu Konflikten kommt es dann schnell, wenn die Hausverwaltung von sich aus unaufgefordert Eigentümerdaten weitergibt. Dies war auch Gegenstand einer an mich adressierten Beschwerde einer Wohnungsinhaberin in einem Eigentumsobjekt.

Im konkreten Fall schickte die Hausverwaltung das Protokoll einer Eigentümerversammlung mitsamt einer Liste der „relevanten Kontaktdaten" an alle Wohnungseigentümer/innen. Pikant daran war, dass die Auflistung nicht nur die Anschrift der einzelnen Eigentümer/innen beinhaltete, sondern auch jeweils eine Spalte mit privaten Festnetz- und Mobilfunknummern und auch der privaten E-Mail-Adresse. Bei einem Eigentümer fanden sich dort sogar die dienstliche Telefonnummer und E-Mail-Adresse.

Damit zeigte sich die Wohnungseigentümerin nicht einverstanden. Sie war der Ansicht, dass die Hausverwaltung sie

zuvor um ihre Zustimmung hätte fragen müssen. Mit dieser Vorstellung wandte sie sich an meine Behörde, wurde sie doch vor dem Versand der Eigentümerliste nicht einbezogen. Eine von der Hausverwaltung geführte Eigentümerliste enthält alle im Grundbuch eingetragenen Wohnungseigentümer/innen jeweils mit vollständigem Namen und ladungsfähiger Anschrift. Die Hausverwaltung ist bereits aus dem Verwaltervertrag verpflichtet, eine derartige Liste zu führen und auf dem aktuellen Stand zu halten. Ferner benötigt sie diese schlechterdings, um überhaupt die ihr aus dem Wohnungseigentumsgesetz erwachsenden Pflichten erfüllen zu können.

Es ist unbestritten, dass es sich bei einer Wohnungseigentümergemeinschaft keinesfalls um eine anonyme Gemeinschaft handelt. Vielmehr hat jeder Eigentümer bzw. jede Eigentümerin Anspruch darauf, zu erfahren, wer die weiteren Gemeinschaftsmitglieder sind. Alle Mitglieder der Wohnungseigentumsgemeinschaft sind rechtlich miteinander verbunden und haben jeweils Rechte und Pflichten. Die Kenntnis der Miteigentümer/innen ist unabdingbare Voraussetzung dafür, dass jeder einzelne Eigentümer bzw. jede einzelne Eigentümerin einige der ihm/ihr im Wohnungseigentumsgesetz eingeräumten Rechte überhaupt erst wahrnehmen kann. Beispielhaft sei hier auf die Initiative zur Einberufung einer außerordentlichen Eigentümerversammlung (§ 24 Abs. 2 WEG) oder das Zustandekommen eines Beschlusses in Textform (Umlaufverfahren, § 23 Abs. 3 Satz 1 WEG) verwiesen. Außerdem muss es einer/m Eigentümer/in möglich sein, sich mit einem Rundschreiben an einzelne oder alle Gemeinschaftsmitglieder zu wenden. Die einzelnen Mitglieder stimmen ferner über das Gemeinschaftseigentum ab und haben die Möglichkeit, an der einmal jährlich stattfindenden Eigentümerversammlung teilzunehmen.

Dementsprechend regelt das Wohnungseigentumsgesetz auch in seinem § 18 Abs. 4, dass jeder Wohnungseigentümer bzw. jede Wohnungseigentümerin Einsicht in die Verwaltungsunterlagen verlangen kann, wozu auch die Eigentümerliste zählt. Insoweit besteht eine gesetzliche Pflicht der

Hausverwaltung, Zugang zu den betreffenden Unterlagen zu gewähren, siehe Art. 6 Abs. 1 Buchst. c in Verbindung mit Abs. 2 DSGVO.

Allerdings entzündet sich in der Praxis vielmals ein Streit darüber, welche Eigentümerdaten die Hausverwaltung herausgeben darf oder muss. Fest steht, dass der Herausgabeanspruch nicht schrankenlos ist, sondern sich nach dem Zweck richtet, für den die Eigentümerliste benötigt wird. Im Hinblick darauf, dass die darin enthaltenen Personendaten eine wechselseitige Kontaktaufnahme zwischen den Gemeinschaftsmitgliedern ermöglichen sollen, reichen hierfür bereits Vor- und Nachname sowie ladungsfähige Anschrift aller im Grundbuch eingetragenen Eigentümer aus. Weitere Kontaktdaten wie E-Mail-Adressen oder Telefonnummern sind für diesen Zweck nicht notwendig, siehe hierzu das Urteil des Landgerichts Düsseldorf vom 4. Oktober 2018, Az. 25 S 22/18.

Möchte die Verwaltung folglich elektronische oder telefonische Kontaktdaten weitergeben, kann sie dies nur mit Einwilligung der Beteiligten. Nur insoweit kommt also die Einwilligungslösung des Art. 6 Abs. 1 Buchst. a in Verbindung mit Art. 4 Nr. 11, Art. 7 DSGVO zum Tragen.

Es zeigte sich in dem mir zugetragenen Fall, dass die Hausverwaltung leichtfertig und überschießend alle ihr bekannten Kontaktdaten der Mitglieder verschickt hat, womöglich, um proaktiv entsprechenden Nachfragen zuvorzukommen. Ich kam schlussendlich nicht umhin, deswegen der Hausverwaltung gegenüber eine datenschutzrechtliche Verwarnung auszusprechen, Art. 58 Abs. 2 Buchst. b DSGVO. Diese in erster Linie für geringfügige Verstöße infrage kommende Abhilfemaßnahme soll dem Verantwortlichen vor Augen führen, dass er im Widerspruch zu datenschutzrechtlichen Vorschriften agiert hat. Ich verbinde damit gleichzeitig die Hoffnung, dass ich mit dieser Rüge zur Bewusstseinsbildung beitrage und die verantwortlichen Stellen in Zukunft mehr Sorgfalt beim Umgang mit den personenbezogenen Daten walten lassen.

Was ist zu tun?

Für die gegenseitige Kontaktaufnahme der Mitglieder einer Wohnungseigentumsgemeinschaft reichen der vollständige Name sowie die ladungsfähige Anschrift aus. E-Mail-Adressen und Telefonnummern der Miteigentümer/innen darf die Hausverwaltung nur mit entsprechender Einwilligung weitergeben.

2.2.17 Bekanntgabe von Prüfungsergebnissen an Ausbildungsbetriebe

↗ § 31 Abs. 2 HandwO

Ich wurde darauf hingewiesen, dass seitens verschiedener Ausbildungsbetriebe zunehmend Notenübersichten von ihren Auszubildenden angefordert werden, und dazu um eine rechtliche Bewertung gebeten. Dazu hat bereits mein Amtsvorgänger in seinem 7. Tätigkeitsbericht für den öffentlichen Bereich (9.3.2, Seite 105 f.) auf die Regelung in § 31 Abs. 2 Handwerksordnung hingewiesen. Dort heißt es: „Dem Ausbildenden werden auf dessen Verlangen die Ergebnisse der Gesellenprüfung des Lehrlings (Auszubildenden) übermittelt. Sofern die Gesellenprüfung in zwei zeitlich auseinanderfallenden Teilen durchgeführt wird, ist das Ergebnis der Prüfungsleistung im ersten Teil der Gesellenprüfung dem Prüfling schriftlich mitzuteilen." Eine entsprechende Regelung enthält auch § 37 Abs. 2 Berufsbildungsgesetz.

Angesichts dieser klaren Regelung kann nicht von der Zulässigkeit der generellen Übermittlung von Notenübersichten ausgegangen werden.

Darüber hinaus kann man im Einzelfall prüfen, ob eine weitere Datenübermittlung gemäß § 3 Abs. 1 Sächsisches Datenschutzdurchführungsgesetz für eine Berufsausbildung erforderlich ist. Einen entsprechenden Maßstab kann man den ausdrücklichen Regelungen in anderen Bundesländern entnehmen. So bestimmt beispielsweise § 47 Abs. 9 Thüringer Allgemeine Schulordnung für die berufsbildenden Schulen: „Die Schulen informieren die Ausbildenden möglichst frühzeitig über unentschuldigte Fehlzeiten, angedrohte und verhängte Ordnungsmaßnahmen sowie einen deutlichen Abfall der schulischen Leistungen, wenn durch diesen der erfolgreiche Abschluss der schulischen Ausbildung gefährdet ist." Wünschenswert wäre eine entsprechende Klarstellung in der Schulordnung Berufsschule.

Kritisch ist hingegen eine Einwilligungslösung (beispielsweise in Ausbildungsverträgen) für eine weitergehende Datenübermittlung zu sehen. Auszubildende stehen in ei-

nem Über-/Unterordnungsverhältnis sowohl mit dem Ausbildungsbetrieb als auch mit der Berufsschule als staatliche Stelle. Eine Einwilligung, die auf der freien Entscheidung der Auszubildenden beruht und somit gemäß § 4 Nr. 11 DSGVO freiwillig ist, ist somit nur schwer vorstellbar. Es bleibt einem bzw. einer Auszubildenden selbstverständlich freigestellt, seine/ihre Noten selbst seinem/ihrem Ausbildungsbetrieb mitzuteilen.

Was ist zu tun?
Notenübermittlungen an Ausbildungsbetriebe dürfen nur im gesetzlichen Rahmen erfolgen.

2.2.18 Überwachte Schultoilette

↗ SchulG

Ich wurde von Sorgeberechtigten darauf hingewiesen, dass an der Schule ihres Kindes alle Lehrer von der Schulleitung aufgefordert wurden, sämtliche Schülerinnen und Schüler mit Datum und Uhrzeit zu erfassen, die die Schultoiletten benutzen.
Nach Information der Schulleitung stellte sich der Sachverhalt wie folgt dar: An der Schule hat es zuletzt zwei Vandalismus-Vorfälle gegeben. Zum einen wurde ein Brand in den Mädchentoiletten gelegt, der einen Brandalarm ausgelöst hat. Im nächsten Fall wurde mit gewässertem Toilettenpapier in der Jungentoilette „Unfug getrieben". In der Schule wird seitdem im Klassenbuch notiert, welcher Schüler bzw. welche Schülerin in der Unterrichtszeit die Toilette aufgesucht hat. In den Pausenzeiten erfolgt keine Kontrolle.
Nach meiner Einschätzung war eine Aufzeichnung der Toilettengänge, beschränkt auf die Unterrichtszeit, im vorliegenden Fall wegen der vorhergegangenen Vorfälle grundsätzlich zulässig. Allerdings waren die vorgenommenen Aufzeichnungen im Klassenbuch nicht angemessen. Nur eine Aufzeichnung außerhalb des Klassenbuches dürfte erforderlich sein; beispielsweise ein Eintrag in eine (gegebenenfalls) Tagesliste und die zeitnahe Vernichtung dieser Liste (etwa nach ein bis zwei Tagen). Die Maßnahmen sollten auch nur für einen begrenzten Zeitraum durchgeführt werden, um dann die Wirksamkeit zu überprüfen.

Was ist zu tun?
Schulen sollten auch bei als Reaktion auf Vandalismus etablierten Datenverarbeitungen die Angemessenheit beachten.

Die Schulleitung teilte mir daraufhin mit, dass derzeit keine entsprechende Erfassung mehr erfolgt. Sollte diese nach ihrer Einschätzung jedoch wieder notwendig werden, wird diese entsprechend der von mir gegebenen Hinweise datenschutzgerecht erfolgen. Das sah ich als ausreichend an.

2.2.19 Schulaufnahmeuntersuchung, Einschätzung der Kindertageseinrichtung

↗ § 3 bis 5 Schulordnung Grundschule, § 4 SachsSchulGesPflVO, §§ 26a und 27 SachsSchulG

18. Tätigkeitsbericht für den öffentlichen Bereich:
↗ sdb.de/tb2111

Ein erneuter Fall überzogener Datenerhebung (siehe schon 18. Tätigkeitsbericht für den öffentlichen Bereich, 10.2.5, Seite 117 ff.) wurde mir im Rahmen einer anonymen Beschwerde über das Gesundheitsamt eines Landratsamtes/einer Kreisfreien Stadt bekannt. Dieses verwendet einen Fragebogen „Einschätzung des Kindergartens". Der Fragebogen wurde mit der Einladung zur Schulaufnahmeuntersuchung an die Eltern versandt. Die Kindertageseinrichtung (Kita), die das Kind besucht, soll den Fragebogen ausfüllen. Der Fragebogen weist detaillierte Fragen zum Entwicklungsstand des Kindes auf.
So fanden sich unter anderem Fragen, ob die aufgeführten Probleme bei dem genannten Kind in den letzten sechs Monaten im Kindergarten aufgetreten sind; hier die gravierendsten Fragen zu diesem Punkt (Es ist „stimmt" oder „stimmt nicht" anzukreuzen):

Das Kind:

1. nässt mindestens einmal pro Woche tagsüber ein
2. kotet mindestens einmal pro Woche tagsüber ein
3. kaut Fingernägel
4. ist mehrmals im Monat traurig, weinerlich ohne erkennbaren Anlass
5. gehorcht immer, widerspricht nie
6. ist leicht ablenkbar und unkonzentriert
7. ist sehr unruhig, zappelig, kann nicht stillsitzen
8. ist beim Spielen sehr unvorsichtig und riskant in seinem Verhalten

9. hat mindestens zweimal pro Woche einen Wutanfall oder ähnliche unangemessene Reaktionen
10. hält häufig Regeln und Absprachen nicht ein
11. sucht häufig Streit mit anderen Kindern.

Die soziale Kompetenz wird in vier Abstufungen von deutlich überdurchschnittlich, überdurchschnittlich, durchschnittlich, auffällig und stark auffällig ermittelt. Dies ist bei folgenden Fragen anzukreuzen:

Das Kind hat ...

- einen oder mehrere Freunde innerhalb der Gruppe
- bringt eigene Ideen oder Lösungsvorschläge ein
- kann neue Anforderungen verstehen und umsetzen
- zeigt eine gute Auffassungsgabe
- kann eigene Interessen zugunsten der Gruppe zurückstellen
- kann seine Gefühle angemessen zeigen oder verbal äußern
- kann Frustrationserlebnisse angemessen verarbeiten.

Nach meiner Einschätzung ist eine detaillierte Datenerhebung des Gesundheitsamts bei der jeweiligen Kita rechtswidrig, da dazu keine rechtliche Befugnis vorliegt. Den Rechtsgrundlagen für die Schulaufnahmeuntersuchung, § 26a, § 27 Sächsisches Schulgesetz (SächsSchulG), § 4 Sächsische Schulgesundheitspflegeverordnung (SächsSchulGesPflVO) und §§ 3 bis 5 Schulordnung Grundschule, ist nicht zu entnehmen, dass vor der Schulaufnahmeuntersuchung Daten zum Entwicklungsstand des Kindes bei der Kita, die das Kind besucht, erhoben werden können.
Die Schulgesundheitspflege wird nach § 26a Abs. 1 Satz 2 SächsSchulG von den Behörden des öffentlichen Gesundheitsdienstes in Zusammenarbeit mit dem Schulleiter, den Lehrern, den Schülern und den Eltern wahrgenommen. Die Schulaufnahmeuntersuchung ist in § 26a Abs. 3 Nr. 1 SächsSchulG aufgeführt. Sie ist vom Gesundheitsamt durchzuführen (§ 26a Abs. 5 SächsSchulG).

Eine Datenerhebung auf Grundlage einer Einwilligung der Erziehungsberechtigten scheidet nach meiner Auffassung indes ebenfalls aus. Nach dem Vorbehalt des Gesetzes (vgl. Art. 20 Abs. 3, 2. Halbsatz Grundgesetz [GG] in Verbindung mit der Grundrechtsbindung, Art. 1 Abs. 3 GG und dem Demokratieprinzip, Art. 20 Abs. 1 GG) dürfen Träger öffentlicher Gewalt (wie der Landkreis/die Kreisfreie Stadt) nicht im größeren Maße ihnen im Gesetz nicht ausdrücklich zugewiesenen Aufgaben mithilfe einer lediglich durch Einwilligung der Betroffenen gerechtfertigten Verarbeitung personenbezogener Daten an sich ziehen und erfüllen und dazu durch Verarbeitung personenbezogener Daten in Grundrechte eingreifen.
Die Verwendung des Fragebogens wurde deshalb von mir gestoppt.

Was ist zu beachten?
Eine Datenerhebung des Gesundheitsamts vor der Schulaufnahmeuntersuchung bei der Kita zum Entwicklungsstand des Kindes ist mangels Rechtsgrundlage nicht zulässig.

2.2.20 Elektronische Hochschulcard als Studierendenausweis

Ich wurde darauf hingewiesen, dass möglicherweise eine unberechtigte Datenverarbeitung personenbezogener Daten durch eine Hochschule im Rahmen der Einführung einer elektronischen Hochschulcard erfolge.
An der betreffenden Hochschule wird seit dem Jahr 2023 der Studierendenausweis gemäß Immatrikulationsordnung als elektronische Karte ausgegeben.
In einer Nutzungsordnung wurde abschließend festgelegt, für welche Zwecke die Hochschulcard von den Studierenden eingesetzt werden kann. Die neue Hochschulcard kann demnach für die Nutzung als Studierendenausweis, als elektronisches Semesterticket sowie als Bibliotheksausweis eingesetzt werden. Ferner kann sie als Geldbörse für Dienstleistungen des Studentenwerkes, beispielsweise zur Zahlung des Mensaessens genutzt werden.
Gemäß der gültigen Nutzungsordnung der Hochschulcard dürfen personenbezogene Daten auf der Hochschulcard gespeichert werden, dies umfasst unter anderem den Namen, Vornamen (optisch), die Matrikelnummer (optisch), die hochschulübergreifende Identifikationsnummer (optisch und elek-

tronisch) und das Lichtbild (optisch). Die Studierenden haben zur Erstellung ihrer Hochschulcard ein geeignetes Lichtbild in elektronischer Form zur Verfügung zu stellen. Mit dieser Karte können sich dann die Studierenden offiziell als Studentin oder Student ihrer Hochschule ausweisen. Bei der Verwendung der Hochschulcard als Studierendenausweis ist ferner zur Überprüfung der Teilnahmeberechtigung auf Verlangen ein amtlicher Lichtbildausweis vorzulegen.

In einer Stellungnahme teilte mir die Hochschule mit, dass für die verschiedenen Zugriffe der Beteiligten technische und organisatorische Maßnahmen vorgesehen sind, sodass diese Zugriffe auf die Hochschulcard getrennt voneinander erfolgen. Auf der Karte selbst wäre für jeden Anwendungsfall eine separate verschlüsselte Applikation enthalten.

Insbesondere der Name und das Lichtbild der betroffenen Personen sind nur optisch auf der Hochschulcard aufgedruckt und nicht elektronisch auf der Karte gespeichert. Die wesentlichen Daten liegen jeweils in der Fachanwendung des Verfahrensteilnehmers. Diese Fachanwendungen sind technisch und organisatorisch voneinander getrennt und können nur vom jeweiligen Verfahrensteilnehmer genutzt werden. Eine Zusammenführung von Daten über Verfahrensteilnehmer hinweg über die Hochschulcard selbst ist somit bereits technisch ausgeschlossen.

Was ist zu beachten?
Eine elektronische Hochschulcard als Studierendenausweis ist unter Beachtung maßgeblicher datenschutzrechtlicher Anforderungen zulässig.

Einen Datenschutzverstoß habe ich bei meiner Überprüfung der Einführung der elektronischen Karte an der Hochschule nicht festgestellt.

2.2.21 Losbasierte Bürgerbeteiligung und Meldedaten

↗ § 37 Abs. 1 und § 34 Abs. 1 BMG; Art. 6 Abs. 1 Buchst. a, c, e DSGVO; Art. 6 Abs. 3 Satz 1 DSGVO

Basisdemokratische Ansätze haben vor allem auf kommunalpolitischer Ebene deutlich an Bedeutung gewonnen. Der Freistaat Sachsen betreibt beispielsweise ein Bürgerbeteiligungsportal, auf dem Kommunen für die Bürger/innen verschiedene Möglichkeiten schaffen, sich aktiv in Entschei-

dungs- und Gestaltungprozesse einzubringen. Eine Art der Partizipation hierzu ist die sogenannte Losbasierte Bürgerbeteiligung oder Losbasierte Bürgerräte.

Hierzu hat sich eine kleinere sächsische Gemeinde für die Ausarbeitung eines Stadtentwicklungskonzeptes nun entschieden. Datenschutzrechtlich ist dies nicht unproblematisch umzusetzen, da nicht jeder Bürger bzw. jede Bürgerin damit einverstanden sein wird, dass seine/ihre Daten für diese Zwecke verwendet werden. Um die potenziellen Teilnehmer/innen eines Bürgerrates auszulosen und anzuschreiben, bedarf es hierzu aber notwendigerweise ihrer personenbezogenen Daten. Nicht nur Namen und Adressen, sondern auch Alter, Beruf und anderes spielen hier eine Rolle, denn ein Bürgerrat sollte einen repräsentativeren Querschnitt der Gemeindeeinwohner abbilden.

Die jeweilige Gemeinde wandte sich nun an mich mit der Frage, ob Meldedaten aus dem örtlichen Melderegister ohne vorherige Einwilligung des Bürgers bzw. der Bürgerin hierzu verwendet werden können.

Dies musste ich der Gemeinde aber verneinen. Die bei den Meldebehörden gespeicherten Daten genießen einen gesetzlich verankerten besonderen Schutz. Die hier geplante Stichprobenziehung aus dem Melderegister zur Verarbeitung im Rahmen von Bürgerbeteiligungsformaten erfolgt im Anwendungsbereich der Datenschutz-Grundverordnung (DSGVO) und bedarf einer tragfähigen Rechtsgrundlage. Dieser Schutz kommt in dem Bundesmeldegesetz (BMG) – und den entsprechenden landesrechtlichen Ausführungsgesetzen und Verordnungen – zum Ausdruck.

Gesetzlich ist aber selbst eine behördeninterne Weitergabe nur dann vorgesehen, wenn diese Datenweitergabe zur eigenen Aufgabenerfüllung der Meldebehörde oder zur Erfüllung einer dem Empfänger obliegenden öffentlichen Aufgabe erforderlich ist, § 37 Abs. 1 und § 34 Abs. 1 BMG. Anderenfalls ist die Weitergabe nicht zulässig.

Rechtlich ist daher vorgesehen, dass die Behörde eine gesetzlich hinreichend bestimmte (Pflicht-)Aufgabe treffen muss, und diese ohne die entsprechenden Meldedaten nicht (oder

nicht in zumutbarer Weise) zu bewerkstelligen ist. Bürgerbeteiligung ist aber gerade keine (Pflicht-)Aufgabe der Gemeinde. Verarbeiten öffentliche Stellen nun personenbezogene Daten im Rahmen von Bürgerbeteiligungsformaten, agieren sie auch hier nicht als Personen des Privatrechts, sondern haben als staatliche Akteure das Grundrecht der betroffenen Personen auf informationelle Selbstbestimmung zu beachten. An diesem Befund ändert auch der Umstand nichts, dass Bürgerbeteiligung nicht als hoheitliche Eingriffsverwaltung qualifiziert werden kann, sondern ja wohl gerade einem Austausch „auf Augenhöhe" und einer engeren Abstimmung zwischen Kommune und den von ihren Entscheidungen betroffenen Personen dient und insoweit als eine Form demokratischer Teilhabe grundsätzlich begrüßenswert ist.

Rechtliche Wertung anhand der DSGVO

Eine datenschutzrechtliche Einwilligung (Art. 6 Abs. 1 Buchst. a DSGVO), die im Verhältnis zwischen Staat und Bürgerinnen und Bürgern als Rechtsgrundlage für die Verarbeitung personenbezogener Daten zwar grundsätzlich problematisch ist, für die Verarbeitung personenbezogener Daten im Rahmen von Bürgerbeteiligungsformaten aber gegebenenfalls in Betracht gezogen werden könnte, scheidet als Verarbeitungsgrundlage hinsichtlich der (zufälligen) Auswahl von Bürgerinnen und Bürgern – bereits wegen fehlender Praktikabilität – aus.

Eine Datenverarbeitung, zu der auch die verwaltungsinterne Weitergabe gehört, bedarf daher einer wirksamen Rechtsgrundlage, Art. 6 Abs. 3 Satz 1 in Verbindung mit Art. 6 Abs. 1 Buchst. c und e DSGVO. Diese Norm bestimmt, dass die Rechtsgrundlage für die Verarbeitungen durch Unionsrecht oder das Recht der Mitgliedsstaaten festgelegt wird, dem der Verantwortliche unterliegt.

Ich musste der Gemeinde mitteilen, dass derzeit dem vorgestellten Kontext keine gesetzliche Zuweisung der Aufgabe „Bürgerbeteiligung" vorliegt. Kommunale Satzungen sind indes ebenfalls als Rechtsvorschriften im Sinne von Art. 6 Abs. 3 DSGVO anzusehen, weswegen ich der anfragenden Gemeinde nur raten konnte, eine entsprechende Satzung auf den Weg zu

bringen und zu beschließen. Sämtliche bisher durchgeführten kommunalen Bürgerbeteiligungsformate werden sachsenweit auf Grundlage kommunaler Satzungen durchgeführt.
Satzungen gehören zum sogenannten rein materiellen Recht und stehen im Gegensatz zum formellen Recht, das heißt zu den parlamentarisch beschlossenen Rechtsnormen. Auch wirksam beschlossene kommunale Satzungen werden indes unter bestimmten Voraussetzungen als Rechtsvorschriften im Sinne von Art. 6 Abs. 3 DSGVO angesehen. Eine Aufgabenzuweisungsnorm kann – solange eine landesrechtliche Regelung fehlt – nach alledem auch per kommunaler Satzung erfolgen. Wesentlich ist, dass die Aufgabe, für die die Stichprobenziehung aus dem Melderegister erforderlich ist, in der Satzung klar und hinreichend bestimmt geregelt sein muss.
Die Schaffung einer landesweiten formal-gesetzlichen Grundlage für die Durchführung von Bürgerbeteiligungsformaten unter Berücksichtigung datenschutzrechtlicher Aspekte halte ich allerdings als vorzugswürdig. Hierzu ist eine Regelung durch den sächsischen Gesetzgeber notwendig, die (im Unterschied zu anderen Bundesländern) noch nicht erfolgt ist.

Was ist zu tun?
Gemeinden dürfen nicht auf Meldedaten zugreifen, wenn es darum geht, Bürger/innen an politischen Entscheidungsprozessen zu beteiligen. Vielmehr ist eine entsprechende Satzung als eigene Rechtsgrundlage für die Datenverarbeitung zu beschließen.

2.2.22 Datenverarbeitung eines kommunalen Gutachterausschusses zur Erstellung der Kaufpreissammlung

↗ BauGB, BGB, SächsGAVO

Ein Petent wandte sich gegen die Weiterleitung seines Kaufvertrags durch den den Kaufvertrag beurkundenden Notar an den kommunalen Gutachterausschuss.
Nach der Datenschutz-Grundverordnung ist eine Datenverarbeitung und mithin also auch eine Datenübermittlung zulässig, so sie auf eine gültige Rechtsgrundlage, also Rechtsnorm, gestützt werden kann.
Gemäß § 195 Abs. 1 Baugesetzbuch (BauGB) ist jeder Vertrag über eine entgeltliche Grundstücksveräußerung in Abschrift dem Gutachterausschuss zur Führung der Kaufpreissammlung zu übersenden.

Entgeltlichkeit ist dann anzunehmen, wenn der Erwerber für die Eigentumsübertragung eine wirtschaftliche Gegenleistung erbringen muss. Als Gegenleistung kommt insbesondere die Zahlung einer Geldsumme oder einer Rente, der Erlass einer Schuld und der Verzicht auf einen Anspruch in Betracht. Nicht übersendungspflichtig sind daher nur Verträge, die zur unentgeltlichen Übertragung des Eigentums an einem Grundstück – etwa im Wege einer reinen Schenkung nach § 516 Bürgerliches Gesetzbuch – verpflichten. Hierunter dürften jedenfalls Überlassungsverträge fallen, in denen weder bestimmte Gegenleistungen vereinbart noch Rechte vorbehalten werden. So es sich mithin um den Fall einer entgeltlichen Grundstücksveräußerung handelt, ist die Datenweitergabe durch den Notar an den Gutachterausschuss nicht zu beanstanden. Falls zur Führung der Kaufpreissammlung erforderlich, sind durch den Gutachterausschuss weitere Ermittlungen gemäß § 197 BauGB durchzuführen.

Die Aufgaben der Gutachterausschüsse wie auch die Rechte und Pflichten der Gutachter sind in der Sächsischen Gutachterausschussverordnung geregelt.

Die Gutachter haben danach die ihnen durch ihre Tätigkeit zur Kenntnis gelangten Informationen, sofern diese nicht öffentlich zugänglich sind, auch über den Bestellungszeitraum hinaus geheim zu halten. Die Gutachter sind vor der Übernahme ihrer Tätigkeit auf diese Pflicht besonders zu verpflichten.

Nach § 9 der genannten Verordnung sind Verträge und sonstigen Rechtsvorgänge nach § 195 Abs. 1 BauGB sowie die nach § 13 der Verordnung übermittelten Informationen nach Weisung des Gutachterausschusses unverzüglich auszuwerten und in die Kaufpreissammlung aufzunehmen. Die Kaufverträge und die anderen Urkunden sind nach ihrer Auswertung zu vernichten.

Die Kaufpreissammlung steht nur den Mitgliedern des Gutachterausschusses und den Bediensteten der Geschäftsstelle in dem zur Erfüllung ihrer Aufgaben erforderlichen Umfang zur Verfügung. Durch geeignete Maßnahmen ist sicherzustellen, dass Unbefugte keine Kenntnis vom Inhalt der Kaufpreissammlung erhalten. § 195 Abs. 2 BauGB bleibt unberührt.

Was ist zu beachten?
Nach § 195 Abs. 1 BauGB ist ein Vertrag über eine entgeltliche Grundstücksveräußerung dem Gutachterausschuss für die Kaufpreissammlung zu übersenden.

Nach § 10 der Verordnung sind auf schriftlichen Antrag unter bestimmten Voraussetzungen grundstücksbezogene Auskünfte aus der Kaufpreissammlung zu erteilen. Der Name und die Anschrift des Eigentümers oder sonstiger berechtigter Personen dürfen nicht mitgeteilt werden. Die im Rahmen von Auskünften übermittelten Informationen dürfen nur für den Zweck verwendet werden, zu dessen Erfüllung sie erteilt worden sind.

2.2.23 Corona-Entschädigung nach § 56 Abs. 1a Infektionsschutzgesetz – Vorlage von Geburtsurkunden

↗ § 56 Abs. 1a IfSG

Die Landesdirektion Sachsen (LDS) hat laut Pressemitteilung vom 3. August 2023 300.973 Anträge auf Corona-Entschädigung nach dem Infektionsschutzgesetz (IfSG) bearbeitet und über 221 Millionen Euro an Entschädigungsleistungen ausgezahlt. Insgesamt wurden bisher 342.528 Anträge gestellt.
Es ist daher nicht verwunderlich, dass mich eine Anfrage zum Umfang der für die Prüfung erforderlichen Unterlagen erreichte. Der Petent zog in Zweifel, dass die Aufforderung der LDS, eine Geburtsurkunde für das zu betreuende Kind im Rahmen der Prüfung einer Entschädigung nach § 56 Abs. 1a IfSG vorzulegen, zulässig sei.
Gemäß § 56 Abs. 1a IfSG erhält eine erwerbstätige Person unter bestimmten Voraussetzungen eine Entschädigung wegen Verdienstausfalls, wenn sie während der Pandemie ihre Kinder betreuen musste, weil Krippe, Kindertagesstätte, Schule und Hort oder Einrichtungen für Menschen mit Behinderungen durch die Behörden aufgrund des IfSG vorübergehend geschlossen wurden oder deren Betreten, auch aufgrund einer Absonderung, untersagt wurde.

Weitere Voraussetzungen sind, dass

- die Person ihr Kind, dass das zwölfte Lebensjahr noch nicht vollendet hat, betreuen musste,
- keine anderweitige zumutbare Betreuungsmöglichkeit bestand.

Nach § 56 Abs. 1a S. 1 Nr. 2 IfSG muss es sich um das eigene Kind der erwerbstätigen Person handeln („ihr Kind"). Erfasst sind davon nur leibliche Eltern, Adoptiveltern und – wie § 56 Abs. 1a Satz 4 IfSG klarstellt – Pflegeeltern, wenn sie das Kind in Vollzeitpflege nach § 33 Achtes Buch Sozialgesetzbuch (SGB VIII) in ihren Haushalt aufgenommen haben.

Nicht erfasst sind Fälle, in denen Erwerbstätige ein haushaltsangehöriges Kind, das nicht das eigene Kind ist, selbst betreuen.

Diese Voraussetzungen für den Entschädigungsanspruch sind von der LDS zu prüfen. Der Antragsteller hat die Elternschaft nachzuweisen. Das geeignete Mittel dazu ist, so die LDS, die Geburtsurkunde des Kindes. Daraus ergeben sich sowohl das Alter des Kindes als auch die Namen der Eltern.

Da die Geburtsurkunde die Namen beider Elternteile enthält, ermöglicht diese zudem die Prüfung, ob der andere von dem jeweiligen Entschädigungsverfahren nicht erfasste Elternteil für denselben Zeitraum ebenfalls einen Antrag auf Entschädigung wegen Kinderbetreuung gestellt hat. Diese Prüfung ist notwendig, weil nur einem Elternteil der Entschädigungsanspruch zusteht. Weiterhin lässt sich dann prüfen, ob der andere Elternteil im Betreuungszeitraum möglicherweise selbst in Quarantäne war. Auch hier scheidet in der Regel ein Anspruch des betreuenden Elternteils aus, da dem anderen Elternteil in Quarantäne die gleichzeitige Betreuung des Kindes grundsätzlich zumutbar ist. Die Prüfung der Geburtsurkunde vermeidet damit auch unzulässige Doppelentschädigungen.

Ich teile die Auffassung der LDS, dass die Vorlage der Geburtsurkunde erforderlich ist, um nachzuweisen, dass es sich um das eigene Kind handelt, das das zwölfte Lebensjahr noch nicht vollendet hat, wie § 56 Abs. 1a Nr. 2 IfSG es fordert. Zudem können dadurch unzulässige Doppelentschädigungen vermieden werden.

Was ist zu beachten?
Bei der Prüfung einer Corona-Entschädigung nach § 56 Abs. 1a IfSG kann die Landesdirektion Sachsen die Vorlage der Geburtsurkunde des Kindes verlangen.

2.2.24 Halterabfrage zum Ehemann zur Prüfung der Zahlungsfähigkeit bezüglich einer Bußgeldforderung gegen die Ehefrau

↗ § 5b Abs. 1 Nr. 2 VwVG, § 33 Abs. 1 StVG

Ein Petent wandte sich an mich mit dem Vortrag, ein sächsischer Landkreis (LK) hätte eine Halterabfrage zu den auf ihn zugelassenen Kraftfahrzeugen durchgeführt. Vorausgegangen sei ein Bußgeldverfahren des LK gegen seine Ehefrau, welche das Bußgeld zum Zeitpunkt der Halterabfrage noch nicht beglichen hatte. Der von mir um Stellungnahme gebetene LK bestätigte den Sachverhalt. Die Ehefrau des Petenten habe im Rahmen der Vollstreckung des Bußgeldes den LK auf eine angebliche Zahlungsunfähigkeit hingewiesen. Die Halterabfrage zum Petenten sei durchgeführt worden, weil das Ehepaar laut einer vormals abgegebenen Vermögensauskunft der Ehefrau in einer Zugewinngemeinschaft lebte und daher davon ausgegangen worden sei, dass die Ehefrau Miteigentümerin der Fahrzeuge, deren Halter ihr Ehemann ist, sei. Gemäß § 6 Fahrzeugzulassungsverordnung ist die Zulassung eines Kraftfahrzeuges nur auf eine natürliche Person möglich, was aber nicht dagegengesprochen habe, dass die Ehefrau gleichwohl Miteigentümerin der Kraftfahrzeuge sei.

Eine Behörde darf personenbezogene Daten nur auf Grundlage einer gesetzlichen Vorschrift abrufen und verarbeiten. Die vorliegende Halterabfrage zum Petenten im Rahmen des Bußgeldverfahrens gegen seine Ehefrau als Vollstreckungsschuldnerin war mangels einer solchen Rechtsgrundlage datenschutzwidrig. Gemäß § 17 Abs. 1 Sächsisches Verwaltungsvollstreckungsgesetz (SächsVwVG) hat der Vollstreckungsschuldner dem Gerichtsvollzieher eine Vermögensauskunft zu erteilen, wenn die Vollstreckungsbehörde dem Gerichtsvollzieher ein schriftliches Vollstreckungsersuchen übergeben und ihm einen entsprechenden Auftrag erteilt hat. Anstatt den Auftrag an den Gerichtsvollzieher zu erteilen, können die Landkreise, Kreisfreien Städte und Gemeinden gemäß § 17 Abs. 5 SächsVwVG verlangen, dass der

Vollstreckungsschuldner die Auskunft über sein Vermögen ihnen gegenüber erteilt, das heißt, die Vollstreckungsbehörden haben die Möglichkeit, dem Vollstreckungsschuldner die Vermögensauskunft auch durch eigene Bedienstete abnehmen zu lassen. Auskünfte bei Dritten zu dem Vollstreckungsschuldner – wie vorliegend beim Kraftfahrt-Bundesamt (KBA) – dürfen die Vollstreckungsbehörden allerdings nicht selbst einholen, sondern müssen hierfür gemäß § 17 Abs. 3 SächsVwVG den Gerichtsvollzieher beauftragen. Schon allein aus diesem Grund war die Abfrage des hier verantwortlichen LK beim KBA rechtswidrig. Hätte der LK als Vollstreckungsbehörde einen Gerichtsvollzieher mit der Einholung der Auskunft beauftragt, so wäre eine Abfrage des Gerichtsvollziehers beim KBA zum Petenten allerdings ebenfalls rechtswidrig gewesen. § 17 Abs. 3 SächsVwVG verweist unter anderem auf den § 802l Zivilprozessordnung, wonach der Gerichtsvollzieher die Fahrzeug- und Halterdaten nach § 33 Abs. 1 Straßenverkehrsgesetz (StVG) beim KBA zu einem Fahrzeug erheben darf, als dessen Halter der Vollstreckungsschuldner eingetragen ist. Im vorliegenden Fall war Vollstreckungsschuldnerin allerdings die Ehefrau des Petenten und Fahrzeughalters. Dies habe ich dem verantwortlichen LK entsprechend erläutert, welcher daraufhin mitteilte, dass der Vorgang intern ausgewertet und zum Anlass genommen worden sei, die Beschäftigten im zuständigen Referat bezüglich datenschutzrechtlicher Aspekte erneut zu sensibilisieren. Die zuständigen Mitarbeiter seien in diesem Zusammenhang ausdrücklich auf die Rechtswidrigkeit der Fahrzeug- und Halterabfragen betreffend einen Nichtschuldner sowie die Erforderlichkeit einer einschlägigen Rechtsgrundlage hingewiesen und aktenkundig belehrt worden. Ich begrüße diese behördeninterne Vorgehensweise zur Vermeidung künftiger Datenschutzverstöße und habe davon abgesehen, über eine Verwarnung hinaus weitere Maßnahmen zu ergreifen.

Was ist zu tun?

Eine Behörde darf personenbezogene Daten nur auf gesetzlicher Grundlage abrufen und verarbeiten. Ob eine solche Grundlage und deren Voraussetzungen vorliegen, ist seitens der Behörde vor dem Abruf und der Verarbeitung zu prüfen.

2.2.25 Aufzeichnung von Telefongesprächen durch eine Behörde

↗ § 4 Abs. 1 Nr. 2 SächsDSDG, Art. 6 Abs. 1 Buchst. a und f DSGVO

Wie bereits in den vergangenen Jahren erreichte mich der Hinweis eines Petenten, dass Telefonate aufgezeichnet werden. Bei einem Anruf bei einer öffentlichen Stelle, einer SGB-Stelle, wurde zunächst eine Warteschlange aktiviert. Anschließend erfolgte ein automatisierter Hinweis, dass das Gespräch aufgezeichnet werde. Eine Einwilligung des Betroffenen wurde vor der Aufzeichnung nicht eingeholt. Ein späterer Widerspruch war erfolglos, da der Mitschnitt nicht unterbrochen werden konnte.

Die Behörde teilte mit, dass die Aufzeichnung der Telefonate nicht zur Qualitätssicherung oder der Kontrolle der Beschäftigten der öffentlichen Stelle erfolge, sondern zu deren Schutz. Im Jahr 2017 habe die SGB-Stelle eine Bombendrohung erhalten. Ebenso wurden Beschäftigte telefonisch persönlich bedroht.

Eine Behörde kann sich im Rahmen ihrer Aufgabenerfüllung nicht auf Art. 6 Abs. 1 Buchst. f Datenschutz-Grundverordnung (DSGVO) berufen. Nach Art. 6 Unterabsatz 2 DSGVO gilt Unterabsatz 1 Buchst. f nicht für die von Behörden in Erfüllung ihrer Aufgabe vorgenommene Verarbeitung. Erwägungsgrund 47 Satz 5 zur DSGVO lautet: „Da es dem Gesetzgeber obliegt, per Rechtsvorschrift die Rechtsgrundlage für die Verarbeitungen personenbezogener Daten durch die Behörden zu schaffen, sollte diese Rechtsgrundlage nicht für Verarbeitungen durch Behörden gelten, die diese in Erfüllung ihrer Aufgaben vornehmen."

Das Hausrecht als Annexkompetenz auf der Grundlage von Art. 6 Abs. 1 Buchst. e DSGVO steht dem jeweiligen Verwaltungsträger zu, um den Zugang zu und das Verweilen in Verwaltungsgebäuden zu regeln. Das Hausrecht und die Möglichkeit, dies zu regeln, ergibt sich aus der sogenannten Annexkompetenz des Behördenleiters. Auf der Grundlage des Hausrechts können auch andere Ordnungsmaßnahmen erlassen werden. Die Regelung, dass alle Telefonate mit der SGB-Stelle auf-

gezeichnet werden, könnte eine Ordnungsmaßnahme auf der Grundlage des Hausrechts sein.

Jede auf der Grundlage des Hausrechts getroffene Maßnahme muss einen legitimen Zweck verfolgen, geeignet und erforderlich sein, um diesen Zweck zu erreichen und in einem angemessenen Verhältnis zu gegebenenfalls beeinträchtigten (Grund-)Rechten stehen.

Es ist davon auszugehen, dass Telefonate der SGB-Stelle nur mit Personen geführt werden, die ihren Namen sowie ihre Identifikationsnummer (Kundennummer) angegeben haben, damit deren Identität geklärt werden kann, bevor ein Gespräch beginnt. Selbst bei einem Telefonat, das zum Beispiel nur einer Terminverschiebung dient, werden personenbezogene Daten, gegebenenfalls sogar Sozialdaten, ausgetauscht.

Plant eine Person von vornherein eine Drohung auszusprechen, wird sie sich nicht mit ihrem Klarnamen zu Beginn des Telefonats melden. Insoweit bleibt als Anhaltspunkt die Telefonnummer. Falls diese nicht unterdrückt wurde, ist sie auch ohne Aufzeichnung erkennbar.

Durch die Aufzeichnungen werden keine neuen Erkenntnisse über den Anrufer gewonnen. Dies wäre auch durch einen Vermerk des Beschäftigten zum Telefonat möglich. Die generelle Aufzeichnung aller Telefonate ist folglich kein geeignetes Mittel. Hinzu kommt, dass die Aufzeichnung sämtlicher Telefonate der SGB-Stelle nicht erforderlich ist, da ein anderes milderes Mittel zur Verfügung steht. Es ist möglich, über das Telefonat einen Vermerk zu erstellen.

Die Verarbeitung kann auch nicht auf § 4 Abs. 1 Nr. 2 Sächsisches Datenschutzdurchführungsgesetz gestützt werden, da keine konkreten Anhaltspunkte vorliegen, die eine Gefährdungslage einer tatsächlichen schwerwiegenden Beeinträchtigung rechtfertigen.

Die angeführte Bombendrohung liegt bereits sechs Jahre zurück. Die übrigen Drohungen sind nicht substanziiert dargelegt. Entscheidend könnte beispielsweise eine Häufung solcher Drohungen im Zeitraum vor Beginn der Aufzeichnungen sein. Hinzu kommt, dass die Aufzeichnung eines Telefonats nicht als taugliches Mittel zur Abwehr einer schwerwiegenden Be-

einträchtigung dient. Durch die Aufzeichnungen werden keine neuen Erkenntnisse über den Anrufer gewonnen. Aus der Bombendrohung, dem einmaligen und weit zurückliegenden Ereignis, ergab sich jedoch keine aktuelle Bedrohungslage. Selbst wenn eine konkrete Bedrohung am Telefon ausgesprochen wird, ist Aufzeichnung des Telefonats nicht zur Verhütung geeignet. Die Person, die eine Bedrohung aussprechen will, wird ihren Namen nicht nennen. Das Gespräch wird keine Erkenntnisse über die Person bringen. Zudem ist die Abschreckungswirkung der bloßen Ankündigung, dass das Gespräch aufgezeichnet werde, als gering einzuschätzen.

Damit besteht als rechtlich zulässige Möglichkeit der Aufzeichnung von Telefonaten nur die vorherige Einwilligung im Sinn des Art. 6 Abs. 1 Buchst. a DSGVO. Zu den Anforderungen an eine wirksame Einwilligung verweise ich auf meinen Tätigkeitsbericht 2022 (2.3.2, Seite 99 ff.).

Tätigkeitsbericht Datenschutz 2022:
↗ sdb.de/tb2022

Die Behörde wurde von mir aufgefordert, ab sofort die Aufzeichnung von Telefonaten einzustellen, soweit keine vorherige Einwilligung nach Art. 6 Abs. 1 Buchst. a DSGVO erteilt wurde.

Die noch vorliegenden Mitschnitte von Telefonaufzeichnungen waren umgehend zu löschen. Die Beendigung der Aufzeichnung der Telefonate sowie die umgehende Löschung der Mitschnitte der Telefonate wurden mir schriftlich bestätigt. Die Behörde ist der Aufforderung umgehend nachgekommen.

Was ist zu tun?
Eine Behörde darf Telefonate nicht ohne vorherige Einwilligung des Betroffenen aufzeichnen.

2.2.26 Datenverarbeitung im Rahmen des Leistungsbezugs nach dem SGB II bei Bezug von Pflegegeld

↗ EStG, SGB II

Ein Petent war der Auffassung, dass an ihn gezahltes Pflegegeld nicht auf seine Leistungen nach dem Zweiten Buch Sozialgesetzbuch (SGB II) angerechnet und die Optionskommune daher hierzu auch keine Angaben von ihm erheben darf. Streitig war insbesondere die Frage, ob der Petent die von ihm gepflegte Person benennen muss.

Meine Prüfung ergab:

Allein der Nachweis, Pflegeperson zu sein, genügt nicht. Maßgeblich ist für die Frage der (Nicht-)Anrechnung, ob es sich bei der Pflegeperson um eine Angehörige bzw. einen Angehörigen oder – nur – um einen sonstigen Dritten handelt bzw. ob für die Pflegeperson eine sittlich-moralische Verpflichtung im Sinne des § 33 Absatz 2 Einkommensteuergesetz zur Pflege des Pflegebedürftigen besteht, das heißt Pflegeperson und pflegebedürftige Person in einem engen Verhältnis zueinanderstehen, allerdings nicht zwangsläufig miteinander verwandt sind.

Diese entscheidungserhebliche Feststellung zu treffen obliegt einer Einzelfallfeststellung der verantwortlichen Stelle und kann im Ergebnis nur festgestellt werden, so die zu pflegende Person zweifelsfrei bekannt ist.

Hinweis: Optionskommunen sind die sächsischen Landkreise, die die Aufgaben nach dem SGB II ohne die Bundesagentur für Arbeit eigenverantwortlich betreiben und daher meiner aufsichtlichen Zuständigkeit unterliegen. Das betrifft – nur – die Landkreise Bautzen, Görlitz, Leipzig, Meißen und den Erzgebirgskreis.

Für alle anderen Jobcenter auf dem Gebiet des Freistaates Sachsen ist der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit die zuständige Aufsichtsbehörde.

Was ist zu tun?
Für die Frage der Anrechnung von Pflegegeld auf Leistungen nach dem SGB II ist auch die Benennung der zu pflegenden Person maßgeblich.

2.2.27 Nutzung von Versichertendaten durch die Krankenkasse zwecks Impfaufruf

↗ SGB V

Ein Petent hatte sich an mich gewandt, nachdem er Post von seiner Krankenkasse erhalten hatte. Diese hatte an ihn ein Schreiben des Bundesministeriums für Gesundheit (BMG) weitergereicht, einen Impfaufruf an über 60-Jährige betreffend. Dem Schreiben des BMG war für mich zu entnehmen, dass die Krankenversicherung gebeten worden war, dem Betroffenen das Schreiben zuzusenden. Es war zudem ersichtlich, dass keine Übermittlung personenbezogener Daten zu seiner Person seitens der Krankenkasse an das Bundesministerium

erfolgt war, vielmehr die Adress- und Altersangaben aus dem Datenbestand der Krankenkasse stammten, diese das BMG-Schreiben personalisiert und zwecks Versand mit Adressdaten versehen hatte.

Dem Betroffenen, der sich gegen diese – in datenschutzrechtlicher Hinsicht als Nutzung seiner Versichertendaten einzuordnende – Datenverarbeitung gewandt hatte, habe ich wie folgt geantwortet:

Mit § 20i Abs. 4 Satz 2 Fünftes Buch Sozialgesetzbuch (SGB V) wurde durch den Gesetzgeber eine Rechtsgrundlage zur versichertenbezogenen Ansprache für Informationen über Impfungen geschaffen. Diese Regelung stellt eine Ermächtigung gemäß § 284 Abs. 3 Satz 1 SGB V dar: Danach dürfen rechtmäßig erhobene und gespeicherte versichertenbezogenen Daten für die Zwecke der Aufgaben nach Absatz 1 der Vorschrift in dem jeweils erforderlichen Umfang verarbeitet werden, allerdings wie hier, aber auch für andere Zwecke, soweit dies durch Rechtsvorschriften des Sozialgesetzbuchs angeordnet oder erlaubt ist, was mit § 20i Abs. 4 Satz 2 SGB V geschehen ist.

Was ist zu beachten?
Mit § 20i Abs. 4 Satz 2 SGB V wurde eine Rechtsgrundlage zur versichertenbezogenen Ansprache für Informationen über Impfungen geschaffen.

Ein datenschutzwidriges Verhalten der Krankenkasse war also nicht festzustellen.

2.2.28 Bereitstellung von Eigentümerdaten für Windenergieanlagenunternehmen

↗ § 11 Abs. 2 Satz 4 SächsVermKatG

Projektentwickler von Windenergieanlagen schließen zur Aufstellung von Windrädern Pachtverträge mit Eigentümerinnen und Eigentümern über hierzu geeignete Flächen. Dabei müssen sie aber zunächst wissen, wer denn Eigentümer/in ist. Ich erhielt in diesem Zusammenhang die Anfrage, unter welchen Voraussetzungen das Liegenschaftskataster (geführt vom Staatsbetrieb Geobasisinformation und Vermessung) Auskünfte zu Eigentumsverhältnissen geben muss bzw. darf. Hierzu bedarf es laut Gesetz eines „berechtigten Interesses" des Windkraftunternehmens nach § 11 Abs. 2 Satz 4 Sächsisches Vermessungs- und Katastergesetz (SächsVermKatG).

16. Tätigkeitsbericht für den öffentlichen Bereich:
↗ sdb.de/tb16oeb

Ursprünglich sah das Sächsische Staatsministerium des Inneren (SMI) erst dann das berechtigte Interesse als gegeben an, wenn für die Errichtung einer Windenergieanlage im betreffenden Gebiet bereits von der zuständigen Umweltbehörde eine immissionsschutzrechtliche Genehmigung erteilt worden ist – nicht jedoch vorher. Diese Auffassung teilte auch mein Amtsvorgänger, wie im 16. Tätigkeitsbericht (5.14.1, Seite 68 f.) berichtet.

Mittlerweile musste ich diese Auffassung aber ändern, insbesondere vor dem Hintergrund einer hierzu zwischenzeitlich ergangenen Entscheidung des Verwaltungsgerichts Dresden vom 06.11.2019 (AZ 4 K 5232/17) und eines veröffentlichten Leitfadens des Sächsischen Staatsministeriums für Regionalentwicklung (SMR) zur Handhabung von Auskünften vom 29. Juli 2020. Das SMR hat die Zuständigkeit für das Liegenschaftskataster vom SMI übernommen.

Hintergrund der Entscheidung war folgender: Ein Windkraftunternehmen hat am Verwaltungsgericht (VG) Dresden Klage gegen einen Ablehnungsbescheid des Freistaates Sachsen eingelegt, der die Eigentümerdaten aus dem Kataster nicht vor Erteilung einer immissionsschutzrechtlichen Genehmigung gewährte. Mit hierauf ergangenem oben genanntem Urteil hat das Verwaltungsgericht Dresden die bestehende Rechtsansicht des SMI verworfen.

In diesem Urteil wird das berechtigte Interesse des Projektträgers im Sinne des § 11 Abs. 2 Satz 4 SächsVermKatG auch schon dann bejaht, wenn die Eigentümerangaben erst zur Anbahnung von Verhandlungen bzw. vorgelagert zur Klärung der Verkaufsbereitschaft der jeweiligen Eigentümerin bzw. des jeweiligen Eigentümers benötigt werden. Auch die Tatsache, dass sich ein entsprechender Regionalplan noch in der Aufstellungsphase befindet, steht dem berechtigten Interesse der Klägerin nicht entgegen, so das VG Dresden.

Demnach sollen die Vermessungsbehörden das „berechtigte Interesse" bereits in einem frühen Planungsstadium bejahen, wenn ermittelt werden soll, ob Eigentümer/innen ihre Grundstücke für eine Windenergienutzung zur Verfügung stellen würden, mithin die Eigentümerdaten für die Planung

und Durchführung von Windenergieanlagenprojekten in einem planerischen Anfangsstadium erforderlich sind.
Nur wenn im Zeitpunkt der Antragstellung feststeht, dass eine immissionsschutzrechtliche Genehmigung nach diesem Stand von vornherein ausgeschlossen ist, weil damit das Ziel der Errichtung und des Betriebs von Windenergieanlagen, mithin auch die Notwendigkeit der Kenntnis von Eigentümerdaten entfällt, ist das „berechtigte Interesse" abzulehnen. Ein solcher Fall liegt zum Beispiel vor, wenn sich die vorgesehene Errichtung von Windenergieanlagen im weiteren Grenzbereich außerhalb eines im Regionalplan ausgewiesenen Vorrang- und Eignungsgebietes befindet.
Anhand dieser Rechtsprechung folgte sodann ein entsprechender „Handlungsleitfaden zur Bereitstellung von Eigentümerdaten des amtlichen Vermessungswesens für private Nutzer, speziell für Windenergieanlagenunternehmen". Dieser wurde an die unteren Vermessungsbehörden versendet. Es wurden die vom VG aufgestellten Voraussetzungen an das „besondere Interesse" aufgenommen. Im Wesentlichen kann man vereinfachend festhalten, dass Auskünfte aus dem Liegenschaftskataster dann zulässig sind, wenn die begehrte Fläche sich in dem im Regionalplan ausgeschriebenen Vorranggebiet befindet. Datenschutzrechtliche Bedenken konnte ich gegen den derzeit geltenden Handlungsleitfaden des SMR nicht erkennen.
Ein Windkraftunternehmen äußerte sich indes mir gegenüber skeptisch, ob auch die neuerliche Auslegung nicht zu eng bemessen sei und Auskünfte auch dann erfolgen sollen, wenn Windkraftprojekte sich außerhalb von Vorrang- und Eignungsgebieten nach dem Regionalplan befinden. Ich musste hierzu darauf hinweisen, dass diese Frage nicht in meine Zuständigkeit fällt. Hier kommt es auf die Auslegung des § 11 Abs. 2 Satz 4 SächsVermKatG, dort insbesondere der Reichweite des „besonderen Interesses", an. Dies ist eine Frage, die nach dem Fachrecht, nicht nach dem Datenschutzrecht zu beantworten ist.
Ob der Handlungsleitfaden noch mit dem Datenschutzrecht vereinbar sein sollte, sollte die Reichweite des Begrif-

Was ist zu tun?
Das berechtigte Interesse im Sinne des § 11 Abs. 2 Satz 4 SächsVermKatG als Schranke des Rechts auf informationelle Selbstbestimmung ist am Einzelfall zu entscheiden.

fes „besonderes Interesse" noch weiter gefasst werden, kann nicht „im Voraus" beantwortet werden. Es 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.

2.2.29 Fingerabdruckpflicht bei Beantragung von Personalausweisen laut Verordnung (EU) 2019/1157

Aufgrund der „Verordnung (EU) 2019/1157 des europäischen Parlaments und des Rates vom 20. Juni 2019 zur Erhöhung der Sicherheit der Personalausweise von Unionsbürgern und der Aufenthaltsdokumente, die Unionsbürgern und deren Familienangehörigen ausgestellt werden, die ihr Recht auf Freizügigkeit ausüben – Verordnung (EU) 2019/1157" müssen ab dem 2. August 2021 bei der Beantragung von Personalausweisen EU-weit zwingend Fingerabdrücke abgegeben werden.

Auch wenn diese von den Pass- und Registerbehörden elektronisch nur auf dem Ausweis und in keiner zentralen Datenbank abgespeichert werden dürfen, so ist diese Verordnung auch in Fachkreisen nicht unumstritten. Zudem wurde die Rechtmäßigkeit dieser Verordnung in einem Vorlageverfahren vor dem Europäischen Gerichtshof (EuGH) in Zweifel gezogen, Rechtssache EuGH C-61/22, vorgelegt vom Verwaltungsgericht Wiesbaden. Zum Zeitpunkt des Redaktionsschlusses dieses Tätigkeitsberichtes ist eine Entscheidung noch nicht verkündet worden.

Alle EU-Verordnungen sind in den EU-Mitgliedsstaaten unmittelbar geltendes Recht und müssen zwingend auch so umgesetzt werden. In der Bundesrepublik Deutschland wurde die Verordnung im Übrigen durch das „Gesetz zur Stärkung der Sicherheit im Pass-, Ausweis- und ausländerrechtlichen Dokumentenwesen" (verkündet im Bundesgesetzblatt I 2020, Nr. 60 vom 11.12.2020, Seite 2744) eingeführt.

Im Berichtszeitraum erreichte mich hierzu nun eine Anfrage aus der Bevölkerung, ob denn die Abgabe der Fingerabdrücke auf irgendeinem Weg umgangen werden kann, da dem EuGH die Verordnung zur Prüfung vorgelegt wurde.

Zunächst musste ich den Bürger darauf verweisen, dass das Verfahren vor dem EuGH keine aufschiebende Wirkung entfaltet. Dies bedeutet, dass trotz der Vorlagefrage die oben genannte Verordnung derzeit geltendes Recht ist und die Ausweisbehörden verpflichtet sind, dieses auszuführen. Das derzeit anhängige Verfahren steht der Wirksamkeit der Verordnung deswegen nicht entgegen.

Eine aufschiebende Wirkung wurde indes durch das Verwaltungsgericht Hamburg geschaffen. Auf einen Antrag hin hatte das Verwaltungsgericht (VG) Hamburg in einem einstweiligen Verfahren ein Anordnungsbeschluss erlassen (VG Hamburg – 20 E 377/23). Dieser Beschluss bestimmt, dass Hamburger Bürger/innen – folgend der Vorlagefrage an den EuGH – vorläufig nicht zur Abgabe von Fingerabdrücken bei der Ausstellung eines neuen Personalausweises gezwungen werden können, und zwar so lange nicht, bis der EuGH entweder die Wirksamkeit der Verordnung feststellt oder diese verwirft.

Dieser Beschluss entfaltet allerdings außerhalb des Bundeslands Hamburg für die sonstigen Bundesländer keine Rechtswirkung.

Dem anfragenden Bürger wurde von der zuständigen Passbehörde angeboten, einen vorläufigen Personalausweis zu beantragen, der jedes Quartal verlängert werden müsste, solange die Frage vom EuGH nicht entschieden wurde.

Etwas anderes konnte ich dem Fragesteller auch nicht mitteilen oder raten. Einzig würde ihm verbleiben, einen Antrag im einstweiligen Verfahren an das zuständige Verwaltungsgericht zu bringen – wie in Hamburg geschehen – und eine aufschiebende Wirkung der Verordnung zu erwirken. Dies würde indes wiederum nur im Zuständigkeitsgebiet des Verwaltungsgerichtes wirken.

Bei gerichtlicher Durchsetzung darf ich zudem als unabhängige Aufsichtsbehörde bereits per Gesetz keine Klagen/Anträge unterstützen. Den Fragesteller musste ich deswegen auf an-

Was ist zu tun?
Bei der Durchsetzung subjektiver Rechte der Bürgerinnen und Bürger muss ich als unabhängige Aufsichtsbehörde auf anwaltliche Hilfe oder Interessenvertretungen verweisen.

waltliche Hilfe verweisen, wenn er denn ernsthaft gegen die Fingerabdruckpflicht vorgehen möchte.

2.3 Einwilligungsfragen

2.3.1 Wirtschaftliche bzw. berechtigte Interessen des Eigenbetriebs bei der Datenverarbeitung

↗ Art. 6 Abs. 1 Buchst. f DSGVO, Art. 6 Abs. 1 Unterabsatz 2 DSGVO

Eine Frage zu einem (Kultur-)Eigenbetrieb bestand darin, ob sich dieser auf den Erlaubnistatbestand zur Datenverarbeitung nach Art. 6 Abs. 1 Buchst. f DSGVO berufen kann. Hiernach ist die 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, die den Schutz personenbezogener Daten erfordern, überwiegen". Nach Art. 6 Abs. 1 Unterabsatz 2 DSGVO gilt die vorbenannte Regelung aber wiederum nicht für die von Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung.
Der Eigenbetrieb wollte die bereits aus vergangenen Ticketerwerben bekannten und gespeicherten Daten dafür nutzen, um Angebotsflyer und Abo-Werbeangebote zu verteilen. Ich habe der betroffenen Gemeinde indes mitteilen müssen, dass dies datenschutzkonform nur nach Einholung einer Einwilligung möglich ist. Der Kultureigenbetrieb ist schließlich Teil der öffentlichen Verwaltung.
Auch hilft an dieser Stelle nicht weiter, dass auch Öffentlichkeitsarbeit als Aufgabe von öffentlichen Stellen anerkannt ist. Öffentlichkeitsarbeit in diesem Sinne meint vielmehr Information der Bürgerschaft zur behördlichen Tätigkeit in einer Art Transparenz und Informationsfreiheit, nicht den Versand von Werbung.
Öffentliche Stellen, somit auch der Eigenbetrieb, können sich höchstens für privatrechtliche Hilfsgeschäfte auf Art. 6 Abs. 1 Buchst. f DSGVO stützen, soweit dies nach der betreffenden

nationalen Rechtsordnung zulässig ist und die Behörde in gleicher Weise wie private Akteure am Privatrechtsverkehr teilnimmt. Hierunter zählen indes Geschäfte zur Mittelbeschaffung oder etwa zur Anmietung von Räumlichkeiten etc., nicht der hier vorgestellte Sachverhalt.

Dem Eigenbetrieb konnte deswegen nur mitgeteilt werden, dass der personalisierte Versand des Werbe- bzw. Infomaterials ausschließlich nach Einwilligung erfolgen kann. Einer Einwilligungslösung steht dem Kultureigenbetrieb hier im Fall der Werbung die ansonsten im öffentlichen Bereich kritisch zu hinterfragende Voraussetzung der Freiwilligkeit zudem nicht entgegen.

Eine abweichende Wertung wäre dann geboten, wenn die Einrichtung nicht als Eigenbetrieb, sondern als Gemeindeunternehmen in privatrechtlicher Rechtsform betrieben würde.

Was ist zu beachten?
Anders als privatrechtlich organisierte (Kommunal-)Unternehmen sind Eigenbetriebe auch datenschutzrechtlich konsequent als öffentliche Stellen zu betrachten.

2.3.2 Versendung von Elternbriefen durch den Deutschen Kinderschutzbund

↗ §§ 8, 46 Abs. 1 BMG; § 16 SGB VIII, Art. 6 Abs. 1 Buchst. a DSGVO

Eine interessante Anfrage erreichte mich von einer größeren sächsischen Stadt zum Thema Elternbriefe des Deutschen Kinderschutzbundes (DKSB). Diese Briefe enthalten Informationen zur Unterstützung der Eltern, seien es Empfehlungen zur Entwicklungsförderung oder Unterstützung zu schwierigen Lebens- oder Krisensituationen. Zudem werden Anregungen zur Lösung von Problemen, die in jeder Familie vorkommen können, gegeben, und es werden Ansprechpartner/innen benannt, die in bestimmten Angelegenheiten weiterhelfen können. Insgesamt gibt es vom DKSB 46 dieser Briefe, jeweils passend für einzelne Altersabschnitte (vom ersten bis zum achten Lebensjahr).

Dieses Angebot des DKSB ist auch im Sinne der Stadt, insbesondere im Hinblick auf den Allgemeinen Förderauftrag zur Erziehung in der Familie nach § 16 Achtes Buch Sozialgesetzbuch (SGB VIII). Ziel ist es hier, das Verantwortungsbewusstsein junger Eltern unter anderem mittels einer breitgefächerten Aufklärungs- und Informationsarbeit zu

unterstützen. Die Stadt unterhält hierzu auch eine Kooperation mit dem DKSB. Die ersten drei Briefe werden mit der Begrüßungsmappe auf dem Standesamt den Eltern überreicht.
Datenschutzrechtlich problematisch wird es nun ab dem Moment, in dem die Zusendung der weiteren Briefe an die Familie durch den DKSB automatisch und unaufgefordert erfolgt. Hierfür erhält der Verein die Familiennamen und die aktuelle Anschrift der Kindsmütter aller neugeborenen und gemeldeten Kinder, soweit es sich um Erstgeborene handelt, aus dem Melderegister. Hierzu bedarf es der Erteilung von Melderegisterauskünften durch die Stadt als örtliche Meldebehörde. Die rechtlichen Voraussetzungen hierfür sind gesetzlich genau vorgegeben und dürfen nicht überschritten werden. Deswegen halte ich das Vorgehen der Stadt in diesem Fall nicht für datenschutzkonform.
Die Stadt gibt als Rechtsgrundlage für diese Datenübermittlungen die Norm des § 46 Abs. 1 Bundesmeldegesetz (BMG) – Gruppenauskünfte – an. Nach dieser Norm ist es zulässig, eine Melderegisterauskunft über eine Vielzahl nicht namentlich bezeichneter Personen (Gruppenauskunft) zu erteilen, wenn sie im öffentlichen Interesse liegt. Die Gruppenzusammensetzung darf zudem allein nach den Kriterien gemäß § 46 Abs. 1 BMG erfolgen.
Ein öffentliches Interesse wird dann angenommen, wenn der Zweck der Anfrage über die Belange einer Person oder einer Gruppe hinausgeht, sie im Interesse der Allgemeinheit liegt und es sich außerdem um ein innerstaatliches öffentliches Interesse handelt. Zudem darf die Auskunft, gemessen an ihrer Eignung und ihrer Erforderlichkeit zu dem vorgesehenen Zweck, die betroffene Person nicht unverhältnismäßig belasten, § 8 BMG.
Der Begriff des öffentlichen Interesses ist ein sogenannter unbestimmter Rechtsbegriff, der einer Interpretation und Auslegung zugänglich ist. Die Stadt hat mich nun gebeten, hierzu Stellung zu beziehen, da hiervon auch die Rechtmäßigkeit der bisherigen Praxis abhängt. Die Stadt hatte Schwierigkeit bei einer eigenen rechtlichen Einschätzung, da hierzu auch in den Aufsichtsbehörden der Bundesländer verschiedene Ansichten

vertreten werden. Die Schlüsselfrage war daher, ob bei rein karitativen Zwecken ein öffentliches Interesse im Sinne von § 46 BMG angenommen werden kann.
Zur Beantwortung habe ich mich zunächst auf die entsprechende Gesetzesbegründung bezogen (Gesetzentwurf der Bundesregierung Entwurf eines Gesetzes zur Fortentwicklung des Meldewesens (MeldFortG) – BT-Drs. 17/7746, Seite 45):

> „Ein öffentliches Interesse liegt vor, wenn der Zweck der Anfrage über die Belange einer Person oder einer Gruppe hinausgeht und im Interesse der Allgemeinheit liegt. Außerdem muss es sich um ein innerstaatliches öffentliches Interesse handeln. Im öffentlichen Interesse können beispielsweise Untersuchungen oder Tätigkeiten der Forschung und Wissenschaft sowie Maßnahmen der Gesundheitsvorsorge liegen. In Absatz 1 Satz 2 Nummer 6 wird genauer differenziert, welche Angaben zum Familienstand für die Zusammensetzung der Personengruppen bei einer Auskunft über eine Vielzahl nicht namentlich bezeichneter Personen herangezogen werden dürfen."

Auch wenn die Aufzählung nicht abschließend ist, so kann ich nicht ersehen, dass die hier verfolgten karitativen Zwecke – Informationsbereitstellung zur Verbesserung der Lebenschancen der Kinder – einen ähnlich hohen Stellenwert einnehmen können wie Forschungszwecke oder Zwecke der Gesundheitsvorsorge.
Ohne die sozialgesellschaftliche Bedeutung dieser Informationskampagne zu verkennen, ist auch nicht aus den Augen zu verlieren, dass durch Gruppenauskünfte eine Vielzahl an Meldedatensätzen an nichtstaatliche Organisationen übermittelt werden und deswegen die Eingriffsvoraussetzungen hier entsprechend hoch sein müssen.
In Bayern beispielsweise wird dieses Problem auf landesgesetzlicher Ebene gelöst – nach § 8 der bayerischen Verordnung zur Übermittlung von Meldedaten ist eine regelmäßige Übersendung der Daten Neugeborener an die Jugendäm-

ter vorgesehen, die dann die Versendung der „Elternbriefe" übernehmen können.
So musste ich feststellen und der anfragenden Stadt auch mitteilen, dass für derartige Datenverarbeitung eine gesetzliche Rechtsgrundlage fehlt. Die Versendung solcher Briefe – wie jede Datenverarbeitung, die auf keine Rechtsgrundlage gründet – kann nur erfolgen, wenn eine ausdrückliche Einwilligung von der betroffenen Person vorliegt, Art. 6 Abs. 1 Buchst. a Datenschutz-Grundverordnung.
Ich habe der Stadt empfohlen, die Einholung der Einwilligung mit der bereits oben erwähnten Ausgabe der Begrüßungsmappe des Standesamtes zu verbinden, so könnte das Einwilligungsformular in die Mappe gelegt werden, verbunden mit einem Hinweis des Standesamtes.

Was ist zu tun?
Kommunen sollten genau prüfen, ob tatsächlich eine Rechtsgrundlage zur Datenübermittlung vorliegt, und dies nicht vorschnell annehmen. Ein noch so wohlgemeinter, karitativer Zweck ersetzt keine Rechtsgrundlage.

2.3.3 Einwilligung bei Schulversuch

↗ Art. 7 Abs. 3, Art. 58 Abs. 2 Buchst. d DSGVO

Mehrere Petenten wiesen mich darauf hin, dass sie von ihrer Schule aufgefordert worden wären, eine Vereinbarung zu unterzeichnen, die eine generelle Foto- und Videoerlaubnis sowie eine entsprechende Nutzungsgenehmigung für Öffentlichkeitsarbeit enthält. Diese soll nur aus wichtigem Grund widerruflich sein. Für den Fall einer Nichtunterzeichnung wurde eine Schulversetzung angedroht.
Gemäß Art. 7 Abs. 3 Datenschutz-Grundverordnung (DSGVO) haben betroffene Personen in jedem Fall das Recht, ihre Einwilligung jederzeit zu widerrufen. Eine Beschränkung auf einen wichtigen Grund ist daher unzulässig. Weiterhin hat eine Einwilligung nach Art. 4 Nr. 11 DSGVO freiwillig zu erfolgen. Sie darf nach Art. 7 Abs. 4 DSGVO nicht mit anderen Verträgen gekoppelt werden. Hiergegen wurde mit der Androhung einer Schulversetzung verstoßen.
Schließlich schreibt Nr. II. 5. c) VwV Schuldatenschutz für die Einwilligung in eine Veröffentlichung von personenbezogenen Daten, Fotos, Videos oder Filmen zwingend die Verwendung eines bestimmten Musters vor. Dieses wurde jedoch vorliegend nicht verwendet.

Die von mir zur unverzüglichen Rücknahme der Androhung einer Schulversetzung sowie zur Stellungnahme aufgeforderte Schulleitung ging in ihrer Antwort offensichtlich davon aus, dass sie wegen ihres Status als Schulversuch (gemäß § 7a SchulG) einer staatlichen Gemeinschaftsschule und der dabei „gelebten Dynamik" sowie der über die Grenzen der Bundesrepublik hinaus beobachten und rezipierten intensiven Begleitforschung nicht an (europa-)rechtliche Vorgaben gebunden sei. Für die wenigen Eltern, die die Dynamik und die sonstigen Herausforderungen des Schulversuches bei der Anmeldung ihrer Kinder unterschätzt haben oder aus anderen Gründen nicht mittragen wollen, hätte man zwar großes Verständnis; für diese Eltern sei diese Schule jedoch nicht der richtige Ort.

Angesichts dieser offen zur Schau getragenen Unkenntnis der für sie einschlägigen rechtlichen Rahmenbedingungen habe ich mich an das Sächsische Staatsministerium für Kultus als Aufsicht gewandt. Dieses forderte schließlich die betroffene Schule auf, meinen Aufforderungen nachzukommen, also den fraglichen Text aus dem Schulvertrag herauszunehmen, das Muster für die Einwilligung aus der VwV Schuldatenschutz zu verwenden und den Schulbesuch nicht von dieser freiwilligen Einwilligung abhängig zu machen.

Leider erreichten mich auch danach weitere Beschwerden wegen eines anschließenden Schreibens an die „Schul-Gemeinschaft": Wer nicht gefilmt werden möchte oder darf, kann demnach immer Bescheid sagen und soll am besten einfach hinter der Kamera bleiben. Auch sollen die Sorgeberechtigten mit ihren Kindern darüber sprechen, wie sie sich verhalten möchten, wenn eine Kamera dabei ist.

Ich habe die Schule darauf hingewiesen, dass sie geeignete organisatorische Maßnahmen zu treffen hat, um sicherzustellen, dass nur Daten von einwilligenden Schülern verarbeitet werden. Nicht ausreichend dafür ist, dass es zum einen in der Verantwortung der Kinder liegt, zu entscheiden, ob sie gefilmt werden oder nicht (die Einwilligung ist durch die Personensorgeberechtigten zu erteilen), und zum anderen die nicht einwilligenden Sorgeberechtigten Sorge dafür zu tragen haben, dass ihre Kinder nicht gefilmt werden. Es ist vielmehr

Was ist zu beachten?
Auch innovative Schulformen befreien nicht von der Einhaltung datenschutzrechtlicher Vorgaben. So ist eine Datenverarbeitung außerhalb des Erziehungs- und Bildungsauftrags grundsätzlich nur mit Einwilligung möglich, die selbstverständlich auch verweigert werden kann. In diesem Fall muss durch die Schule dafür Sorge getragen werden, dass keine Datenverarbeitung stattfindet.

die Verantwortung der Schule, sicherzustellen, dass nur Kinder mit wirksamer Einwilligung gefilmt werden.
Nachdem als Antwort lediglich ein Gespräch angeboten wurde, habe ich ein Verfahren zu einer Anweisung nach Art. 58 Abs. 2 Buchst. d DSGVO gestartet, geeignete organisatorische Maßnahmen dahingehend zu treffen, dass bei fehlender Einwilligung keine Daten von Schülern zu Dreharbeiten für Fernsehbeiträge verarbeitet werden.

2.3.4 Wohnungsfotos beim Immobilienverkauf rechtskonform verwenden

↗ Art. 4 Nr. 1, 2 und 7 DSGVO; Art. 5 Abs. 2, Art. 6 Abs. 1 Buchst. a, Art. 7, Art. 17 Abs. 1 Buchst. b DSGVO

Nachdem sich der Inhaber einer vermieteten Eigentumswohnung zum Verkauf entschlossen hatte, bekamen die Mieter eines Tages Besuch von einem Mitarbeiter des von diesem mit der Vermarktung beauftragten Maklerunternehmens. Sie ließen sich am Ende von diesem überzeugen, dass er Fotos von der Mietwohnung anfertigt, um diese in der Wohnungsbeschreibung (Exposé) zu verwenden. Vereinbart wurde nach Darstellung der Mieter allerdings, dass ihnen die Bilder vor deren Veröffentlichung zur Ansicht und Freigabe vorgelegt werden, also nur Bildmaterial verwendet wird, in das sie zuvor ausdrücklich eingewilligt haben.
Kurze Zeit später erhielten die Mieter schließlich die Information über den Vermarktungsstart der Immobilie. Als sie daraufhin die Internetseite des Maklerunternehmens aufriefen, fanden sie dort auch tatsächlich das Exposé ihrer Mietwohnung. Mit Erstaunen mussten sie jedoch bei genauerem Hinschauen feststellen, dass darin auch ein Bild ihrer Küche mit dem Abwasch, Küchenutensilien und der Kücheneinrichtung zu sehen war. Sie befürchteten, dass das Exposé auch weitere Bilder der Mietwohnung enthielt. Für den Zugang zu den genaueren Wohnungsdetails hätten sie jedoch beim Maklerunternehmen ein offizielles Kaufinteresse signalisieren müssen, da sie von diesem nicht anders als „normale" Wohnungsinteressenten betrachtet wurden. Indes waren sie nicht bereit, nur deshalb

mehrere Formulare auszufüllen und ein nicht vorhandenes Kaufinteresse vorzutäuschen, nur um herauszufinden, ob noch weitere Innenaufnahmen ihrer Wohnung in dem Exposé verwendet wurden. Dies veranlasste die Bewohner schließlich dazu, meine Behörde hier um Hilfe zu bitten.

Fotos der Inneneinrichtung einer (Miet-)Wohnung geben Einblicke in die persönlichen Lebensverhältnisse und damit die private Sphäre der Bewohner und Bewohnerinnen. Die angefertigten und im Besitz des Maklerunternehmens befindlichen Wohnungsbilder stellten somit eindeutig personenbezogene Daten dar (Art. 4 Nr. 1 Datenschutz-Grundverordnung [DSGVO]). Indem die Bildaufnahmen im Exposé verwendet und auf diese Weise für Außenstehende zugänglich gemacht wurden, ließ sich nicht nur für Kaufinteressenten, die einen Maklervertrag unterzeichnet hatten, sondern auch für sonstige interessierte Personen anhand der Beschreibung der Objektlage auf die konkrete Wohnung und letztlich die Identität der Wohnungsmieter schließen. Insofern sind derartige Fotos auch nicht mit den Standardbildern eines Möbelhauses – in einem Katalog oder Verkaufsprospekt – vergleichbar, wie mir das Maklerunternehmen glaubhaft machen wollte. Demnach lag auch in der Veröffentlichung der Bildaufnahmen eine Verarbeitung personenbezogener Daten.

Möchte der Eigentümer bzw. die Eigentümerin oder ein beauftragtes Maklerunternehmen also Bilder einer bewohnten Mietwohnung anfertigen und diese später in Verkaufsprospekten oder einem Exposé verwenden, um damit die Ausstattung und Details der Wohnung zu veranschaulichen und letzten Endes das Objekt auch besser vermarkten zu können, geht dies nur mit Einwilligung der Bewohner und Bewohnerinnen, Art. 6 Abs. 1 Buchst. a in Verbindung mit Art. 4 Nr. 7 und Art. 7 DSGVO.

In dem dargestellten Fall gab bereits das im Exposé frei zugängliche Bild genaue Einblicke in die Lebensumstände der Mieter. Zusammen mit den für jedermann im Internet einsehbaren Objektdetails des Wohnungsexposés war nicht auszuschließen, dass ein Rückschluss auf die zum Verkauf stehende Wohnung und damit die dort wohnhaften Mieter

möglich war, sodass auch die diesbezüglichen Vermarktungsaktivitäten eine Verarbeitung personenbezogener Daten zum Gegenstand hatten.

Das Befragen des Maklerunternehmens bestätigte zwar die Angaben der Bewohner, dass die Fotos mit deren Einwilligung zustande kamen. Der Mitarbeiter des Maklerunternehmens ging aber offensichtlich davon aus, dass sich diese auch auf die Verwendung der Bilder bei der Vermarktung der Immobilie bezog. Dies stand allerdings im Widerspruch zur Aussage der Bewohner. Damit schien es in diesem Punkt ein kommunikatives Missverständnis zwischen den beteiligten Parteien gegeben zu haben, welches sich im Nachhinein durch meine Behörde nicht aufklären ließ. Auch wenn es keine Formvorgaben für die Einwilligung gibt, empfiehlt sich allein zur Vermeidung von Fehlannahmen die Wahl der Schriftform, nicht zuletzt auch vor dem Hintergrund der gesetzlichen Nachweispflicht (Art. 5 Abs. 2 DSGVO). Mir blieb deshalb nichts anderes übrig, als den betroffenen Mietern mitzuteilen, dass ich einen Datenschutzverstoß nicht eindeutig und zweifelsfrei feststellen konnte, zumal in der Zwischenzeit die Wohnungsbilder aus dem Exposé entfernt wurden. Ein nachgewiesener Datenschutzverstoß wäre jedoch Voraussetzung gewesen, um überhaupt Maßnahmen nach Art. 58 Abs. 2 DSGVO gegenüber dem Maklerunternehmen zu ergreifen.

Da die Mieter noch Sorge hatten, dass die im Besitz des Maklerunternehmens befindlichen Fotos weiterverwendet werden und sich (auch) dies ihrer Kontrolle entzieht, verlangten sie dem Unternehmen gegenüber die umgehende Löschung der Bildaufnahmen. Unter datenschutzrechtlichen Gesichtspunkten lag in dem Löschungsbegehren implizit ein Widerruf der zuvor erteilten Einwilligung zur Anfertigung der Fotos. Da es für das Maklerunternehmen somit keinen Rechtsgrund (mehr) gab, der ihm die weitere Aufbewahrung der Wohnungsbilder gestattet hätte, konnten die Mieter auch zulässigerweise die Löschung verlangen (Art. 17 Abs. 1 Buchst. b DSGVO). Nach anfänglichem Widerstand lenkte das Maklerunternehmen schließlich auch in dieser Frage ein und bestätigte mir schriftlich die Löschung aller Innenaufnahmen der Wohnung.

Was ist zu beachten?

Fotoaufnahmen einer bewohnten Mietwohnung sind nicht mit Katalogaufnahmen oder Darstellungen in Werbeprospekten vergleichbar. Da sie im Regelfall die persönlichen Lebensverhältnisse der Bewohnerinnen und Bewohner wiedergeben, handelt es sich um personenbezogene Daten. Diese dürfen nur dann angefertigt und weiterverwendet werden, wenn hierzu eine wirksame datenschutzrechtliche Einwilligung vorliegt.

2.3.5 Werbeansprachen durch den Verwalter einer Wohnungseigentümergemeinschaft

↗ §§ 9b, 27 WEG; § 7 Abs. 3 UWG; Art. 5, 25 DSGVO

Nach einem Wechsel des Verwalters in einer Eigentümergemeinschaft nach dem Gesetz über das Wohnungseigentum und das Dauerwohnrecht (Wohnungseigentumsgesetz [WEG]) wandte sich ein Eigentümer beschwerdeführend an mich. Abweichend von bisherigen Gepflogenheiten nutzte der neue Verwalter den Zugriff auf die Daten der Eigentümer/innen, um diesen – unter anderem per E-Mail – neben Glückwünschen zu Feiertagen auch Informationen zum Immobilienmarkt und Geschäftsofferten zu unterbreiten.

Ich habe die Angelegenheit wie folgt bewertet: Die Verwaltung nach WEG gründet auf einer gesetzlichen Pflicht. Die für ihre Tätigkeit erforderliche Informationsverarbeitung zieht eine Verarbeitung der Eigentümerdaten nach sich. Insoweit kommt eine Anwendbarkeit des Privilegs für Bestandskunden gemäß § 7 Abs. 3 Gesetz gegen den unlauteren Wettbewerb (UWG) für E-Mail-Werbung nicht in Betracht, da es hier bereits an den für die Anwendung dieses Gesetzes erforderlichen Voraussetzungen fehlt. Eine (typische) Unternehmer-Kunden-Beziehung, in die sich der Empfänger der Werbung hineinbegeben hat, besteht vorliegend gerade nicht. Der/Die Verwalter/in ist von Gesetzes wegen vorgesehenes handelndes Organ der Eigentümergemeinschaft, §§ 9b, 27 WEG.

Dies hat dann auch zur Folge, dass für Glückwünsche oder Festtagsgrüße wiederum nicht der strenge Maßstab der Werbung anzulegen wäre, solange die Ansprachen im Rahmen der Verwaltungstätigkeit verbleiben. Falls in diesen Ansprachen der schlichte Hinweis auf die Immobiliensparte des Verwalters (bspw. in Firmenlogo und Signatur) enthalten wäre, würde dies aus meiner Sicht nicht schon zu einer Unzulässigkeit der Ansprache führen, vgl. Art. 5 Abs. 1 Buchst. b Datenschutz-Grundverordnung (DSGVO), erster Halbsatz.

Für eine gezielte Ansprache der Eigentümer/innen auf verwaltungsfremde Angelegenheiten gilt dies aber nicht.

Verwalter/innen, die ihre Eigentümergemeinschaft gelegentlich oder regelmäßig zu Nichtverwaltungsangelegenheiten kontaktieren möchten, sind daher angehalten, hierzu vorab individuelle Einwilligungen der Eigentümer/innen einzuholen.
Nach Konsultationen mit dem vom Unternehmen benannten Datenschutzbeauftragten habe ich die Zusicherung erhalten, dass das Unternehmen die beschriebene Praxis bei Werbe-Mails einstellt. Damit sollten Daten, die ausschließlich im Zusammenhang mit der Verwaltertätigkeit nach WEG anfallen, nicht mehr zur Akquise im Geschäftsbereich Immobilienhandel genutzt werden.
Bei dem Beschwerdevorgang hatte das mit der Verwaltung beauftragte Immobilienhandels- und Verwaltungsunternehmen eine überschaubare Größe, sodass eine gegenseitige Vertretung der einzelnen Beschäftigten der Normalfall und unvermeidlich war. Ab einer bestimmten Größe sollten in dieser Form auftretende Mischunternehmen jedoch die informationelle Trennung des Datenbestandes von sonstigen Geschäftsbereichen auch datenschutzorganisatorisch über ein Rollenkonzept absichern, Art. 25 DSGVO.

Was ist zu tun?
Ein/e Verwalter/in im Sinne des WEG, der/die die Mitglieder der Eigentümergemeinschaft auch zu Nichtverwaltungsangelegenheiten (zum Beispiel über den Immobilienmarkt) zu informieren beabsichtigt, hat hierzu vorab individuelle Einwilligungen der Eigentümer/innen einzuholen.

2.3.6 Weiterleitung von Eingaben

↗ § 3 SächsDSDG, § 7 GeschoSReg, Art. 6 Abs. 1 Buchst. e DSGVO

Ich erhielt sowohl von Petenten Beschwerden als auch von behördlichen Datenschutzbeauftragten Nachfragen hinsichtlich der Weiterleitung von Eingaben wegen Unzuständigkeit. Es betraf jeweils Fälle, in denen Bürgereingaben „zuständigkeitshalber" an andere Stellen weitergeleitet wurden, ohne dass eine Einwilligung der betroffenen Person eingeholt worden wäre. Diese erhielten lediglich eine Abgabenachricht.
Die Rechtmäßigkeit der Verarbeitung personenbezogener Daten in diesem Zusammenhang ist dann rechtmäßig, wenn eine Einwilligung vorliegt, Art. 6 Abs. 1 Buchst. a Datenschutz-Grundverordnung (DSGVO) oder wenn es für die Verarbeitung der personenbezogenen Daten eine Rechtsgrundlage gibt (Art. 6 Abs. 1 Buchst. e in Verbindung mit Abs. 2 und 3 Satz 1 DSGVO).

Als Rechtsgrundlage zur Verarbeitung personenbezogener Daten im Zusammenhang mit Bürgereingaben kann Artikel 6 Abs. 1 Buchst. e DSGVO in Verbindung mit § 3 Abs. 1 Sächsisches Datenschutzdurchführungsgesetz (SächsDSDG) und Artikel 35 der Verfassung des Freistaates Sachsen herangezogen werden. Artikel 35 der Verfassung des Freistaates Sachsen bestimmt, dass jede Person einen Anspruch auf einen begründeten Bescheid innerhalb angemessener Frist hat, wenn sie sich mit Beschwerden an die zuständige Stelle richtet. Liegt die Beantwortung der Eingabe in der Zuständigkeit der angeschriebenen Behörde, ist daher die Verarbeitung personenbezogener Daten über die oben angegebenen Rechtsgrundlagen gedeckt. Liegt die Zuständigkeit dagegen in einer anderen Behörde, kann die oben genannte Rechtsgrundlage nicht herangezogen werden, da § 3 SächsDSDG nur auf die Erforderlichkeit für die eigene Aufgabenerfüllung des Verantwortlichen abstellt, die bei Unzuständigkeit gerade nicht gegeben ist.

Es ist keine Rechtsgrundlage ersichtlich, in der allgemein festgelegt ist, dass eine unzuständige Behörde Beschwerden oder Anfragen an die zuständige Behörde weiterleiten soll oder darf. Nur für ganz bestimmte Fälle bestehen in wenigen Fachgesetzen Regelungen, wonach „Anträge" an die zuständige Behörde weiterzuleiten sind, zum Beispiel dem § 16 Abs. 2 Satz 1 Erstes Buch Sozialgesetzbuch (SGB I), § 7 Abs. 3 Sächsisches Umweltinformationsgesetz oder auch § 7 der Geschäftsordnung der Sächsischen Staatsregierung, wonach die Ministerpräsidentin oder der Ministerpräsident an sie oder ihn gerichtete Schreiben an das zuständige Mitglied der Staatsregierung weiterleiten kann.

Insbesondere Nr. 26 VwV Dienstordnung kommt nicht als Rechtsgrundlage im Sinne von Art. 6 Abs. 1 Buchst. e DSGVO in Betracht, weil eine Verwaltungsvorschrift (VwV) nur eine Wirkung innerhalb der Verwaltung entfalten kann, jedoch keine Regelungen im Verhältnis von Verantwortlichem (nach Art. 4 Nr. 7 DSGVO) und betroffener Person treffen kann.

Abgesehen davon halte ich das Vorgehen zur Wahrung der Rechte der/des Betroffenen auch vor dem Hintergrund für geboten, dass durchaus Fälle denkbar sind, in denen die Weiter-

leitung an eine bestimmte zuständige Stelle nicht im Interesse der Petentin oder des Petenten liegen dürfte – zum Beispiel, wenn er oder sie als Beschwerdeführer/in dieser Stelle gegenüber nicht genannt werden möchte, wofür es verschiedene (unter Umständen auch persönliche) Gründe geben kann.
Eine Weiterleitung von Eingaben wegen Unzuständigkeit wird daher regelmäßig nur mit Einwilligung zulässig sein. Eine solche kann auch konkludent erfolgen, das heißt sich aus dem Inhalt des Schreibens ergeben. Dies ist jedoch im Einzelfall zu prüfen; es kann keinesfalls pauschal davon ausgegangen werden, dass Petenten grundsätzlich ein Interesse an einer Weiterleitung an die zuständige Behörde haben – wie auch die Petitionen an mich zeigen. Ich empfehle daher, bei der Nutzung entsprechender Formulare eine Einwilligung vorzusehen.
Ergänzend möchte ich auf die Ausführungen „Erleichterte Datenweitergabe innerhalb von Stadtverwaltungen unter Geltung der DSGVO?" hinweisen – erschienen im Tätigkeitsbericht 2021 (1.2, Seite 41 ff.) –, wonach selbst für Übermittlungen innerhalb einer Stadtverwaltung wegen des funktionalen Stellenbegriffs bzw. der informationellen Gewaltenteilung eine Rechtsgrundlage für eine Übermittlung erforderlich ist.

Tätigkeitsbericht 2021:
↗ sdb.de/tb2021

Was ist zu tun?
Eine Weiterleitung von Eingaben wegen Unzuständigkeit wird regelmäßig unzulässig sein, sofern sich aus dem Inhalt der Eingabe im Einzelfall keine Einwilligung entnehmen lässt bzw. eine solche auf Nachfrage erteilt wird.

2.4 Sensible Daten, besondere Kategorien personenbezogener Daten

2.4.1 Forschungsprivileg im Sächsischen Krankenhausgesetz

↗ § 29 SächsKHG

Der Datenschutzbeauftragte eines Universitätsklinikums hat mich um Stellungnahme zum Forschungsprivileg nach § 29 Sächsisches Krankenhausgesetz (SächsKHG) gebeten.
Ärztinnen und Ärzte des Universitätsklinikums gehen nach § 29 Abs. 1 SächsKHG davon aus, dass sie auch mit behandlungs- und fachrichtungsfremden Patientendaten forschen

dürften, soweit diese am Universitätsklinikum zur Behandlung verarbeitet werden.
So möchte zum Beispiel eine Ärztin oder ein Arzt aus der Klinik und Poliklinik für Hämatologie, Zelltherapie, Hämostaseologie und Infektiologie auch Daten der Klinik und Poliklinik für Kardiologie für ein Forschungsprojekt nutzen. Hierfür müsste sie oder er auf die Patientendaten der Klinik und Poliklinik für Kardiologie zugreifen, die Daten selektieren und für die Forschung aufbereiten.
Kann sich die Ärztin bzw. der Arzt hierzu auf Art. 9 Abs. 4 DSGVO und Art. 89 DSGVO in Verbindung mit § 29 SächsKHG berufen, oder steht dies im Widerspruch zu § 28 Abs. 7 SächsKHG? Ist § 29 SächsKHG der Erlaubnistatbestand für die Datenverarbeitungen?
§ 29 SächsKHG lautet:

> „(1) [1]Ärztinnen und Ärzte dürfen Patientendaten, die innerhalb ihrer Fachabteilung oder bei Hochschulen innerhalb ihrer medizinischen Einrichtungen, in den Universitätsklinika oder in sonstigen medizinischen Einrichtungen gespeichert sind, für eigene wissenschaftliche Forschungsvorhaben verarbeiten. [2]Dies gilt entsprechend für sonstiges wissenschaftlich tätiges Personal dieser Einrichtungen und Personen, die zur Vorbereitung auf einen Beruf an diesen Einrichtungen wissenschaftlich tätig sind, soweit diese der Geheimhaltungspflicht nach § 203 des Strafgesetzbuches unterliegen."

§ 28 Abs. 7 SächsKHG fordert:

> „(7) [1]Nach Abschluss der Behandlung unterliegen Patientendaten, die in automatisierten Verfahren gespeichert und direkt abrufbar sind, dem alleinigen Zugriff der jeweiligen Fachabteilung. [2]Dies gilt nicht für Daten, die für das Auffinden der sonstigen Patientendaten erforderlich sind. [3]Der Direktzugriff auf den Gesamtdatenbestand darf anderen Stellen im Krankenhaus nur unter den Voraussetzungen des Absatzes 3 und nur mit Einwilligung der Fachabteilung gewährt werden."

§ 29 SächsKHG ist nach meiner Auffassung die Spezialregelung (lex specialis) zu § 28 SächsKHG. Die Regelungen des § 28 SächsKHG finden also, wenn es sich bei der geplanten Datenverarbeitung von Patientendaten nicht um einen normalen Behandlungsvorgang, sondern um ein Forschungsvorhaben handelt, nur Anwendung, soweit § 29 SächsKHG direkt darauf Bezug nimmt.

Nach dem Wortlaut des Gesetzes wird in § 29 Abs. 1 SächsKHG das Universitätsklinikum als Ganzes angesprochen. Das Sächsische Staatsministerium für Soziales und Gesellschaftlichen Zusammenhalt teilt meine Einschätzung, dass das jeweilige Universitätsklinikum in seiner Gesamtheit angesprochen wird. Aus Sicht des Sächsischen Staatsministeriums für Soziales und Gesellschaftlichen Zusammenhalt ist zwingend zu beachten, dass jedoch in jedem Fall sichergestellt sein muss, dass eine (übergreifende) Verarbeitung nur **zum Zwecke** (eigener) **wissenschaftlicher Forschungsvorhaben** erfolgen darf.

Was ist zu beachten?
§ 29 SächsKHG ist die Spezialregelung (lex specialis) zu § 28 SächsKHG.

Gegenstand des § 29 SächsKHG ist indes nur die Privilegierung der Eigenforschung, also die Forschung mit personenbezogenen Daten, die ausschließlich durch das eigene Personal der verantwortlichen Stelle durchgeführt wird.

2.4.2 Datenverarbeitungsbefugnisse einer Hochschule bei Geltendmachung einer Prüfunfähigkeit von Studierenden

Aufgrund zahlreich an mich gerichteter Anfragen und entsprechender Medienberichterstattung habe ich mich im Berichtszeitraum erneut zum Thema Prüfunfähigkeitsnachweis bei Studentinnen und Studenten geäußert:

Nach der Rechtsprechung (BVerwG, Beschluss vom 14.07.2004, BVerwG 6 B 30.04; OVG Berlin-Brandenburg, Beschluss vom 21.7.2014 – OVG 10 S 5.14) fällt die Prüfungskommission der Hochschule die Entscheidung über die Prüfungsunfähigkeit von Studierenden. Grundlage hierfür ist in der Regel ein ärztliches Attest, das für Nichtmedizinerinnen und -medi-

ziner nachvollziehbar darlegt, warum Studierende nicht an einer Prüfung teilnehmen können. Das ärztliche Attest hat in diesem Zusammenhang die Funktion, die gesundheitlichen Beeinträchtigungen des Prüflings zu beschreiben und anzugeben, welche Auswirkungen sich daraus für das Leistungsvermögen in der konkreten Prüfung ergeben, um die sachgerechte Beurteilung zu ermöglichen.
Ob die Voraussetzungen der Prüfungs(un)fähigkeit gegeben sind, ist somit eine Rechtsfrage, die die Prüfungsbehörde anhand des von ihr ermittelten Sachverhaltes in eigener Verantwortung zu beantworten hat (BVerwG a. a. O.). Es ist dagegen nicht Sache der Ärztin oder des Arztes, selbst die Prüfungsunfähigkeit festzustellen. Zur Erfüllung der Nachweisfunkton genügt es daher auch nicht, wenn sich ein Attest allgemein auf die Angabe einer Arbeitsunfähigkeit oder Prüfungsunfähigkeit beschränkt (OVG Berlin-Brandenburg a. a. O. mit weiteren Nachweisen).
Im 16. Tätigkeitsbericht für den öffentlichen Bereich (13.1, Seite 117) hatte sich mein Amtsvorgänger zu der Thematik bereits wie folgt geäußert:

> „Gleich mehrfach erreichten mich Eingaben Studierender zu Formularen ihrer Prüfungsbehörden, die Betroffene von ihrem Arzt ausfüllen lassen sollten, wenn sie aus gesundheitlichen Gründen nicht an einer Prüfung teilnehmen, sie abbrechen oder nach Beendigung von ihr zurücktreten wollen. Die Betroffenen wollten von mir wissen, inwieweit dies zulässig ist. Das Verlangen einer Prüfungsbehörde, zum Nachweis der Prüfungsunfähigkeit ein ärztliches Attest vorzulegen, stellt einen Eingriff in das Recht des Studierenden dar, grundsätzlich selbst über die Verwendung seiner Daten zu entscheiden. Ein solcher Eingriff bedarf einer gesetzlichen Grundlage, die sich in der Regel aber aus den jeweils einschlägigen Prüfungsordnungen ergibt, die als Satzungen auf Grundlage der Bestimmungen des Sächsischen Hochschulgesetzes erlassen wurden.

Die Prüfungsunfähigkeit ist allerdings ein Rechtsbegriff, dessen Voraussetzungen vom Prüfungsausschuss, nicht vom Arzt festzustellen sind (vgl. BVerwG, DVBl. 1996, S. 1379 f.). Demgemäß ist der Prüfungsausschuss befugt, solche Daten zum Leistungsvermögen des Prüflings zu erheben, die ihn als Prüfungsbehörde befähigen, in eigener Verantwortung eine Entscheidung darüber zu treffen, ob gesundheitliche Gründe es rechtfertigen, nicht an der Prüfung teilzunehmen, sie abzubrechen oder nach Beendigung von ihr zurückzutreten. Im Attest müssen somit die aus ärztlicher Sicht bestehenden krankheitsbedingten und zugleich prüfungsrelevanten körperlichen, geistigen und/oder seelischen Beeinträchtigungen und deren Auswirkungen auf das Leistungsvermögen des Prüflings konkret und nachvollziehbar beschrieben werden.
Es ist jedoch nicht erforderlich, neben den Befunden bzw. Krankheitssymptomen und den sich aus diesen ergebenden Beeinträchtigungen auch die ärztliche Diagnose als solche zu erheben, also Arzt oder Prüfling eine verpflichtende Preisgabe der Krankheitsangabe abzuverlangen. Da Formulare einzelner Prüfungsbehörden gleichwohl entsprechende Angaben vorsahen, bin ich mehrfach tätig geworden, auch dann, wenn das entsprechende Formularfeld ausdrücklich mit dem Hinweis „optional" gekennzeichnet war, weil dies trotzdem zu Angaben verleitet, die eine Prüfungsbehörde nicht beanspruchen kann."

Gerade vor dem Hintergrund der letztgenannten Gründe wäre mithin eine Abfrage der Bezeichnung der Krankheit/Diagnose, auch so dies nur mit Einwilligung der/des Betroffenen erfolgen soll, aus meiner Sicht unzulässig.

Im Ergebnis ist festzuhalten:

Wird als Entschuldigung für eine versäumte (oder abgebrochene) Prüfung eine krankheitsbedingte Prüfungsunfähigkeit geltend gemacht und die Möglichkeit einer weiteren

Wiederholung der Prüfung beansprucht, muss das Vorliegen des Hinderungsgrundes gegenüber der Hochschule nachgewiesen werden, um einem Missbrauch wirksam vorzubeugen und den Grundsatz der Chancengleichheit zu wahren. Das ist gefestigte höchstrichterliche Rechtsprechung, worauf sich die Hochschulen berufen können.
Zu den mir in den vorgelegten Formularen enthaltenen Abfragen der benannten Beeinträchtigungen wie Prüfungsangst, Prüfungsstress oder chronische Erkrankungen finden sich ausdrücklich Ausführungen in der von mir bereits zitierten Rechtsprechung, siehe OVG Berlin-Brandenburg, Beschluss vom 21.07.2014 – OVG 10 S 5.14. Denn gerade eine Prüfungsangst kann danach wohl nicht immer bereits zu einer Prüfunfähigkeit führen, die letztlich einen Hinderungsgrund begründen kann:

> „Die gestellte Diagnose, die auf eine psychische Störung hinweist, legt zudem nahe, dass die (behaupteten) Beschwerden des Antragstellers – wie vom Antragsgegner vermutet – im Zusammenhang mit einer Prüfungsangst stehen könnten, so dass selbst bei Bestätigung der geschilderten körperlichen Auswirkungen zu prüfen wäre, inwieweit diese eine Prüfungsunfähigkeit im Rechtssinn begründen. Prüfungsstress und Examensangst, die bei vielen Prüflingen anzutreffen sind und in unterschiedlichem Maß zu einer Beeinträchtigung der Leistungsfähigkeit führen können, werden der Risikosphäre des Prüflings zugerechnet und stellen keinen Fall der Prüfungsunfähigkeit dar (vgl. BVerwG, Urteil vom 28. November 1980 - BVerwG 7 C 54.78 -, BVerwGE 61, 211, juris Rn. 17; OVG Bln-Bbg, Beschluss vom 14. Dezember 2006 - OVG 7 M 16.06 u.a. -, BA S. 8; OVG NW, Beschluss vom 18. Dezember 2012 - 14 E 1040/12 -, juris Rn. 3). Etwas Anderes mag bei Vorliegen einer schwerwiegenden psychischen Beeinträchtigung gelten, die über eine allgemeine Examenspsychose hinausgeht und Krankheitswert hat, wobei in diesem Fall zu prüfen wäre, inwieweit ein

> die Leistungsfähigkeit des Prüflings prägendes Dauerleiden vorliegt, das ebenfalls nicht zu einer Prüfungsunfähigkeit im Rechtssinne führt (vgl. BVerwG, Beschluss vom 13. Dezember 1985 - BVerwG 7 B 210.85 -, NVwZ 1986, 377, juris Rn. 6; Beschluss vom 3. Juli 1995 - BVerwG 6 B 34.95 -, Buchholz 421.0 Prüfungswesen Nr. 352, juris Rn. 7)."

Was ist zu tun?
Ob die Voraussetzungen der Prüfungs(un)fähigkeit gegeben sind, ist eine Rechtsfrage, die die universitäre Prüfungsbehörde anhand des von ihr ermittelten Sachverhaltes in eigener Verantwortung zu beantworten hat.

Schließlich habe ich darauf hingewiesen, dass es sich bei der Festlegung, welche Beeinträchtigungen als Voraussetzung für eine Prüfunfähigkeit angesehen werden können, nicht um eine datenschutzrechtliche Fragestellung handelt und mithin nicht meiner Zuständigkeit obliegt.

2.4.3 Wann liegt eine abgeschlossene Behandlung im Sinne des § 28 Abs. 7 SächsKHG vor?

↗ § 8 Abs. 5 KHEntG, § 28 Abs. 7 SächsKHG, §§ 39, 115a SGB V

Der Datenschutzbeauftragte eines Universitätsklinikums bat mich um Stellungnahme, wann eine abgeschlossene Behandlung im Sinne des § 28 Abs. 7 Sächsisches Krankenhausgesetz (SächsKHG) vorliegt. Dazu schilderte er folgendes Beispiel:

> Ein Patient kommt erneut zur Behandlung in unser Klinikum. Zur optimalen Behandlung ist für das medizinische Personal die Einsichtnahme in die Behandlungsdokumentation aus den früheren Behandlungen erforderlich. Ist dies nur mit „der Einwilligung" der vorherigen Fachabteilung im Sinne des § 28 Abs. 7 Satz 3 SächsKHG möglich? Wird für jeden Datenzugriff der vorangegangenen Patientendokumentation diese Einwilligung benötigt?

Nach seiner Auffassung ist dies nicht praxistauglich und gegebenenfalls patientengefährdend, da zum Beispiel die Einsichtnahme in alte Medikamentenpläne und Diagnosen fehlt, dies jedoch medizinisch notwendig ist.

Das Rollen- und Berechtigungskonzept im Krankenhausinformationssystem des Universitätsklinikums sieht vor, dass das medizinische Personal nur nach Vorliegen eines Behandlungsauftrags Einsicht in die medizinischen Patientendaten erhält. Insofern bestünde aus seiner Sicht kein Risiko des unbefugten Datenzugriffs und auch kein direkter Abruf der Patientendaten im Sinne des § 28 Abs. 7 Satz 1 SächsKHG.
§ 28 Abs. 7 SächsKHG lautet:

> „(7)[1]Nach Abschluss der Behandlung unterliegen Patientendaten, die in automatisierten Verfahren gespeichert und direkt abrufbar sind, dem alleinigen Zugriff der jeweiligen Fachabteilung. [2]Dies gilt nicht für Daten, die für das Auffinden der sonstigen Patientendaten erforderlich sind. [3]Der Direktzugriff auf den Gesamtdatenbestand darf anderen Stellen im Krankenhaus nur unter den Voraussetzungen des Absatzes 3 und nur mit Einwilligung der Fachabteilung gewährt werden."

Bei der Änderung des § 28 Abs. 7 Satz 3 SächsKHG wurde das Wort „Zustimmung" durch das Wort „Einwilligung" ersetzt. In Anbetracht der Landtags-Drucksache zur Änderung des SächsKHG handelt es sich nach meiner Einschätzung dabei lediglich um eine sprachliche Anpassung an die DSGVO.
Dies stellt aus meiner Sicht keine Änderung der bisherigen Rechtslage nach dem „alten" § 28 Abs. 7 Satz 3 SächsKHG dar. § 28 Abs. 7 Satz 1 SächsKHG setzt voraus, dass die Behandlung abgeschlossen ist. Nach § 28 Abs. 7 Satz 3 SächsKHG darf anderen Stellen im Krankenhaus der Direktzugriff auf den Gesamtdatenbestand nur unter den Voraussetzungen des Absatzes 3 und nur mit Einwilligung der Fachabteilung gewährt werden.
Definitionen zum Abschluss der Behandlung sind dem Glossar zur Orientierungshilfe (OH) Krankenhausinformationssysteme, Seite 1, sowie § 39 Fünftes Buch Sozialgesetzbuch (SGB V) zu entnehmen.

Glossar OH Krankenhausinformationssysteme:

„**Behandlungsfall**: Eine medizinische Behandlung umfasst alle Anamnese-, Diagnose-, Therapie- und Nachbehandlungsmaßnahmen zu derselben Krankheit, Verdachtsdiagnose oder Symptomatik, wegen der der Patient stationär aufgenommen wurde. Medizinisch kann eine Behandlung aus mehreren ambulanten und stationären Behandlungsfällen bestehen und über Jahrzehnte andauern (chronische Krankheiten).
Unter Behandlungsfall ist bei einer stationären Behandlung die gesamte Behandlung derselben Erkrankung zu verstehen, die ein Patient in einem Krankenhaus von der stationären Aufnahme bis zur Entlassung aus der stationären Behandlung erhält. Eingeschlossen sind die dem Behandlungsfall zuzuordnenden vor- und nachstationären Behandlungen im Sinne von § 115 a SGB V, sowie Wiederaufnahmen innerhalb der oberen Grenzverweildauer im Sinne von § 8 Abs. 5 Krankenhaus-Entgeltgesetz (KHEntG)."

Die Orientierungshilfe (OH) Krankenhausinformationssysteme sieht zum Fall der abgeschlossenen Behandlung vor, Seite 5:

„**Einschränkung der Zugriffsrechte nach Abschluss des Behandlungsfalls**. […]
26. Wird ein Patient nach Wirksamwerden der Zugriffsbeschränkung erneut behandelt, darf die Beschränkung des Zugriffs auf Daten aus früheren Behandlungsfällen aufgehoben werden. Der Zugriff auf Vorbehandlungsdaten ist nur soweit zulässig, wie das Landeskrankenhausrecht dies gestattet."

Ist im Beispielsfall die Behandlung des Patienten abgeschlossen, so bedarf der Direktzugriff auf den Gesamtdatenbestand nach § 28 Abs. 7 SächsKHG,

- dass Absatz 3 vorliegt (Behandlungsvertrag oder Einwilligung des Patienten) und die
- Einwilligung der Fachabteilung gewährt wird.

Was ist zu beachten?
Definitionen, wann eine abgeschlossene Behandlung eines Patienten vorliegt, sind dem Glossar zur OH Krankenhausinformationssysteme, Seite 2, sowie § 39 SGB V zu entnehmen.

Wird die Einwilligung der Fachabteilung im Hinblick auf die nunmehrige Behandlung gewährt, ist die Beschränkung des Zugriffs nach § 28 Abs. 7 SächsKHG aufgehoben. Nach meiner Einschätzung bedarf es nicht einer „mehrmaligen" Einwilligung durch die Fachabteilung. Die Einwilligung kann über das Krankenhausinformationssystem erfolgen.

3 Betroffenenrechte

3.1 Spezifische Pflichten des Verantwortlichen

3.1.1 Automatisierte Abfrage in das Sächsische Melderegister bei Auskunfts- und Übermittlungssperren

↗ § SächsAGBMG

Im Berichtszeitraum wandte sich eine sächsische Kommune an mich mit der folgenden, durchaus interessanten Frage, die das Spannungsverhältnis zwischen der fortschreitenden Zentralisierung und Digitalisierung im Meldewesen und der Verantwortlichkeit der einzelnen Gemeinde für die Daten der eigenen Bürger/innen etwas beleuchtet.
Gemäß den Regelungen des Sächsischen Gesetzes zur Ausführung des Bundesmeldegesetzes (SächsAGBMG) werden die Zuständigkeiten zwischen den Gemeinden als örtliche Meldebehörden und der Sächsischen Anstalt für kommunale Datenverarbeitung (SAKD) als zentrale Meldebehörde verteilt. Die SAKD ist unter anderem zuständig für die Führung des landesweit einheitlichen Sächsischen Melderegisters, aus dem auch Einzelabfragen durch Behörden oder Einwohnermeldeauskünfte seitens Unternehmen und Privatpersonen nach dem Bundesmeldegesetz (BMG) erfolgen können.
Die Gemeinden haben in diesem Zusammenhang die Pflicht, der SAKD gemäß § 8 Abs. 2 SächsAGBMG die Meldedaten zu übertragen und etwaige spätere Änderungen tagesaktuell zu melden, damit das zentrale Melderegister stets aktuell bleibt.

Nicht selten ist für einzelne Bürger/innen entweder eine Auskunfts- oder/und eine Übermittlungssperre im Meldedatensatz hinterlegt. Für die Eintragung und die Prüfung der Voraussetzungen ist nicht die SAKD, sondern die jeweilige Gemeinde als Ortsmeldebehörde zuständig, § 1 Abs. 3 SächsAGBMG.
Eine **Auskunftssperre nach § 51 BMG** ist dann einschlägig und wird (auf Antrag oder auch von Amts wegen) eingetragen, wenn Tatsachen vorliegen, „die die Annahme rechtfertigen, dass der betroffenen oder einer anderen Person durch eine Melderegisterauskunft eine Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Interessen erwachsen kann". Dies umfasst unter anderem Fälle von häuslicher Gewalt, Bedrohungen, Beleidigungen sowie unbefugte Nachstellungen. Somit sind hier Fälle umfasst, in denen der Aufenthaltsort dem/der Täter/in und seinem/ihrem Umfeld nicht bekannt sein darf. Die Voraussetzungen der Auskunftssperre werden zudem alle zwei Jahre neu geprüft und festgestellt.
Ein Widerspruch gegen Übermittlungen (**Übermittlungssperre**) liegt dagegen dann vor, wenn der oder die Bürger/in schlicht nicht wünscht, dass seine/ihre Daten an bestimmte Organisationen und Einrichtungen herausgegeben werden:

- Parteien, Wählergruppen und andere Trägerinnen und Träger von Wahlvorschlägen im Zusammenhang mit Wahlen und Abstimmungen zum Zwecke der Wahlwerbung, § 50 Abs. 5 BMG
- Mandatsträgerinnen und Mandatsträger, Presse oder Rundfunk über Alters- oder Ehejubiläen, § 50 Abs. 5 BMG
- Adressbuchverlage zur Herausgabe von Adressverzeichnissen in Buchform, § 50 Abs. 5 BMG
- eine öffentlich-rechtliche Religionsgesellschaft durch den Familienangehörigen eines Mitglieds dieser Religionsgemeinschaft, § 42 Abs. 3 BMG
- das Bundesamt für das Personalmanagement der Bundeswehr zum Zwecke der Übersendung von Informationsmaterial, § 58c Abs. 1 Satz 1 des Soldatengesetzes (SG), § 36 Abs. 2 BMG

Hier reicht ein kurzer Antrag, der weder zu begründen ist noch einer Befristung unterliegt. Die Voraussetzungen sind somit um einiges niederschwelliger als bei einer Auskunftssperre.

Die Auskunfts- als auch Übermittlungssperren sind gegenüber der jeweiligen Gemeinde als örtliche Meldebehörden zu erklären, diese ist auch zuständig für die Prüfung der jeweiligen formellen und materiellen Voraussetzungen und der darauffolgenden Meldung der Sperren an die SAKD im Zuge des Änderungsdienstes.

Nun kam in dem zugrunde liegenden Fall die Frage auf, wie das Verhältnis und die Zuständigkeitsverteilung konkret zwischen der jeweiligen Gemeinde und der SAKD sich darstellt und ob die Gemeinde es in der Hand hat, welche Daten über eingehende automatisierte Abfragen herausgegeben werden oder dies in alleiniger Verantwortung der SAKD liegt.

Die SAKD erklärt das zugrunde liegende Prozedere wie folgt: Trifft eine Anfrage an das Sächsische Melderegister auf einen mit einer Auskunftssperre nach § 51 BMG gekennzeichneten Datensatz, dann beantwortet zunächst das Sächsische Melderegister die Anfrage mit einer neutralen Antwort gegenüber der oder dem Anfragenden, aus der diese bzw. dieser nicht schließen kann, ob eine Sperre oder bereits überhaupt kein eindeutiger Datensatz zu der betroffenen Person vorliegt. Alsdann wird die Anfrage zur (manuellen) Weiterbearbeitung an die örtliche Meldebehörde ausgesteuert. Diese behandelt die eingegangene Anfrage im Weiteren in eigener Zuständigkeit manuell und als nicht automatisierte Anfrage anhand der rechtlichen Vorgaben des § 34 Abs. 5 und § 51 BMG.

Nach alledem konnte ich gegenüber der anfragenden Gemeinde feststellen, dass sie bei dieser Zuständigkeitsverteilung nicht für automatisierte Abfragen in das Melderegister betroffen ist, indes auch in diesen Fällen über eine Kontrolle über „gesperrte" Datensätze verfügt. Bei manuellen Abfragen oder bei manueller Weiterbearbeitung nach Weiterleitung durch das Sächsische Melderegister erscheint die Problematik nicht, da jede Anfrage im Einzelnen händisch geprüft und bearbeitet wird.

Was ist zu beachten?
Durch die Systematik und Zuständigkeitsverteilung zwischen zentraler und örtlicher Meldebehörde ist dafür gesorgt, dass auch bei einem zentralen Datenbestand im Falle einer Sperre eine manuelle Überprüfung stattfindet.

Somit wird durch diese gesetzliche Zuständigkeitsaufteilung auch der Schutz der Auskunfts- und Übermittlungssperren gewährleistet, da die betroffenen Datensätze trotz automatisierter Anfrage noch eine individuelle manuelle Prüfung erfahren.

3.2 Auskunftsrecht

3.2.1 Datenschutzrechtliche Anforderungen an die Auskunftserteilung – Identitätsfeststellung

↗ Art. 12, Art. 15 DSGVO

Regelmäßig erhält meine Behörde Anfragen verunsicherter Verantwortlicher, die sich mit Auskunftsersuchen konfrontiert sehen und nicht genau wissen, welche Maßnahmen zur Identitätsfeststellung zu treffen sind und in welcher Form das Auskunftsersuchen beantwortet werden kann bzw. muss. Dem Datenschutzbeauftragten eines Krankenhauses lag ein Auskunftsersuchen nach Art. 15 Datenschutz-Grundverordnung (DSGVO) einer ehemaligen Patientin vor. Die Patientin hatte das Auskunftsersuchen zunächst per E-Mail und nochmals per Fax gestellt. Aus Sicht des Datenschutzbeauftragten war eine sichere Identitätsfeststellung, die eine Beantwortung des Auskunftsersuchens und damit auch eine Übermittlung von sensiblen Gesundheitsdaten erlaubte, nicht möglich. Daher wurden zur Beantwortung des Auskunftsersuchens die Informationen/Unterlagen auf CDs über die Deutsche Post AG mittels „Einschreiben/eigenhändig" versandt. Damit sollte eine Identitätsfeststellung durch die Deutsche Post AG (im Rahmen der Zustellung) sichergestellt werden. Da der Zustellversuch (eigenhändige Übergabe) jedoch scheiterte, wurde das Schreiben in der Postfiliale zur Abholung durch die Betroffene hinterlegt. Allerdings hat die Betroffene das Schreiben jedoch nicht abgeholt, sodass eine Rücksendung an das Krankenhaus erfolgte.
Die Patientin teilte danach dem Krankenhaus mit, dass sie auf einer Zustellung mit einem „Einschreiben/Einwurf" be-

stehe. Aus Sicht des Krankenhauses war diese Zustellart jedoch nicht datenschutzkonform, da es sich um besonders sensible Gesundheitsdaten handele und über Fax oder E-Mail-Adresse eine hinreichend sichere Identitätsfeststellung nicht möglich erscheine, obgleich von der Patientin eine geschwärzte Ausweiskopie vorgelegt worden sei.

Der Datenschutzbeauftragte des Krankenhauses bat mich daher um eine Einschätzung zu diesem Sachverhalt.

Zunächst ist zu unterscheiden zwischen der Identitätsfeststellung des bzw. der Auskunftsersuchenden und der anschließenden datenschutzkonformen Übermittlung der Antwort auf das Auskunftsersuchen durch den Verantwortlichen.

Hat der Verantwortliche begründete Zweifel an der Identität der natürlichen Person, die den Antrag gemäß Art. 15 DSGVO gestellt hat, so kann er unbeschadet des Artikels 11 DSGVO zusätzliche Informationen anfordern, die zur Bestätigung der Identität der betroffenen Person erforderlich sind, Art. 12 Abs. 6 DSGVO. Vorliegend wurde eine geschwärzte Ausweiskopie übersandt. Aus Sicht meiner Behörde bringt die Übermittlung eines Ausweisdokuments (per Post oder über gesicherte E-Mail bzw. gesicherte Website) eine höhere Sicherheit in Bezug auf die Identifizierung. Auch ist eine Schwärzung möglich, da lediglich Name, Anschrift, Geburtsdatum und Gültigkeitsdauer zur Identifizierung benötigt werden.

Üblicherweise erfolgt auch die Antwort des Auskunftsersuchens an die im Ausweisdokument angegebene Anschrift. In diesem Zusammenhang ist zu beachten, dass sich allein aus der Art der Daten (personenbezogene Daten nach Art. 6 DSGVO oder besonderer Kategorien personenbezogener Daten nach Art. 9 DSGVO) keine höheren Anforderungen/Standards an die Identitätsfeststellung aus Art. 12 Abs. 6 DSGVO ergeben.

Höhere Anforderungen bzw. Standards können sich jedoch im Hinblick auf die konkrete Art der Beauskunftung, das heißt den Übertragungsweg ergeben (zum Beispiel per verschlüsselter E-Mail).

Abschließend habe ich dem Datenschutzbeauftragten des Krankenhauses mitgeteilt, dass es aus meiner Sicht grundsätzlich genügt, wenn die schriftliche Beauskunftung mittels Posteinwurf erfolgt, soweit vorher die Identität zum Beispiel mittels teilweise geschwärzter Ausweiskopie festgestellt wurde und keine (weiteren) begründeten Zweifel an der Identität bestehen. Die vorliegend gewählte Variante Zustellung per „Einschreiben/eigenhändig" bzw. gegebenenfalls Abholung in der Postfiliale ist auch noch als datenschutzkonform anzusehen, insbesondere wird dadurch die Geltendmachung des Auskunftsanspruches nicht vereitelt bzw. unverhältnismäßig erschwert, sodass ich im Ergebnis keinen Anhaltspunkt für einen Datenschutzverstoß gesehen habe.

Was ist zu tun?
Der Verantwortliche ist pflichtig, eine Auskunftserteilung sowohl an die allein berechtigte betroffene Person sicherzustellen als auch die Übermittlung der Informationen auf datenschutzgerechte Weise – gesichert – durchzuführen.

3.2.2 Umfang des Auskunftsanspruchs gegenüber einem gegnerischen Rechtsanwalt

↗ § 29 Abs. 1 Satz 2 BDSG § 43 a Abs. 2 BRAO, Art. 15 Abs. 1 und 3 DSGVO

Ein Bürger, der Partei eines Rechtsstreites war, forderte den gegnerischen Rechtsanwalt auf, ihm in vollem Umfang gemäß Art. 15 Datenschutz-Grundverordnung (DSGVO) Auskunft zu erteilen und seine bei ihm gespeicherten personenbezogenen Daten zu löschen. Der Rechtsanwalt reagierte darauf nicht, und der Bürger reichte deshalb bei meiner Behörde Beschwerde ein.
Nach Prüfung der Rechtslage hat meine Behörde entschieden, dass der Petent grundsätzlich von einem gegnerischen Rechtsanwalt keine Auskunft bzw. Löschung verlangen kann. Diese Einschränkung des Auskunftsrechts gemäß Art. 15 DSGVO ergibt sich gemäß Art. 23 Abs. 1 Buchst. g DSGVO in Verbindung mit § 29 Abs. 1 Satz 2 Bundesdatenschutzgesetz (BDSG). Danach ist das Auskunftsrecht ausgeschlossen, soweit durch die Auskunft Informationen offenbart würden, die nach einer Rechtsvorschrift geheim gehalten werden müssen. Hierzu gehören insbesondere solche Informationen, die der berufsrechtlichen Verschwiegenheitspflicht unterfal-

len, also grundsätzlich alles, was der Rechtsanwältin oder dem Rechtsanwalt im Rahmen der Berufsausübung bekannt geworden ist (§ 43 a Abs. 2 Bundesrechtsanwaltsordnung [BRAO]).

Dies gilt nicht für Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen. Diese Voraussetzung dürfte nur in seltenen Ausnahmefällen erfüllt sein. Denn selbst die Tatsache, dass überhaupt personenbezogene Daten einer Person bekannt sind, kann im Rahmen eines Mandatsverhältnisses und der gegebenenfalls Durchsetzung von Rechtsansprüchen der Mandantin oder des Mandanten relevant sein und unterliegt daher grundsätzlich der Geheimhaltungspflicht. Anderenfalls würde sich die Rechtsanwältin bzw. der Rechtsanwalt der Verletzung dieser Berufspflichten aussetzen.

Der Rechtsanwalt in diesem Falle hatte sich auch darauf berufen, dass er hier zu keinerlei Auskunft verpflichtet ist, da dies die Verschwiegenheitspflicht aus seinem Mandatsverhältnis bzw. den gesetzlichen Verpflichtungen, wie dargestellt, widersprechen würde.

Aus den dargestellten Gründen besteht daher nach der Rechtsauffassung meiner Behörde für die Partei eines Rechtsstreits kein Auskunftsrecht gegenüber einer gegnerischen Rechtsanwältin bzw. einem Rechtsanwalt.

Zudem gibt es vielfältige Konstellationen, wonach Daten im Zusammenhang mit derartigen Gerichtsbeschlüssen für den Rechtsstreit relevant sein können und auch deshalb der Geheimhaltung unterliegen.

Insoweit greift also die generelle Regel des § 29 Abs. 1 Satz 2 Bundesdatenschutzgesetz, wonach der Auskunftsanspruch Informationen nicht umfasst, die der berufsrechtlichen Verschwiegenheitspflicht unterfallen, also grundsätzlich alles, was Rechtsanwältinnen bzw. Rechtsanwälten in Ausübung ihres bzw. seines Berufes bekannt geworden ist, § 43a Abs. 2 Satz 2 BRAO.

Was ist zu tun?

Aufgrund ihrer/seiner berufsrechtlichen Verschwiegenheitspflicht ist eine Rechtsanwältin oder ein Rechtsanwalt einer Gegnerin oder einem Gegner zu keinerlei Auskunft über die Speicherung oder Verarbeitung von deren bzw. dessen personenbezogenen Daten verpflichtet.

3.2.3 Auskunftsanspruch gegenüber einem gegnerischen Rechtsanwalt – Vollmacht

↗ § 29 Abs. 2 BDSG, Art. 15 Abs. 1 und 3 DSGVO

Im Berichtszeitraum erreichten mich mehrere Anfragen und Beschwerden zum Umfang des Auskunftsrechts gegenüber einem gegnerischen Rechtsanwalt.

Ein Petent rügte, dass die gegnerische Rechtsanwältin durch die fehlende Vorlage einer Vollmacht die Auskunftspflicht nach der Datenschutz-Grundverordnung (DSGVO) verletzt habe.

Diese Beschwerde hatte keinen Erfolg. Nach Art. 15 DSGVO kann eine betroffene Person Auskunft von der Person oder dem Unternehmen verlangen, die bzw. das ihre personenbezogenen Daten verarbeitet. Aus einer anwaltlichen Vollmacht geht hervor, wer einen Rechtsanwalt in einer bestimmten Angelegenheit gegen den Betroffenen bevollmächtigt hat. Es handelt sich damit nicht um einen Auskunftsanspruch nach Art. 15 DSGVO, da in dieser Vollmacht nicht angegeben wird, welche der personenbezogenen Daten der betroffenen Person der gegnerische Rechtsanwalt verarbeitet und woher er diese Daten erhalten hat. Die Vollmacht ist zudem Teil der Anwaltsakte, vgl. auch § 29 Abs. 2 Bundesdatenschutzgesetz.

Ob der Betroffene vom gegnerischen Rechtsanwalt die Vorlage einer Vollmacht verlangen kann, ist gegebenenfalls noch eine zivilrechtliche Frage, für die ich nicht zuständig bin. Meine Behörde darf zivilrechtlich auch keinen Rechtsrat erteilen. Dies wäre sonst ein Verstoß gegen das Rechtsdienstleistungsgesetz.

Im Allgemeinen ist auch darauf hinzuweisen, dass die betroffene Person zunächst selbst einen datenschutzrechtlichen Auskunftsanspruch gemäß Art. 15 DSGVO gegenüber dem Verantwortlichen erheben muss. Dies ist meiner Behörde nachzuweisen. Erst danach – falls dieser dann von dem Verantwortlichen nicht erfüllt wird – kann meine Behörde als Aufsichtsbehörde tätig werden.

Soweit eine Bürgerin oder ein Bürger meint, dass eine Rechtsanwältin oder ein Rechtsanwalt darüber hinaus ihre bzw. seine anwaltlichen Berufspflichten verletzt, müsste sie oder er dies

Was ist zu beachten?
Nach dem datenschutzrechtlichen Auskunftsanspruch Art. 15 DSGVO kann eine Partei von einem gegnerischen Rechtsanwalt bzw. einer Rechtsanwältin nicht die Vorlage einer Vollmacht verlangen.

bei der für diese Rechtsanwältin bzw. diesen Rechtsanwalt zuständigen Rechtsanwaltskammer vorbringen.

3.2.4 Auskunftsrecht bei finanziertem Autokauf (verbundene Verträge)

↗ Art. 4 Nr. 1 und 7, Art. 15 Abs. 1 und 3 DSGVO

Ein Bürger schilderte meiner Behörde, dass er im Jahre 2020 bei einem Autohändler in Leipzig einen Kaufvertrag über einen Pkw und zu dessen Finanzierung auch einen Darlehensvertrag bei einer Bank unterzeichnet hatte. Beide Verträge wurden ihm vom Autohändler zur Unterschrift vorgelegt. Dies ist die übliche Verfahrensweise, wenn der Autohändler sich vorab mit einer Bank verabredet hat, dem Kunden auch eine Finanzierung mit anzubieten. Dabei handelt es sich um verbundene Geschäfte gemäß § 358 Absatz 3 Bürgerliches Gesetzbuch (BGB).

Weiterhin berichtete der Petent, dass ihm aber zu beiden Verträgen keine vollständigen Abschriften übergeben worden sind. Bestimmte Passagen in beiden Verträgen waren geschwärzt. Er stellte mir die Frage, ob ihm **nach Datenschutzrecht** beim Abschluss des Kaufvertrages eine vollständige Kopie der Verträge hätte übergeben werden müssen. (Ob sich dieser Anspruch auch aus denkbaren zivilrechtlichen bzw. eventuell verbrauchervertraglichen Informationspflichten bzw. Nebenpflichten oder allgemeinen vertragsrechtlichen Grundsätzen ergibt, oblag nicht meiner Betrachtung als Datenschutzaufsichtsbehörde.) Das Auskunftsrecht gemäß Art. 15 Abs. 1 Datenschutz-Grundverordnung (DSGVO) setzt voraus, dass der Käufer zunächst selbst nachweislich vom Verkäufer und der Bank, beide sind Verantwortliche gemäß Art. 4 Nr. 7 DSGVO, Auskunft verlangt hat.

Nach Art. 15 Abs. 3 Satz 1 DSGVO hat der Verantwortliche eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung zu stellen, wenn die betroffene Person Auskunft verlangt. Bereits aus dem Wortlaut ergibt sich, dass insoweit nur die personenbezogenen Daten in Kopie zu übergeben sind. Dies wird durch die Kommen-

tarliteratur bestätigt. Nach dem Kommentar von Kühling/Buchner Datenschutz-Grundverordnung Bundesdatenschutzgesetz Kommentar, C.H. Beck Verlag, 3. Aufl. 2020, Art. 15 Rn. 41, ist der Verantwortliche daher berechtigt, andere Daten als personenbezogene Daten, die in demselben Dokument oder derselben Datei enthalten sind, unkenntlich zu machen, bevor er die Kopie herausgibt.

Deshalb kam es vorliegend auf die Frage an, ob die in einem Kaufvertrag über einen Pkw bzw. die in einem gleichzeitig zu dessen Finanzierung abgeschlossenen Darlehensvertrag enthaltenen Daten personenbezogene Daten gemäß Art. 4 Nr. 1 DSGVO darstellen. Dies ist zu bejahen, da die im Darlehensvertrag angegebene Person die Darlehensvertragssumme zu einem bestimmten Zinssatz mit den weiteren Kennzahlen des Darlehensvertrages schuldet. Insoweit ist ein Personenbezug gegeben. Das Gleiche gilt hinsichtlich der Daten des Kaufvertrages über einen bestimmen Personenkraftwagen, den eine Person mit diesem Kaufvertrag erwirbt. Auch insoweit bezeichnen die Kennziffern den Pkw des Kaufvertrages, den die Person erworben hat und abzunehmen verpflichtet ist.

Meine Behörde beantwortete daher die Frage des Petenten dahingehend, dass ihm auf sein Auskunftsbegehren alle wesentlichen Daten des Kaufvertrages und des Darlehensvertrages mitzuteilen und ihm die mit seiner Person verbundenen Informationen in einer Kopie zur Verfügung zu stellen sind. Weder der Verkäufer noch die Bank waren daher berechtigt, die entsprechenden Daten auf der ihm bzw. ihr übergebenen Kopie abzudecken oder zu schwärzen.

Was ist zu tun?
In Kaufverträgen, Darlehensverträgen (oder ähnlichen Verträgen) dürfen kennzeichnende Eigenschaften, die zur Bestimmung des Vertragsgegenstands wesentlich sind, im Exemplar für den Kunden oder die Kundin nicht geschwärzt werden, da sie personenbezogene Daten im Sinne des Datenschutzrechts darstellen.

3.3 Recht auf Löschung

3.3.1 Löschung eines ärztlichen Gutachtens

↗ § 10 Abs. 3 Berufsordnung der Sächsischen Landesärztekammer, § 630f Abs. 3 BGB; Art. 12 Abs. 3 und 4, Art. 17 DSGVO

Mich hat eine Anfrage erreicht, wann und durch wen ein ärztliches Gutachten zu löschen sei, welches in einem Krankenhaus erstellt wurde.

Tätigkeiten in der Gesundheitsversorgung ohne die Verarbeitung von personenbezogenen Daten werden nur in den seltensten Fällen möglich sein. Personenbezogene Daten sollen und dürfen aber auch unbeschränkt verarbeitet und gespeichert werden. Wie lange die Speicherung erfolgen darf, ist im Einzelfall zu entscheiden. Nach dem Ablauf der zulässigen Speicherdauer sind die Daten und damit auch ein ärztliches Gutachten zu löschen.

Die datenschutzrechtliche Pflicht zur Löschung von Patientendaten ergibt sich aus Art. 17 Datenschutz-Grundverordnung (DSGVO). Sie resultiert aus dem Recht auf informationelle Selbstbestimmung.

Die DSGVO enthält selbst keine Definition des Begriffs „Löschen". Das Löschen kann auf unterschiedliche Weise erfolgen. Maßgeblich ist, dass es nach dem Löschen niemandem mehr ohne unverhältnismäßigen Aufwand möglich ist, die jeweiligen Informationen wahrzunehmen (vgl. Kühling/Buchner/Herbst DSGVO Art. 17 Rn. 37).

Zum Löschen ist der für die Verarbeitung personenbezogener Daten Verantwortliche im Sinne des Art. 4 Nr. 7 DSGVO verpflichtet. Dies ist in der Regel die Unternehmensleitung; in dem Fall hier also die Leitung des Krankenhauses.

Art. 5 Abs. 1 Buchst. d DSGVO sieht eine Pflicht zur Löschung beim Vorliegen unrichtiger Daten vor, andererseits enthält Art. 17 Abs. 1 DSGVO Verpflichtungen auch für andere Fälle, so unter anderem, wenn die betroffene Person die Löschung verlangt und keine rechtlichen Gründe die weitere Verarbeitung und insbesondere die Speicherung erlauben.

Gesetzliche oder berufsständische (Mindest-)Aufbewahrungsfristen stellen regelmäßig rechtliche Gründe dar, die trotz einer beantragten Löschung eine weitere Verarbeitung, insbesondere aber eine Speicherung von Patientendaten erlauben. Dementsprechend darf während dieses vorgeschriebenen Zeitraums keine Löschung von Patientendaten erfolgen. Ein Krankenhaus oder auch eine Arztpraxis muss die (auch gutachterlich vorgenommene) Dokumentation der Krankenbehandlung in diesem Zeitraum aufbewahren.

Die berufsrechtliche Verpflichtung zur Aufbewahrung von ärztlichen Unterlagen beträgt regelmäßig 10 Jahre nach Abschluss der Behandlung (vgl. § 10 Abs. 3 der Berufsordnung der Sächsischen Landesärztekammer sowie § 630f Abs. 3 Bürgerliches Gesetzbuch). Über die vorgenommene Löschung bzw. über die Gründe, welcher dieser entgegenstehen, hat der Träger des Krankenhauses die Patienten zu informieren (vgl. Art. 12 Abs. 3 und 4 DSGVO).

Was ist zu beachten?
Einem datenschutzrechtlichen Löschungsanspruch können gesetzliche oder berufsständische Aufbewahrungsfristen entgegenstehen.

Bezüglich der bei mir eingegangenen Anfrage habe ich der betroffenen Person mitgeteilt, dass ich in ihrem Fall mangels gegenteiliger Anhaltspunkte davon ausgehe, dass die zehnjährige Aufbewahrungsfrist noch nicht abgelaufen ist und somit noch keine Löschung des sie betreffenden Gutachtens in Betracht kommt.

3.3.2 Löschung vor Ablauf der regulären Aufbewahrungsfrist

↗ § 5 SachsArchivG, § 7 SachsDSDG, § 147 AO, § 117 SachsBeamtG, Art. 17 Abs. 1 und 3 DSGVO

Ein Einzelfall warf die interessante Frage auf, ob ein behördlicher Vorgang vor Ablauf der regulären Aufbewahrungsfrist gelöscht werden darf. Hintergrund war ein Löschungsbegehren der betroffenen Person nach Art. 17 Abs. 1 Datenschutz-Grundverordnung (DSGVO). In diesem Zusammenhang muss der Verantwortliche prüfen, ob Aufbewahrungsvorschriften nach Art. 17 Abs. 3 Buchst. b DSGVO der Löschung entgegenstehen und ob diese im Einzelfall abgekürzt werden dürfen.
Ich vertrete dazu folgende Meinung: Solange die Aufbewahrungsfrist nicht durch Gesetz vorgeschrieben ist – wie dies etwa bei § 117 Sächsisches Beamtengesetz („Personalakten sind nach ihrem Abschluss von der personalaktenführenden Behörde fünf Jahre aufzubewahren.") oder bei § 147 Abs. 3 Abgabenordnung (zehn Jahre bei bestimmten steuerlich relevanten Unterlagen) der Fall ist –, sondern durch Verwaltungsvorschrift geregelt ist, kann die Frist im begründeten Einzelfall auf Antrag der betroffenen Person abgekürzt werden. Dafür spricht der Umstand, dass die Aufbewahrung des Vorgangs

häufig eher im Interesse der betroffenen Person als im Interesse des Verantwortlichen vorgenommen wird. Daher darf der Verantwortliche, wenn die betroffene Person die Löschung beantragt, auch eher die Aufbewahrungsfrist abkürzen. Voraussetzung ist allerdings, dass der Verantwortliche die Interessen der betroffenen Person richtig erkennt und sorgsam mit seinen eigenen Zwecken abwägt. Tendenziell anders könnte dagegen die Löschung des Schrift- oder Mailverkehrs, der zur Löschung des Vorgangs geführt hat, beurteilt werden. Denn die Aufbewahrung dieses Schrift- oder Mailverkehrs liegt wegen der Dokumentationspflichten nach Art. 5 Absatz 2 DSGVO eher im Interesse des Verantwortlichen.

Die durch § 5 Sächsisches Archivgesetz und § 7 Sächsisches Datenschutzdurchführungsgesetz vorgeschriebene Anbietung durch öffentliche Stellen an das zuständige Archiv bleibt von alledem unberührt; sie ist von öffentlichen Stellen in jedem Fall durchzuführen. Bewertet das zuständige Archiv die Unterlagen als nicht archivwürdig, so sind sie zu vernichten. Der Nachweis der ordnungsgemäßen Vernichtung ist 30 Jahre lang aufzubewahren, § 5 Abs. 7 Satz 3 Sächsischen Archivgesetz.

Was ist zu tun?

Bei einer vorfristigen Löschung von Vorgängen aufgrund eines Löschungsantrages ist sorgfältig zwischen den Interessen der betroffenen Person und dem Zweck der Aufbewahrungsfrist abzuwägen.

4 Pflichten Verantwortlicher und Auftragsverarbeiter

4.1 Verantwortung für die Verarbeitung, Technikgestaltung

4.1.1 Einwilligungspflicht für Google Tag Manager

↗ DSGVO, TTDSG

Ein immer wiederkehrender Dienst bei Beschwerden oder bei der Beratung von Verantwortlichen ist der Google Tag Manager. Der Google Tag Manager ist ein Tool, welches Ersteller einer Website dabei unterstützt, weitere Bestandteile der Website, zum Beispiel Programmcode oder Dienste, bei Bedarf nachzuladen und zu verwalten. Das Produkt wird von der Firma Google angeboten und ist bei vielen komplexen Websites zu finden, welche in dieser oder jener Form Marketing betreiben. Oftmals wird der Google Tag Manager ohne Einwilligung als „erforderlich" eingebunden, meist mit dem Hinweis, dass der Google Tag Manager selbst keine Cookies setzt.

Dies ist in vielen Fällen soweit richtig, allerdings stellt der Google Tag Manager eine Verbindung zu Google-Servern her, um Ausführungscode zu laden. Dabei werden die IP-Adresse sowie Gerätedaten an Google übertragen. Bis zum In-Kraft-Treten des EU-US Data Privacy Framework im Juli 2023 war ein einwilligungsfreier Einsatz des Google Tag Managers bereits aufgrund der möglichen Verarbeitung personenbezogener Daten in den USA bzw. aufgrund des rechtlichen Durchgriffs US-amerikanischer Behörden auf außerhalb der USA gespeicherter Daten US-amerikanischer Firmen nicht möglich (Schrems II – Urteil des EuGH, Urteil v. 16. Juli 2020, C-311/18).

Dies hat sich trotz des neuen Abkommens auch nicht geändert. Eine einwilligungsfreie Verarbeitung würde die Anwendung der Rechtsgrundlage des Art. 6 Abs. 1 Buchst. f DSGVO (berechtigtes Interesse) erfordern. Bereits beim berechtigten Interesse können berechtigte Zweifel angemeldet werden. Die Nutzung des Dienstes von Google ist zwar sehr bequem, gut dokumentiert und weit verbreitet, aber sie ist keinesfalls alternativlos. Die Steuerung und Verwaltung der Abfolge und Verwendung von Programmcode kann auch mit anderen Werkzeugen, zum Beispiel Eigenentwicklungen, offener Software oder Einwilligungsmanagement-Tools, erfolgen. Die verbreitete Nutzung des Tag Managers von Google hat sicherlich auch etwas mit der Marktmacht von Google und wirtschaftlichen Zwängen bei der Vermarktung von Online-Inhalten zu tun. Aufsichtsbehörden sind nicht befugt, über die Nutzung von bestimmten Tools zu entscheiden, sie haben aber die Rechtsgrundlage zu prüfen.

Wenn trotz der geschilderten Bedenken ein berechtigtes Interesse angenommen wird, ist eine Abwägung zwischen den Interessen des Verantwortlichen an einer Übermittlung und Datenverarbeitung und den Risiken für Betroffene vorzunehmen. Bei einer Übermittlung an Google als einem der weitverbreitetsten Akteure im Internet und dem Geschäftsmodell der Sammlung von Daten zur wirtschaftlichen Eigennutzung ist ein hohes Risiko gegeben. Google gibt an, dass Daten zur Verbesserung der eigenen Dienste verwendet werden. Auch wenn der Google Tag Manager als Auftragsverarbeitung angeboten wird, wird bereits hier deutlich, dass ein solches Auftragsverhältnis nicht den Vorgaben des Art. 28 DSGVO entsprechen kann.

Weiterhin findet, auch wenn derzeit ein Datenexport in die USA prinzipiell rechtlich möglich ist, nach Angaben von Google eine weltweite Datenverarbeitung statt, darunter in Ländern wie Taiwan, den Philippinen und Indien. Für zahlreiche dieser Exportländer gibt es keinen Angemessenheitsbeschluss der Europäischen Union.

Neben der Frage der Zulässigkeit nach DSGVO muss auch geprüft werden, ob Tatbestände aus dem Telekommunika-

Was ist zu tun?
Verantwortliche für Websites dürfen den Google Tag Manager nicht ohne Einwilligung einsetzen. Wenn ein Erfordernis für das Verwalten von Website-Tags besteht, sollten einwilligungsfreie Alternativen geprüft werden. Das Hosting einer Tag-Verwaltung im Eigenbetrieb ist in aller Regel einwilligungsfrei.

tion-Telemedien-Datenschutz-Gesetz (TTDSG) einschlägig sind. Werden Speicherungen und/oder Auslesevorgänge auf oder aus dem Endgerät vorgenommen, ist eine gesonderte Einwilligung nach § 25 TTDSG erforderlich. Die Ausnahmetatbestände aus § 25 Abs. 2 TTDSG sind aus den oben genannten Gründen nicht einschlägig.
Als Fazit bleibt also festzuhalten, dass die Nutzung des Google Tag Managers ohne Einwilligung zu einer rechtswidrigen Verarbeitung und damit einem Datenschutzverstoß führt.

4.1.2 Was ist bei der Einbindung von Zahlungsdienstleistern in Websites und Apps zu beachten?

↗ DSGVO, TTDSG

In diesem Jahr erreichten meine Behörde relativ häufig Beschwerden über die Einbindung von Zahlungsdienstleistern in Websites und Apps. Kern der Beschwerden war häufig eine als Datenschutzproblem wahrgenommene Übermittlung von Nutzungsdaten an solche Dienstleister und das Setzen von zahlreichen Cookies, gegen die oftmals keine Möglichkeit der Abwahl bestand.
Die Art und Weise, wie die Zahlungsdienstleister eingebunden waren, hielt bei der Überprüfung der Beschwerden einer datenschutzrechtlichen Kontrolle häufig nicht stand. Die Beschwerden waren in vielen Fällen berechtigt. Im Anhörungsverfahren haben viele Verantwortliche, allesamt Online-Shops, welche natürlich ein starkes Interesse an einer guten Sichtbarkeit und einfachen Verfügbarkeit möglichst vieler Zahlungsmöglichkeiten haben, angegeben, dass sie wenig Einfluss auf die Datenflüsse nehmen können und auch das Cookie-Verhalten nur eingeschränkt steuerbar ist.
Nichtsdestotrotz muss die Einbindung von Zahlungsmöglichkeiten auch bei einem hohen Interesse seitens der Betreiber von Online-Shops an möglichst vielen und unkomplizierten Bezahlarten den datenschutzrechtlichen Standards entsprechen. Dabei ist zu unterscheiden zwischen der Bewertung nach Datenschutz-Grundverordnung (DSGVO) und der nach

Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG). Beide Normen sind relevant, da Zahlungsdienstleister nicht ohne die Verwendung von Cookies oder sonstigen Eingriffen in das Endgerät eines Kunden auskommen.

Eine Bewertung nach DSGVO lässt zunächst den scheinbar einfachen Schluss zu, alle Zahlungsdienstleister in das Cookie-Banner zu integrieren und eine Einwilligung abzufragen, um auf der „sicheren Seite" zu sein. Aufgrund der Anforderung einer einfachen Möglichkeit, alle einwilligungsbedürftigen Datenverarbeitungen mit einem Klick abzulehnen, erweist sich das jedoch als praxisuntauglich, da eine abgelehnte Einwilligung dann dazu führt, dass am Ende nicht bezahlt werden kann, was weder im Interesse des Händlers noch des Kunden liegen dürfte. Die Alternative, alle Zahlungsdienstleister als erforderlich im Sinne eines berechtigten Interesses nach Art. 6 Abs. 1 Buchst. f DSGVO zu erklären und damit nicht abwählbar in die Website einzubinden, hält keiner Prüfung stand. Dies war oftmals der Ausgangspunkt der oben erwähnten Beschwerden, dass Kunden sich darüber beschwerten, dass bereits beim bloßen Besuch eines Online-Shops Daten an Paypal, Amazon oder weitere Zahlungsanbieter übertragen wurden. Eine beim Berufen auf das berechtigte Interesse aus Art. 6 Abs. 1 Buchst. f DSGVO erforderliche Abwägung mit den Interessen der betroffenen Person fällt stets zugunsten der betroffenen Person aus. Zum einen ist eine Übermittlung an Dritte zum Zweck der Abwicklung von Zahlungen beim einfachen Besuch eines Online-Shops genau so wenig erforderlich wie das Auslesen der Kreditkarte beim Betreten eines Ladens in der analogen Welt, da noch gar keine Kauf- und damit Zahlungsabsicht angenommen werden kann. Selbst wenn man diese Erforderlichkeit annehmen würde, wäre die Übermittlung mit hohen Risiken aufseiten des Betroffenen verbunden, da viele Zahlungsdienstleister Datenschutzerklärungen haben, bei denen sämtliche Daten zu weitreichenden Zwecken verarbeitet werden. Ein pauschales berechtigtes Interesse muss daher verneint werden.

Nach den Maßstäben des TTDSG fällt eine Bewertung in aller Regel noch eindeutiger aus, da viele Zahlungsdienstleister

unmittelbar mit der ersten Verbindung zum jeweiligen Server zahlreiche, zum Teil sehr langlebige und eindeutig pseudonyme Cookies setzen bzw. bereits vorhandene auslesen. Ein Ausnahmetatbestand nach § 25 Abs. 2 TTDSG ist hierfür nicht vorhanden, es sei denn, der Kunde hat die Zahlungsart und den Zahlungsdienstleister aktiv ausgewählt.

Was ist zu tun?
Verantwortliche für Websites müssen die Einbindung von Zahlungsdiensten auf datenschutzrechtliche Aspekte prüfen. Insbesondere müssen Art und Weise sowie Zeitpunkt der Einbindung jedes genutzten Zahlungsdienstes auf Erforderlichkeit und eine ausreichende Willenserklärung des Kunden überprüft werden.

Die Zahlungsanbieter datenschutzkonform einzubinden, stellt in Beschwerdeverfahren für Online-Shops in der Praxis oftmals einen erheblichen Aufwand dar. Dies ist möglich, es muss jedoch – und zwar bezogen auf jede Übermittlung an einen konkreten Dienstleister – erforderlich und ausdrücklich vom Kunden erwünscht sein. Ansonsten trägt der Online-Shop nur zu einer zielgerichteten Datenerfassung und -verarbeitung der ohnehin marktbestimmenden Dienstleister bei und riskiert eine Beschwerde.

4.1.3 Videokonferenzdienst Cisco WebEx Cloud

↗ Art. 5 Abs. 1 Buchst. b, c, f DSGVO; Art. 5 Abs. 1 Buchst. a in Verbindung mit Art. 6 Abs. 1 Buchst. e DSGVO; Art. 5 Abs. 2 DSGVO; Art. 31 in Verbindung mit 58 Abs. 1 Buchst. a DSGVO; Art. 32 DSGVO

Tätigkeitsbericht 2021:
↗ sdb.de/tb2021

Wie bereits im Tätigkeitsbericht 2021 (4.1.5, Seite 124 ff.) beschrieben, war und ist der Betrieb des Videokonferenzdienstes Cisco WebEx Cloud aus meiner Sicht im Freistaat Sachsen nicht datenschutzkonform umgesetzt.

Im Januar 2023 habe ich mit der förmlichen Prüfung des Produktes Cisco WebEx Cloud begonnen. Der Staatsbetrieb Sächsische Informatik Dienste (SID) erhielt von mir Hinweise zu Verstößen gegen die DSGVO. Er erbringt den Videokonferenzdienst Cisco WebEx Cloud im Auftrag der Staatsverwaltung im Freistaat Sachsen. Für Web- und Videokonferenzen besteht eine Leistungspflicht des SID und ein Kontrahierungszwang für die Behörden und Einrichtungen der Staatsverwaltung. Der SID entscheidet über die Zwecke und Mittel der Verarbeitung.

Grundsätzlich war zunächst die vertragliche Situation zu klären.

Meine Hinweise beziehen sich auf Verstöße gegen die Einhaltung des Rechtmäßigkeitsgrundsatzes und die angemessene Sicherheit bei der Verarbeitung personenbezogener Daten von Teilnehmenden und der organisierenden Personen durch den SID beim Anbieten des Videokonferenzdienstes Cisco WebEx gegenüber öffentlichen Stellen.

Für die in der Auftragsverarbeitung vorgesehenen Produktverbesserungen mit „Weitergaben" gibt es meines Erachtens keine Rechtsgrundlage.

Der Einsatz speziell des Produktes Cisco WebEx Cloud ist nicht erforderlich. Die Unterarbeitsgruppe Webkonferenzdienst des Arbeitskreises Sächsisches Verwaltungsnetz (UAG) hat im Jahr 2021 risikoärmere und datenschutzkonformere Videokonferenzdienstleister in einem Vergleich verschiedener Anbieter festgestellt. Zudem sind auch Telefonkonferenzen für Besprechungen einsetzbar.

In Bezug auf die geplante Anonymisierung von personenbezogenen Daten gibt es keine Rechtsgrundlage für den Zweck der Produktverbesserung für öffentliche Stellen in Sachsen. Darüber hinaus gab und gibt es keine transparente Analyse oder Bewertung von Risiken der Anonymisierung durch den SID. Die rechtliche Sicherung der Anonymität durch eine vertragliche Vereinbarung mit dem Auftragsverarbeiter, wie beispielsweise ein Verbot der De-Anonymisierung mit einer Vertragsstrafe, existiert nicht. Die Daten, welche anonymisiert werden sollten, wurden nicht präzise vom SID beschrieben. Es erfolgt keine Beschränkung der Weitergabe und der Weiterverarbeitung auf konkrete Verarbeiter und bestimmte Zwecke.

Außerdem erging der Hinweis an den SID, dass Informationen durch den Verantwortlichen in den Räumlichkeiten der Sächsischen Datenschutz- und Transparenzbeauftragten bereitzustellen sind, Art. 31 DSGVO in Verbindung mit Art. 58 Abs. 1 Buchst. a DSGVO. Der SID bzw. dessen Auftragsverarbeiter vertreten die Auffassung, dass bestimmte Unterlagen nur in den Räumlichkeiten des Auftragsverarbeiters eingesehen werden dürften.

Die Stellungnahme des SID zu meinen Hinweisen erfolgte im Juni 2023. Er verwies hinsichtlich des Zwecks der „Produktverbesserung" auf den Supportfall im eigenen Betrieb, zur Verbindungs- und Betriebsverbesserung sowie auf die Cybersicherheit. Gegen diese Auslegung des SID spricht der Wortlaut der geplanten „Weitergabe" in der Auftragsverarbeitungsvereinbarung. Diese stellt im Sinne einer datenschutzrechtlichen Übermittlung keine Verarbeitung für eigene Zwecke dar. Die Systematik und der Inhalt der Auftragsverarbeitung sprechen zudem gegen die erfolgte Auslegung durch den SID (Produktverbesserung = Support und/oder Cybersicherheit). Die Zwecke Support und Cybersicherheit werden an anderer Stelle in der Auftragsverarbeitungsvereinbarung geregelt als der Zweck Produktverbesserung.

Hinsichtlich der Nutzung von risikoärmeren Diensten gegenüber der Cisco WebEx Cloud bezieht der SID nicht die Möglichkeit von Telefonkonferenzen zum Austausch von Informationen mittels Fernkommunikation in seine Betrachtung mit ein. Er nimmt Bezug auf die „Anforderungen der Staatsregierung" und verkennt dabei meiner Ansicht nach, dass sich aus rechtlicher Sicht die Anforderungen aus der DSGVO ergeben. Sicherlich wäre es sinnvoll, den Bedarf bei den Vertragspartnern des SID (Kontrahierungszwang für Behörden und Einrichtungen der Staatsverwaltung) zu erfragen. Die Staatsregierung ist nicht zuständig bzw. verantwortlich im Sinne der DSGVO für die Festlegung von Anforderungen für informationstechnische Leistungen.

Weiter vertritt der SID die Auffassung, dass er aus „methodischen Gründen" der Ansicht der UAG hinsichtlich risikoärmerer Dienste nicht folge, da diese „Cloudprodukte" aus Gründen der mangelnden Erfüllung des Datenschutzes bei ihrem Vergleich der Videokonferenzsysteme ausgeschlossen hatte. Es galt jedoch damals wie heute: Die Verwaltung ist in der Ausgestaltung ihrer Verfahren an Recht und Gesetz gebunden, was in der Konsequenz zu einem Ausschluss nicht datenschutzkonformer Dienste führen muss.

Der SID ist in seiner Stellungnahme außerdem der Ansicht, dass die „Einschätzungsprärogative", welche Funktionen zur

Wahrnehmung der Aufgabe erforderlich sind, der Staatsregierung obliege. Da kein Vergleich durch den SID vom Produkt Cisco WebEx mit anderen Videokonferenzprodukten erfolgte, kann ich eine Entscheidung zwischen mehreren Videokonferenzprodukten (Abwägung) schon dem Grunde nach nicht erkennen.

Cisco hat den Verkauf von Lizenzen für On-Premise-Installationen im Juli 2020 eingestellt und somit die Realisierung des Corona-bedingt gestiegenen Bedarfes von einem Produktwechsel auf die Cloud-basierte Lösung abhängig gemacht. Dass die vom SID vorgetragene technologische Weiterentwicklung von „Cisco WebEx On-Premise" zu „Cisco WebEx Cloud" in einem bestehenden Vertrag erfolgt sei, teile ich nicht. Die Entwicklung von On-Premise (lokale Installation in Sachsen im Rahmen des Sächsischen Verwaltungsnetzwerkes) zur Cloud-Lösung (Installation auf internationalen Servern des Anbieters, Mitarbeiter/innen der Landesverwaltung greifen über das Internet auf den Service zu) ist nach meinem Dafürhalten eine Leistungsänderung (unerwartetes Problem, dessen Lösung von der ursprünglichen Leistungsbeschreibung – hier: Betrieb eines Videokonferenzdienstes lokal in den Räumlichkeiten des SVN-Vertragspartners – nicht erfasst ist) und datenschutzrechtlich die Verwendung einer anderen Technologie. Daten können territorial nicht mehr bestimmbaren Servern zugeordnet werden. Es handelt sich gerade nicht um eine Weiterentwicklung, sondern um ein anderes Produkt. Die Änderung des Inhalts eines Schuldverhältnisses ist gemäß § 311 Abs. 1 Bürgerliches Gesetzbuch selbst ein Vertrag und damit grundsätzlich nur einvernehmlich möglich. Der SID hätte daher aus meiner Sicht die Leistung neu vergeben können und müssen.

Ein erstes Rechtsgespräch mit dem SID erfolgte im Sommer 2023. Die Untersuchungen sind noch nicht abgeschlossen, so sind insbesondere weitere Informationen zur Ermöglichung einer vollständigen datenschutzrechtlichen Untersuchung erforderlich, die meiner Behörde noch nicht bereitgestellt wurden.

Was ist zu tun?

Achten Sie bitte auf die Dokumentation der Verträge mit ihren Auftragnehmern (Überleitung von Schuldverhältnissen) und die Anpassung der dazugehörigen Auftragsverarbeitungsvereinbarungen.
Für öffentliche Stellen gibt es keine Rechtsgrundlage für Produktverbesserungen.
Beachten Sie den Rechtsgrundsatz der Erforderlichkeit.
Prüfen Sie die Alternativen der Besprechung vor Ort oder der Telefonkonferenz.
Die Anonymisierung von personenbezogenen Daten bedarf einer Risikobewertung. Anonymisieren ist das Verändern personenbezogener Daten in der Weise, dass sie nicht mehr oder nur mit einem unverhältnismäßigen Aufwand einer bestimmten oder bestimmbaren Person zugeordnet werden können.
Achten Sie auf Änderungen der Leistungen (neue Technologie).

4.1.4 Datenschutz bei auf Kinder ausgerichteten Internetdiensten

↗ § 25 TTDSG; Art. 5 Abs. 1 Buchst. a in Verbindung mit Art. 6 Abs. 1 DSGVO; Art. 5 Abs. 1 Buchst. b, c, e, f DSGVO; Art. 5 Abs. 2, Art. 7, 8, 12, 13, 21, 24, 25, 32 Abs. 2, 44, 48 DSGVO

Durch eine Datenpanne, die Beschwerde eines Petenten sowie die Berichterstattung in verschiedenen Medien wurde ich auf ein sächsisches Unternehmen aufmerksam, das sich mit neu angebotenen Internetdiensten in Form eines Schülerplaners (Stundenplaneingabe, Hausaufgabeneintrag, Chatmöglichkeit, Persönlichkeitstest) an Kinder in Deutschland wandte. Konkret ging es um eine kostenlos angebotene App sowie den Betrieb einer Internetplattform durch das Unternehmen.
Die Zielgruppe wurde von dem Unternehmen in der Presse mit Kindern im Alter von 12 bis 18 Jahren angegeben.
Zudem stellte ich fest, dass bereits, unmittelbar nachdem die App aufgerufen wurde, mehrere externe Dienste von Dritten, wie beispielsweise einem Chatdienst, gestartet wurden, obwohl der/die Nutzer/in diese Dienste nicht wünschte. Bei der Überprüfung der Internetplattform stellte ich dies ebenfalls fest. Der Nutzerwunsch war und ist hinsichtlich der Speicherung von Informationen in der Endeinrichtung der Nutzerin bzw. des Nutzers oder des Zugriffs auf Informationen maßgeblich, § 25 Abs. 2 Nr. 2 TTDSG. Wird der Nutzerwunsch nicht berücksichtigt, hat dies auch Auswirkungen auf die Rechtmäßigkeit der nachfolgenden Verarbeitung von personenbezogenen Daten.
Erforderliche Einwilligungen der Kinder wurden von dem Unternehmen nicht wirksam eingeholt. Die Datenschutzinformationen wiesen für die App und für das Internetportal zudem wesentliche Mängel auf.
Nachdem dem Unternehmen die Gelegenheit zur Stellungnahme von meiner Seite eingeräumt wurde, stellte es die Startabläufe für Dienste bei der App und dem Internetportal im März 2022 nach eigenen Angaben unter Berücksichtigung des Nutzerwunsches um. Es wurde für Kinder unter 16 Jahren eine weitere App eingeführt, welche kostenpflichtig und nur

mit der Einwilligung der Eltern genutzt werden konnte. Bei der kostenlosen App wurde eine Selbstbestätigung durch die Möglichkeit des Anklickens eines Buttons mit der Aufschrift „Ich bin 16 Jahre alt" eingeführt.

Die ergriffenen Maßnahmen führten nicht zu einer Änderung meiner Bewertung hinsichtlich der Beeinträchtigung der Privatsphäre und der Persönlichkeitsrechte der Kinder durch das Anbieten der App und des Internetportals. Aus meiner Sicht nutzten Kinder unter 16 Jahren weiterhin die kostenlose werbefinanzierte App und das Internetportal. Die kostenpflichtige App fand dagegen keinen Anklang bei den Kindern. Das grundsätzliche Problem der wirksamen Altersabfrage wurde meiner Meinung nach von dem Unternehmen nur kaschiert und nicht rechtskonform gelöst. Es duldete meiner Ansicht nach die Falscheingabe des Alters von Kindern unter 16 Jahren (offenkundige Tatsache bei Altersangabe im Internet). Es ließ sie trotzdem zur Nutzung der App und des Internetportals zu. Chatgruppennamen wie beispielsweise „Mädchen von 10–13", „Für Fünftklässler" oder „alle über 12" wiesen auf die nutzenden Kinder im Alter von unter 16 Jahren hin. Im bereits bekannten Fall des Missbrauchs ist eine Altersverifikation durch eine Selbstbestätigung nach meinem Dafürhalten ungeeignet. Sie führt aus meiner Sicht zu schwebend unwirksamen Verträgen mit der Folge des Nichtvorliegens der Rechtsgrundlage für eine Verarbeitung personenbezogener Daten. Auch die eingeholten Einwilligungen von Kindern im Alter von unter 16 Jahren waren weiterhin unwirksam, Art. 8 Abs. 1 DSGVO.

Die vom Unternehmen angeführte Literaturauffassung, dass die Frage „Wie alt bist du?" ausreiche und eine weitere Altersverifikation aufgrund der Vertragsbedingungen nicht erforderlich sei, kam meiner Auffassung nach aufgrund der vorliegenden Einzelumstände, die auf einen offensichtlichen Missbrauch hinwiesen, bereits nicht in Betracht. Vielmehr habe ich mich in diesem Fall der Meinung angeschlossen, dass einfache Schutzmaßnahmen, wie eine Selbstbestätigung des Alters oder Vertragsbedingungen, wonach nur Personen über 16 Jahren Nutzer/innen sein dürfen, nicht

ausreichen, sondern angemessene Anstrengungen zu unternehmen sind, die die verfügbare Technik berücksichtigen [siehe hierzu Leupold/Wiebe/Glossner, IT-Recht, 4. Auflage 2021, Teil 15.3 Social Media und Datenschutz Rn 81, beck-online mit Verweis auf Paal/Pauly/Frenzel, DS-GVO/BDSG, Art. 8 Rn. 13; Kühling/Buchner/Buchner/Kühling, DS-GVO/BDSG, Art. 8 Rn. 23; Möhrke-Sobolewski/Klas, K&R 2016, 373 (377)]. Nur so kann eine wirksame Einwilligung oder ein Vertrag als Rechtsgrundlage im konkreten Fall sichergestellt werden. Die mangelhafte Vertragsanbahnung führte meiner Meinung nach schon zu schuldrechtlich schwebend unwirksamen Verträgen.

In einem gemeinsamen Erörterungstermin räumte das Unternehmen im Beisein seines Datenschutzbeauftragten sowie des anwaltlichen Vertreters weiter ein, dass eine Überwachung der Kommunikation der Kinder durch beauftragte Dienstleister in den USA anlasslos erfolgte. Neben der Frage der Zulässigkeit des Drittstaatentransfers wies ich daher das Unternehmen auf die Unzulässigkeit der Chatkontrolle hin, da hier regelmäßig eine große Anzahl von personenbezogenen Daten anfallen. Kinder rechnen im Übrigen nicht mit einer Überwachung der Kommunikation. Das Unternehmen erhielt von mir nochmals die Möglichkeit, abschließend zu den von mir erteilten Hinweisen Stellung zu nehmen und vorgenommene Änderungen mitzuteilen. Es beharrte aber letztendlich auf seinen Rechtspositionen, was insbesondere die Überwachung der Kommunikation der Kinder, die Zulässigkeit des Drittstaatentransfers und die angebliche Wirksamkeit von Einwilligungen und von Verträgen mit Kindern anging.

Es erfolgten zwei weitere Überprüfungen der App und des Internetportals Ende 2022 und Anfang 2023. Leider musste ich hierbei im Rahmen der Prüfung im März 2023 feststellen, dass wieder Verbindungen zu Drittdiensten beim Aufruf der App erfolgten, obwohl die minderjährigen Nutzer/innen noch nicht einmal den Wunsch für eine Registrierung geäußert hatten. Das Unternehmen entschuldigte den zweiten Vorfall dieser Art mit einer technischen Panne und stellte den Mangel ab.

Insgesamt wurden 12 Verstöße des Unternehmens im Zeitraum Januar 2022 bis März 2023 durch mich festgestellt. Sie betrafen den § 25 TTDSG sowie die Art. Art. 5 Abs. 1 Buchst. a in Verbindung mit Art. 6 Abs. 1 DSGVO; Art. 5 Abs. 1 Buchst. b, c, e und f DSGVO; Art. 5 Abs. 2 DSGVO; Art. 7 DSGVO; Art. 8 DSGVO; Art. 12 und 13 DSGVO; Art. 21 DSGVO; Art. 24 DSGVO und Art. 25 DSGVO; Art. 32 Abs. 2 DSGVO; Art. 44 DSGVO und Art. 48 DSGVO.

Das verwaltungsrechtliche Verfahren endete im Mai 2023 mit einer Verwarnung gemäß Art. 58 Abs. 2 Buchst. b DSGVO gegenüber dem Unternehmen.

Durch eine Verwarnung wird keine konkrete, unmittelbare Rechtspflicht ausgelöst. Mit einer Verwarnung wird implizit ausgedrückt, dass sich der Adressat künftig datenschutzkonform verhalten soll (Verwaltungsgericht Mainz, Urteil vom 24.05.2020, Az. 1 K 647/19.MZ, Rdnr. 16). Im verfahrensgegenständlichen Fall betraf die Verwarnung das Verhalten des Unternehmens beim Anbieten der App sowie des Internetportals gegenüber nicht volljährigen Nutzerinnen und Nutzern in der Bundesrepublik Deutschland.

Das Unternehmen hat gegen diese Verwarnung den Rechtsweg vor dem Verwaltungsgericht Dresden beschritten.

Was ist zu tun?

Es ist selbstverständlich, dass bei einem neuen Geschäftsmodell die rechtlichen Rahmenbedingungen sondiert und von Anfang an der Datenschutz bei der Entwicklung neuer Internetdienste beachtet wird, bevor eine App oder eine Internetplattform in der EU angeboten wird. Selbst gut gemeinte Kontrollmechanismen sind mit den Persönlichkeitsrechten der Betroffenen in Einklang zu bringen.

4.1.5 Offener E-Mail-Verteiler

↗ Art. 5 Abs. 1 Buchst. c und Art. 6 Abs. 1 DSGVO

In meinem Tätigkeitsbericht Datenschutz 2022 (4.4.1, Seite 143 ff.) führte ich aus, dass bei einem offenen E-Mail-Verteiler die versehentliche Eintragung von E-Mail-Adressen in das Kopie-Feld (Cc) eine der typischen Datenschutzverletzungen ist, die bei mir nach Art. 33 Datenschutz-Grundverordnung (DSGVO) durch die jeweils Verantwortlichen im Sinne von Art. 4 Nr. 7 DSGVO zur Anzeige kommen.

Möglich ist aber auch, dass bewusst eine Vielzahl von E-Mail-Adressen in das Kopie-Feld aufgenommen wird. Eine weitere Konstellation des offenen E-Mail-Verteilers können Gruppen-E-Mails sein, mit denen gleichgelagerte Kurzinformationen an einen größeren Kreis von Adressaten übersandt

Tätigkeitsbericht Datenschutz 2022:

↗ sdb.de/tb2022

werden (zum Beispiel die E-Mail einer Klassenlehrerin/eines Klassenlehrers an die Eltern ihrer/seiner Schüler/innen).
Sofern die Versendung einer Nachricht in einem offenen E-Mail-Verteiler absichtlich erfolgt, will ich nicht ausschließen, dass dies zum Teil in Unkenntnis darüber geschieht, dass dies ein datenschutzrechtliches Problem darstellt.
E-Mail-Adressen, die den Vor- und Nachnamen enthalten, als auch E-Mail-Adressen, die aus selbst erdachten Namen oder sonstigen Kürzeln bestehen, sind personenbezogene Daten, da sich die ihnen zuordenbaren Personen mit weiterem Wissen und Erkenntnissen identifizieren lassen.
Durch die Versendung von E-Mails mit einem offenen Verteiler werden die E-Mail-Adressen aller Empfänger allen anderen Empfängern bekannt gegeben; mithin werden die personenbezogenen Daten durch den Absender verarbeitet.
In der Regel wird für die Verarbeitung keiner der gesetzlichen Erlaubnistatbestände des Art. 6 Abs. 1 Buchst. b bis f DSGVO in Betracht kommen, weshalb die Verwendung einer E-Mail-Adresse in einem offenen E-Mail-Verteiler nur dann möglich ist, wenn jede/r einzelne Inhaber/in der verwandten E-Mail-Adresse in die Verwendung eingewilligt hat. Die Verwendung einer E-Mail-Adresse ohne eine Einwilligung und ohne das Vorliegen eines der Erlaubnistatbestände des Art. 6 Abs. 1 Buchst. b bis f DSGVO stellt einen datenschutzrechtlichen Verstoß dar, der mit einem Bußgeld gemäß Art. 83 Abs. 5 Buchst. a DSGVO geahndet werden und/oder weitere aufsichtsrechtliche Maßnahmen gemäß Art. 58 Abs. 2 DSGVO zur Folge haben kann.
Anders zu betrachten und zu bewerten ist aus meiner Sicht der Fall, wenn dienstliche E-Mail-Adressen entweder innerhalb einer Behörde oder durch eine Bürgerin oder einen Bürger in einem offenen E-Mail-Verteiler verwendet werden. Im Fall einer dienstlichen E-Mail-Adresse handelt es sich zwar auch um personenbezogene Daten, jedoch hat diese ein geringeres Schutzniveau, weil sie für die Kommunikation innerhalb einer Behörde sowie für die öffentliche Kommunikation mit den Bürgerinnen und Bürgern oder anderen Behörden bestimmt ist.

Zur Verwendung von dienstlichen E-Mail-Adressen in einem offenen Verteiler war bei mir im Berichtszeitraum die Anzeige einer Behörde eingegangen. Nach dem mir gegenüber angezeigten Sachverhalt hatte der Verantwortliche in mehreren E-Mails mehr als 30 E-Mail-Adressen von Bediensteten verschiedener Behörden in den Verteiler aufgenommen.
In diesem Fall bestand aus meiner Sicht das Problem darin, dass ich aufgrund des Anliegens des Absenders nicht davon ausgehen konnte, dass mehr als 30 Personen in unterschiedlichen Behörden mit seinem Anliegen betraut sind. Mit Blick auf den Grundsatz der Datenminimierung nach Art. 5 Abs. 1 Buchst. c DSGVO, dessen Nichteinhaltung ein Aufsichtsverfahren nach sich ziehen kann, war die Aufnahme von mehr als 30 Mitarbeiterinnen und Mitarbeitern in den offenn E-Mail-Verteiler hier nicht erforderlich. Ein Verstoß gegen den Grundsatz der Minimierung ist gegebenenfalls auch geeignet, ein Ordnungswidrigkeitsverfahren nach sich zu ziehen.
Weitere Hinweise zum Thema E-Mail-Versand sind in der Orientierungshilfe „Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail" der Datenschutzkonferenz zusammengestellt, abrufbar unter sdb.de/tb2302.
Vgl. auch den Tätigkeitsbericht 2019, 4.1.3, Seite 82 ff.

Was ist zu tun?
Verantwortliche haben sicherzustellen, dass personenbezogene E-Mail-Adressen nicht ohne Einwilligung Dritten zur Kenntnis gegeben werden. Liegt keine Einwilligung vor, ist die Vertraulichkeit der E-Mail-Adressen zu gewährleisten, indem die Empfängeradressen in das sogenannte Bcc-Feld eingetragen werden. Hinterfragt werden sollte stets, ob jeder, dessen E-Mail-Adresse in einer Mitteilung aufgenommen werden soll, tatsächlich auch zu beteiligen ist.

4.1.6 Aufbewahrungspflicht der Kammer für Patientenunterlagen

↗ Sächsisches Heilberufekammergesetz

Schon zu Zeiten meines Amtsvorgängers hatte sich meine Behörde stets darum bemüht, eine normenklare Zuständigkeitsregelung für die leider immer wieder auftretenden Fälle zu erreichen, in denen sich niemand für den Schutz von Patientenunterlagen verantwortlich sieht, wenn eine Arztpraxis – aus welchen Gründen auch immer – geschlossen werden muss. Auch Insolvenzverwalter/innen kommen dann im Rahmen der Abwicklung einer Praxis gerne auf mich zu und verlangen eine Inobhutnahme der Patientenunterlagen seitens meiner Behörde.

Stets habe ich dabei darauf hingewiesen, dass es sich bei der Sicherungspflicht von Patientenunterlagen vorrangig nicht um eine datenschutzrechtliche Frage handelt, sondern um die Einhaltung einer Berufspflicht. So ist in § 20 Sächsisches Heilberufekammergesetz für ein Kammermitglied eindeutig als Berufspflicht normiert, über die in Ausübung ihres Berufes getroffenen Feststellungen und Maßnahmen die erforderlichen Aufzeichnungen zu fertigen, die Aufzeichnungen sowie sonstigen Patientenunterlagen aufzubewahren und nur für Berechtigte zugänglich zu machen.

Stellungnahme zum Gesetzentwurf über die berufsständische Vertretung der Heilberufe im Freistaat Sachsen:
↗ sdb.de/tb2303

Mit der zum 1. August 2023 in Kraft getretenen Novellierung des Sächsischen Heilberufekammergesetzes vom 5. Juli 2023 (SächsGVBl. Seite 559), zu dessen Entwurf ich gerade auch in Bezug auf diese Thematik Stellung genommen habe (siehe Schreiben vom 11. August 2022, LT-Drs. 7/11882 Seite 97 f.), findet sich im Aufgabenkatalog der Kammer in Absatz 3 des § 7 nunmehr folgende Regelung:

> „(3) [1]Die Kammern haben Patientenakten nach § 20 Absatz 1 Satz 2 Nummer 2 aufzubewahren, wenn ein Mitglied oder dessen Rechtsnachfolger nicht in der Lage ist, diese ordnungsgemäß zu verwahren. [2]Sie können andere Mitglieder oder geeignete Dritte mit der Erfüllung dieser Aufgabe betrauen sowie gemeinsame Einrichtungen zur Erfüllung dieser Aufgabe errichten oder nutzen. [3]Die Kammern oder von diesen nach Satz 2 Beauftragte können von dem Mitglied oder dessen Rechtsnachfolger Kostenerstattung verlangen. [4]§ 1936 des Bürgerlichen Gesetzbuches bleibt unberührt."

Was ist zu tun?
§ 7 Absatz 3 Sächsisches Heilberufekammergesetz sieht eine Aufbewahrungspflicht der Kammer in Bezug auf Patientenakten vor.

4.1.7 Auslegung der Vorschlagsliste zur Schöffenwahl

↗ § 36 GVG, § 37 Abs. 1 SächsGemO, Art. 9 und 13 DSGVO, VwV Schöffen- und Jugendschöffenamt

Das ehrenamtliche Amt der Schöffin bzw. des Schöffen und Jugendschöffen ist ein wichtiger Beitrag zur richterlichen Urteilsfindung. Sie werden unter den an dem Amt interessierten Bewerberinnen und Bewerbern aus der Mitte der jeweiligen

Gemeinde/Stadt für fünf Jahre gewählt, § 36 Gerichtsverfassungsgesetz (GVG).
§ 36 GVG lautet:

> „(1) Die Gemeinde stellt in jedem fünften Jahr eine Vorschlagsliste für Schöffen auf. Für die Aufnahme in die Liste ist die Zustimmung von zwei Dritteln der anwesenden Mitglieder der Gemeindevertretung, mindestens jedoch der Hälfte der gesetzlichen Zahl der Mitglieder der Gemeindevertretung erforderlich. Die jeweiligen Regelungen zur Beschlussfassung der Gemeindevertretung bleiben unberührt.
> (2) Die Vorschlagsliste soll alle Gruppen der Bevölkerung nach Geschlecht, Alter, Beruf und sozialer Stellung angemessen berücksichtigen. Sie muss Familienname, Vornamen, gegebenenfalls einen vom Familiennamen abweichenden Geburtsnamen, Geburtsjahr, Wohnort einschließlich Postleitzahl sowie Beruf der vorgeschlagenen Person enthalten; bei häufig vorkommenden Namen ist auch der Stadt- oder Ortsteil des Wohnortes aufzunehmen.
> (3) Die Vorschlagsliste ist in der Gemeinde eine Woche lang zu jedermanns Einsicht aufzulegen. Der Zeitpunkt der Auflegung ist vorher öffentlich bekanntzumachen. […]"

Die Auswahl der Bewerber/innen für die Vorschlagsliste zur Wahl zum Schöffenamt findet durch den jeweiligen Gemeinderat statt und richtet sich in Sachsen ergänzend zu § 36 GVG nach der Verwaltungsvorschrift Schöffen- und Jugendschöffenamt vom 3. Januar 2023 (VwV Schöffen- und Jugendschöffenamt).
Hierzu muss ein bestimmtes, gesetzlich vorgegebenes Prozedere eingehalten werden. Zunächst wird durch den Gemeinderat geprüft, ob der/die Bewerber/in die genannten Mindestvoraussetzungen erfüllt. Wer die Voraussetzungen erfüllt, wird in die Vorschlagsliste der Schöffinnen und Schöffen übernommen. Der Gemeinderat (bzw. bei Städten meist der Jugendhilfeausschuss) muss die Vorschlagsliste mit

Zweidrittelmehrheit bestätigen, dann wird die Vorschlagsliste erstellt und auslegt, anschließend dem (Amts-)Gericht übergeben. An diesem wählt der unabhängige Schöffenwahlausschuss dann die Schöffinnen und Schöffen aus der Vorschlagsliste aus.
Auch die VwV Schöffen- und Jugendschöffenamt, Abschnitt III., Nummer 12 a) „Öffentliche Einsichtnahme in die Liste" bestimmt hierzu:

> „Die Vorschlagsliste ist in der Gemeinde unverzüglich nach ihrer Aufstellung eine Woche lang zu jedermanns Einsicht aufzulegen (§ 36 Absatz 3 Satz 1 des GVG) […]."

Im Berichtszeitraum hatte ich mich in diesem Zusammenhang in zwei unterschiedlichen, aber gleichermaßen interessanten Fällen mit datenschutzrechtlichen Fragestellungen zu beschäftigen.
Einmal wurde mir durch eine Beschwerde bekannt, dass eine kleinere sächsische Gemeinde die gesamte Vorschlagsliste in dem gemeindlichen Amtsblatt veröffentlichte. Das Amtsblatt dieser Gemeinde wird hybrid – das heißt sowohl papiergebunden als auch online geführt. Dies hatte zur Folge, dass personenbezogene, mitunter sensible Daten (siehe oben § 36 Abs. 2 – unter anderem Wohnanschrift, Alter, Beruf) der Bewerber veröffentlicht worden sind.
In der VwV Schöffen- und Jugendschöffenamt, Abschnitt III., Nummer 12 heißt es unter Buchst. c indes nur:

> „Beginn und Ende der Auslegungsfrist sind vorher öffentlich bekannt zu machen (§ 36 Absatz 3 Satz 2 des Gerichtsverfassungsgesetzes)."

Dass die Vorschlagsliste mit den darin enthaltenen gesamten personenbezogenen Daten der Bewerber/innen zu veröffentlichen ist – davon ist in den gesetzlichen Bestimmungen aber gerade nicht die Rede.
Ich musste der Gemeinde somit mitteilen, dass die ihrerseits gewählte Vorgehensweise so gesetzlich nicht gedeckt und die Veröffentlichung der Daten von Bewerberinnen und Be-

werbern somit rechtswidrig ist. Sowohl § 36 GVG als auch die zugehörige VwV (siehe oben) sehen vor, dass die Zeit (und der Ort) der Auslegung öffentlich bekannt zu geben ist. Dies bedeutet aber nicht, dass der gesamte Beschluss samt Inhalt der Vorschlagsliste und der personenbezogenen Daten der Bewerber/innen bekannt gegeben werden muss und darf.

Die Gemeinde hat auf meine Intervention hin eingelenkt und zunächst die personenbezogenen Daten der Bewerber aus dem online eingestellten Amtsblatt entfernt. Auch dies konnte aber zur Wahrung des Datenschutzes noch nicht genügen. Ich musste die Gemeinde nochmals anschreiben und auffordern, den gesamten Beschluss (dieser enthält zwingenderweise die Namen der Kandidaten) aus dem Amtsblatt komplett zu entfernen, denn selbst der Name der vorgeschlagenen Bewerber/innen darf nicht veröffentlicht werden. Deshalb wird dieser im Gemeinderat gerade nicht öffentlich behandelt. Hierzu im Einzelnen sogleich.

Die Gemeinde ist sodann sämtlichen Forderungen meinerseits gefolgt, hat den Beschluss komplett entfernt und zugesichert, in den folgenden Wahlperioden die gesetzlichen Vorgaben und den Datenschutz, insbesondere auch die entsprechenden Informationspflichten nach Art. 13 Datenschutz-Grundverordnung, einzuhalten.

Eine andere Gemeinde fragte im Berichtszeitraum konkret nach der Öffentlichkeit oder Nichtöffentlichkeit der Sitzung, in der die Aufstellung der Vorschlagsliste behandelt wird. Schließlich werden in dieser Sitzung persönliche Eigenschaften und Tatsachen der Bewerber/innen besprochen, die zur Eignung bzw. Nichteignung für das Schöffenamt führen. Andererseits gibt es auch Stimmen, die der Auffassung sind, dass die Öffentlichkeit ein Recht hat zu erfahren, wer aus ihrer Gemeinde zum/zur ehrenamtlichen Richter/in berufen wird und wie diese Entscheidung zustande gekommen ist.

Weder die VwV Schöffen- und Jugendschöffenamt, noch § 36 GVG enthalten eine explizite Bestimmung dazu, ob die Auswahl der Bewerber/innen in öffentlicher oder nichtöffentlicher Sitzung zu erfolgen hat.

Gemäß der VwV Schöffen- und Jugendschöffenamt, Abschnitt III Nummer 10 b) „Auswahl der vorzuschlagenden Personen" soll aber

> „bei der Auswahl der Personen berücksichtigt werden, dass das verantwortungsvolle Amt einer Schöffin und eines Schöffen in hohem Maße Unparteilichkeit, Selbstständigkeit und Reife des Urteils, aber auch geistige Beweglichkeit und wegen des anstrengenden Sitzungsdienstes körperliche Eignung verlangt".

Die Befassung mit diesen Kriterien erfasst indes gezwungenermaßen eine Erörterung von persönlichen Eigenschaften und sensiblen Daten der Bewerber/innen, die auch zum Teil Daten besonderer Kategorien nach Art. 9 DSGVO erfassen können (politische Meinungen, Gesundheit und anderes). Selbst charakterliche Eignungen einer Person werden in dieser Befassung teilweise zur Rede gebracht.
In § 37 Abs. 1 der Sächsischen Gemeindeordnung ist festgelegt, dass in nichtöffentlicher Sitzung zu verhandeln ist, wenn das öffentliche Wohl oder berechtigte Interessen Einzelner dies erfordern. Eine spezialgesetzliche Rechtsgrundlage ist auch nicht ersichtlich, die eine öffentliche Erörterung dieser personenbezogenen, zum Teil auch sensiblen Daten erlauben würde.
Die Öffentlichkeit wird vielmehr über die gesetzlich vorgesehene Auslegung der Vorschlagsliste (siehe oben) hinreichend unterrichtet, zudem wird den Bewerberinnen und Bewerbern selbst die Aufnahme bzw. Nichtaufnahme in die Vorschlagsliste individuell samt den Gründen bekannt gegeben (Nummer 10 d VwV Schöffen- und Jugendschöffenamt), damit eine Überprüfbarkeit der gemeindlichen Entscheidung gegeben ist.
Das Interesse der Öffentlichkeit an der Kenntnis, wer zur Schöffin bzw. zum Schöffen berufen wird, wird durch diese Regelung somit hinreichend gewahrt. Interessierte Bürger/innen haben schließlich eine Woche Zeit, sich hierüber zu informieren. Dem Informationsbedürfnis der Bevölkerung ist somit aus meiner Sicht zur Genüge Rechnung getragen. Ein

Tätigkeitsbericht 2017/2018:
↗ sdb.de/tb2109

Was ist zu tun?
Bei der Aufstellung der Vorschlagsliste für das Amt der Schöffin bzw. des Schöffen und Jugendschöffen müssen Gemeinden genauestens auf die Einhaltung des Datenschutzes achten, da für die Auswahl mitunter sensible Daten der Bewerber/innen relevant sein können. Die Verfahrensweise ist gesetzlich genau vorgegeben und darf nicht überschritten werden. Die Behandlung im Rat muss nichtöffentlich erfolgen.

berechtigtes Interesse der Öffentlichkeit zu erfahren, wer dagegen für die Vorschlagsliste abgelehnt wurde und aus welchen Gründen, kann ich nicht ersehen. Über die Auswahl der Bewerber/innen für die Vorschlagsliste zur Wahl zum Schöffenamt ist nach alledem auch nach meiner Einsicht in nichtöffentlicher Sitzung zu verhandeln.
Zudem hat sich bereits im Tätigkeitsbericht 2017/2018 (2.2.5, Seite 174 f.) mein Amtsvorgänger zu der Frage der Veröffentlichung von Vorschlagslisten positioniert und festgestellt, dass gegen die einwöchige Auslegung der Vorschlagsliste keine Bedenken bestehen, wenn aus dieser nicht hervorgeht, wie viele und welche Bewerber/innen nicht in diese aufgenommen worden sind.

4.1.8 (Un-)Angemessene Bekanntmachung eines erteilten Hausverbots in einer Pflegeeinrichtung

↗ § 3 Abs. 2 Nr. 1 SächsBeWoG, Art. 6 DSGVO, Art. 13 GG

Das Hausrecht und die daraus resultierende Befugnis zur Erteilung eines Hausverbots leitet sich aus dem Grundrecht der „Unverletzlichkeit der Wohnung" nach Art. 13 Grundgesetz (GG) ab. Es gibt dem/der Eigentümer/in als Hausherrn/Hausherrin das Recht, zu bestimmen, wer sich innerhalb seines/ihres Hauses, seiner/ihrer Wohnung oder seinen/ihren Geschäftsräumen aufhalten darf und wer nicht. Aber auch einer Mieterin bzw. einem Mieter oder einer Pächterin bzw. einem Pächter steht das Hausrecht zu. Das Hausrecht und ein damit gegebenenfalls verbundenes Hausverbot können über das Besitzrecht verfügende Personen grundsätzlich beliebig ausüben. Das heißt, dass ein Hausverbot grundsätzlich an kein bestimmtes (Fehl-)Verhalten gebunden ist. Auch ist eine bestimmte Form für die Erteilung des Hausverbots nicht vorgeschrieben.
In stationären Pflegeeinrichtungen gemäß § 2 Abs. 1 Satz 1 Sächsisches Betreuungs- und Wohnqualitätsgesetz (SächsBeWoG) wird das Hausrecht oft als ein Ausdruck des Kontrollrechts der Einrichtung verstanden. Mit Blick auf Art. 13 GG hat aber auch jede/r der Bewohner/innen ein Hausrecht

an seinem/ihrem Zimmer oder seinem/ihrem Wohnbereich. Der Einrichtungsträger besitzt insofern die Verfügungsmacht nur über „ihre" oder „seine Räume", wozu regelmäßig auch der Eingangsbereich als Zugang zu der Einrichtung zählt.
Nach § 3 Abs. 2 Nr. 1 SächsBeWoG haben der Träger und die Leitung einer stationären Einrichtung unter anderem sicherzustellen, dass die Würde sowie die Interessen und Bedürfnisse der Bewohner/innen vor Beeinträchtigungen geschützt werden. Die Kommunikation mit Außenstehenden ist dabei eine der wesentlichen Bedingungen für ein würdiges Leben. Zugangsbehinderungen sind in diesem Fall daher nur bei Vorliegen ganz besonderer Umstände gerechtfertigt.
Ich habe im vergangenen Jahr von den Ermittlungsbehörden ein Ermittlungsverfahren zur Verfolgung einer Ordnungswidrigkeit im Rahmen meiner Zuständigkeit vorgelegt bekommen, welches diese gegen die Leiterin einer Pflegeeinrichtung eingeleitet hatten. Nach dem zur Anzeige gebrachten Sachverhalt hatte die Leiterin der Pflegeeinrichtung gegen einen Besucher ihrer Einrichtung ein Hausverbot ausgesprochen. Zur Information ihrer Beschäftigten und der weiteren Besucher/innen hat sie das erteilte Hausverbot unter Nennung des Namens des Besuchers sowie dessen postalischer Anschrift an mehreren Stellen in der Einrichtung mittels eines Aushangs öffentlich bekannt gemacht.
Dass es sich bei dem Aushang um die Verarbeitung von personenbezogenen Daten handelt, ist offensichtlich. Unabhängig von der Frage, ob diese von einem Erlaubnistatbestand des Art. 6 Datenschutz-Grundverordnung (DSGVO) gedeckt war, habe ich das Verfahren eingestellt, da im Bußgeldrecht nach der DSGVO die wirtschaftliche Einheit eines Unternehmens als Adressat angesehen wird. Nur im Ausnahmefall ist das Verfahren gegen Beschäftigte eines Unternehmens zu führen, nämlich dann, wenn dieser als eigener Verantwortlicher anzusehen wäre, vgl. Tätigkeitsbericht 2021, 6.4.3., Seite 184 ff. Hierfür haben die durchgeführten Ermittlungen keine hinreichenden Anhaltspunkte gegeben.
Auch wenn es nicht in meiner Zuständigkeit liegt, die rechtliche Zulässigkeit eines erteilten Hausverbotes zu prüfen, habe

Tätigkeitsbericht 2021:
↗ sdb.de/tb2021

ich den angezeigten Sachverhalt zum Anlass genommen, um im Rahmen eines Aufsichtsverfahrens nach Art. 58 Abs. 1 DSGVO die Rechtmäßigkeit der vorgenommenen Datenverarbeitung zu überprüfen und zu bewerten. Im Ergebnis meiner Prüfung habe ich keine Tatsachen feststellen können, die die Art und Weise der hier gewählten Bekanntmachungsform hätten rechtfertigen können. Ich habe den (kooperierenden und einsichtigen) Einrichtungsträger darauf hingewiesen, dass es zur Durchsetzung des Hausverbots ausreichend und angemessen gewesen wäre, allein die Beschäftigten in seiner Einrichtung mündlich oder gegebenenfalls schriftlich über ein erteiltes Hausverbot mit der Maßgabe zu informieren, dass bei der Feststellung eines Verstoßes die Heimleitung zu informieren ist; der Aushang war in der Zwischenzeit bereits abgenommen.

Was ist zu tun?
Der Träger einer stationären Pflegeeinrichtung sollte bei der Kommunikation eines erteilten Hausverbotes in seiner Einrichtung darauf achten, dass diese angemessen sein muss.

4.2 Gemeinsam Verantwortliche

4.2.1 Zweitmeinungsservice – ein Fall der gemeinsamen Verantwortlichkeit?

↗ § 140a SGB V, § 630f BGB, Art. 26 DSGVO, MBO-Ä

Der Datenschutzbeauftragte eines Universitätsklinikums im Freistaat Sachsen bat mich um Stellungnahme, ob beim Zweitmeinungsservice zwischen Klinikum und Krankenkasse ein Fall der gemeinsamen Verantwortlichkeit gemäß Art. 26 Datenschutz-Grundverordnung (DSGVO) vorliegt.

Eine Krankenkasse beabsichtigt mit Kliniken einen Vertrag über die Erbringung der medizinischen Leistung für ein „qualifiziertes Zweitmeinungsverfahren" im Sinn des § 140a Fünftes Buch Sozialgesetzbuch (SGB V) zu schließen. In § 140a SGB V sind Form, Art und Inhalt der Leistungserbringung sowie die damit einhergehenden Verfahren geregelt (zum Beispiel durch Normverweise). Zudem hat das Klinikum, insbesondere die Ärztinnen und Ärzte, einrichtungs- und berufsbedingte Verpflichtungen zur Datenverarbeitung (zum Beispiel Dokumentationspflichten nach § 630f Bürgerliches

Gesetzbuch, (Muster-)Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte usw.).
Patientinnen und Patienten (Krankenkassenmitglieder) besuchen bei Inanspruchnahme der vertraglich beabsichtigten Leistungen das Krankenhaus mit den zur Verfügung gestellten Unterlagen. Die Unterlagen beinhalten unter anderem eine Einverständniserklärung sowie eine Schweigepflichtentbindung.
Art. 26 Abs. 1 DSGVO lautet:

> „(1)Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung fest, so sind sie gemeinsam Verantwortliche. Sie legen in einer Vereinbarung in transparenter Form fest, wer von ihnen welche Verpflichtung gemäß dieser Verordnung erfüllt, insbesondere was die Wahrnehmung der Rechte der betroffenen Person angeht, und wer welchen Informationspflichten gemäß den Artikeln 13 und 14 nachkommt, sofern und soweit die jeweiligen Aufgaben der Verantwortlichen nicht durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen die Verantwortlichen unterliegen, festgelegt sind. In der Vereinbarung kann eine Anlaufstelle für die betroffenen Personen angegeben werden."

Nicht jede Verarbeitung, an der mehrere Stellen beteiligt sind, führt zu gemeinsamer Verantwortlichkeit. Es ist die gemeinsame Beteiligung von zwei oder mehr Stellen an der Festlegung der Zwecke und Mittel einer Vereinbarung erforderlich. Beim Zweitmeinungsservice regelt § 140a SGB V dessen Zweck und die Mittel. Einfluss auf Zweck und Mittel haben die Krankenkasse und das Klinikum nicht.
Ich teile die Rechtsauffassung des Datenschutzbeauftragten des Universitätsklinikums, dass in diesem Rechtsverhältnis zwischen Krankenkasse und Klinikum keine gemeinsame Veranwortlichkeit im Sinne des Art. 26 DSGVO besteht.

Was ist zu tun?
Beim Zweitmeinungsservice nach § 140a SGB V liegt keine gemeinsame Verantwortung im Sinne des Art. 26 DSGVO zwischen Krankenkasse und Klinikum vor.

4.3 Auftragsverarbeitung

4.3.1 Auftragsverarbeitungsvertrag, Auftragsverarbeitung und Verpflichtungsgesetz

↗ Verpflichtungsgesetz

Tätigkeitsbericht Datenschutz 2022:
↗ sdb.de/tb2022

In meinem Tätigkeitsbericht 2022 (4.2.2, Seite 140 f.) wird der Fall geschildert, dass ein Landratsamt einem Auftragsverarbeiter Zugriff auf personenbezogene Daten bzw. Gesundheitsdaten gewährt.

Dabei wird ausgeführt: „Beim Abschluss eines Auftragsverarbeitungsvertrags durch eine Behörde, beispielsweise durch ein Landratsamt, ist darauf zu achten, ob für die Wahrnehmung der Aufgabe seitens des Auftragsverarbeiters eine Verpflichtung vorzunehmen ist. […] Die Verpflichtung ist von der verpflichtungsberechtigten öffentlichen Stelle durchzuführen."

Dazu erreichte mich eine Nachfrage durch den Datenschutzbeauftragten eines Landratsamtes. Dieses verpflichtet den Auftragsverarbeiter mit einer „Vereinbarung zur Auftragsverarbeitung", sodass dieser die zur Verarbeitung der Daten befugten Personen zur Vertraulichkeit verpflichtet. Er bat um Stellungnahme, ob dies zulässig ist.

Arbeitspapier „Die förmliche Verpflichtung als Instrument des Datenschutzes":
↗ sdb.de/tb2208

Dem Arbeitspapier des Bayerischen Beauftragten für den Datenschutz ist zu entnehmen, dass das Landratsamt die Verpflichtung vorzunehmen hat, vgl. Rdnr. 11, 15.

Es war zu prüfen, ob diese Rechtslage auch auf den Freistaat Sachsen zutrifft.

Nach § 1 Abs. 1 Nr. 1 Gesetz über die förmliche Verpflichtung nichtbeamteter Personen (Verpflichtungsgesetz) vom 2. März 1974 soll auf die gewissenhafte Erfüllung seiner Obliegenheiten verpflichtet werden, wer, ohne Amtsträger/in (§ 11 Abs. 1 Nr. 2 des Strafgesetzbuches) zu sein, bei einer Behörde oder sonstigen Stelle, die Aufgaben der öffentlichen Verwaltung wahrnimmt, beschäftigt oder für sie tätig ist.

Welche Stelle für die Verpflichtung zuständig ist, bestimmt nach § 1 Abs. 4 Nr. 2 Verpflichtungsgesetz in allen übrigen Fällen diejenige Behörde, die von der Landesregierung durch Rechtsverordnung bestimmt wird.

Die Verordnung der Sächsischen Staatsregierung über Zuständigkeiten nach dem Gesetz über die förmliche Verpflichtung nichtbeamteter Personen vom 20. Oktober 1993 regelt dies für Sachsen. Nach § 1 Nr. 2 Buchst. b der Verordnung ist dies im Geschäftsbereich der kommunalen Träger der Selbstverwaltung die oberste Rechtsaufsichtsbehörde.
In der Verwaltungsvorschrift des Sächsischen Staatsministeriums des Innern über die Bestimmung der nach dem Gesetz über die förmliche Verpflichtung nichtbeamteter Personen zuständigen Behörde vom 17. Januar 1994 wird für den Geschäftsbereich des SMI bestimmt:
Für die Verpflichtung nach § 1 des Verpflichtungsgesetzes ist zuständig: 1. im Falle des § 1 Nr. 1 des Verpflichtungsgesetzes die für die Einstellung oder Bestellung zuständige Behörde oder Stelle. Diese kann sich bei der Durchführung der Verpflichtung der Behörde oder Stelle bedienen, bei der die zu verpflichtende Person beschäftigt oder für die sie tätig ist.
Danach kann sich das Landratsamt bei der Durchführung der Stelle bedienen, bei der die zu verpflichtende Person beschäftigt ist. Das Landratsamt kann deshalb weiterhin den Auftragsverarbeiter verpflichten, dass dieser die zur Verarbeitung der Daten befugte Person zur Vertraulichkeit gemäß Verpflichtungsgesetz verpflichtet.

Was ist zu beachten?
Das Landratsamt kann den Auftragsverarbeiter verpflichten, dass dieser die zur Verarbeitung der Daten befugte Person zur Vertraulichkeit gemäß Verpflichtungsgesetz verpflichtet.

4.4 Meldung von Datenschutzverletzungen

4.4.1 Allgemeine Hinweise zur Meldepflicht von Datenpannen

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

Im Zusammenhang mit der Meldepflicht von Datenschutzverletzungen gemäß Art. 33 Datenschutz-Grundverordnung (DSGVO) weise ich darauf hin, dass sämtliche Datenschutzverletzungen mir gegenüber zu melden sind. Dies ist lediglich dann nicht notwendig, wenn die Datenschutzverletzung vo-

raussichtlich 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 Back-ups, 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 und 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 dargelegten Vorkehrungen zu prüfen und stets auf aktuellem Stand zu halten.

Onlineformular der SDTB zur Meldung einer Datenpanne:
↗ sdb.de/art33

4.4.2 Meldepflicht nach § 83a SGB X für Sozialbehörden

↗ § 83 a SGB X

Aus dem Kreis der AG Datenschutz der sächsischen Landkreise wurde eine Anfrage zur Umsetzung des § 83a Zehntes Buch Sozialgesetzbuch (SGB X) an mich herangetragen. Konkret wurde die Frage gestellt, an welche Stelle etwaige Verletzungen des Schutzes von Sozialdaten konkret zu melden sind.
Nach dieser Norm ist von den jeweils zuständigen Sozialbehörden eine Verletzung des Schutzes von Sozialdaten

neben den Meldepflichten gemäß den Artikeln 33 und 34 der Datenschutz-Grundverordnung auch der Rechts- oder Fachaufsichtsbehörde zu melden.

Aus Sicht des von mir einbezogenen Sächsischen Staatsministeriums für Soziales und Gesellschaftlichen Zusammenhalt (SMS) ergibt sich für Sozialbehörden eine differenzierte Bewertung. § 83a SGB X verweist auf die in § 35 SGB I genannten Leistungsträger nach § 12 in Verbindung mit den §§ 18–29 SGB I. Dazu zählen für den Bereich des SMS die zugelassenen kommunalen Träger der Grundsicherung für Arbeitsuchende (§ 19a SGB I) und örtliche und überörtliche Träger der Sozialhilfe (§ 28 SGB I). Für die zugelassenen kommunalen Träger der Grundsicherung für Arbeitsuchende hat das SMS die Fach- und Rechtsaufsicht (§ 48 Abs. 1 SGB II in Verbindung mit § 15 Abs. 1 Nr. 1a. Abs. 2 und Abs. 3 SächsAGSGB).

Darüber hinaus hat das SMS die Fachaufsicht über die örtlichen und überörtlichen Träger der Sozialhilfe bzgl. Leistungen nach dem 4. Kapitel des SGB XII (§ 14a Abs. 2 Sächsisches Gesetz zur Ausführung des Sozialgesetzbuches [SächsAGSGB]).

In weiteren festgelegten Leistungsbereichen, insbesondere hinsichtlich Kosten der Unterkunft und Heizung sowie Bildung und Teilhabe, führt das SMS zudem die Fach- und Rechtsaufsicht über die Jobcenter (§ 15 Abs. 3 SächsAGSGB in Verbindung mit §§ 6 Abs. 1 Nr. 2, 47 Abs. 2 SGB II).

Nach Auffassung des SMS kommt es für die Zuständigkeit nach § 83a SGB X darauf an, inwiefern die im Einzelfall vorliegende Verletzung des Sozialdatenschutzes den jeweiligen Verantwortungsbereich der Fach- und/oder Rechtsaufsicht der hierfür zuständigen Behörde tangiert. So ist beispielsweise nicht anzunehmen, dass jedwede Verletzung von Sozialdaten in einem Sozialamt dem SMS zu melden ist, sondern diese müsste im Zusammenhang mit einer Leistungsgewährungsversagung nach dem 4. Kapitel SGB XII stehen. Im Bereich der zugelassenen kommunalen Träger der Grundsicherung für Arbeitsuchende müsste der Verstoß im Zusammenhang mit einer Leistungsgewährungsversagung nach dem SGB II erfolgen.

Was ist zu tun?
Sozialbehörden haben im Fall einer Meldepflicht nach den Artikeln 33 und 34 der DSGVO auch § 83a SGB X zu erfüllen.

Wegen ihrer generellen Rechtsaufsicht gemäß 65 Abs. 1 Sächsische Landkreisordnung, § 112 Abs. 1 Satz 1 Sächsische Gemeindeordnung über die Landkreise und Kreisfreien Städte ist aus Sicht des SMS auch die Landesdirektion von § 83a SGB X tangiert. Dies entspricht auch meiner Rechtsauffassung.

4.4.3 Neuer Höchstwert bei Meldungen nach Artikel 33 DSGVO

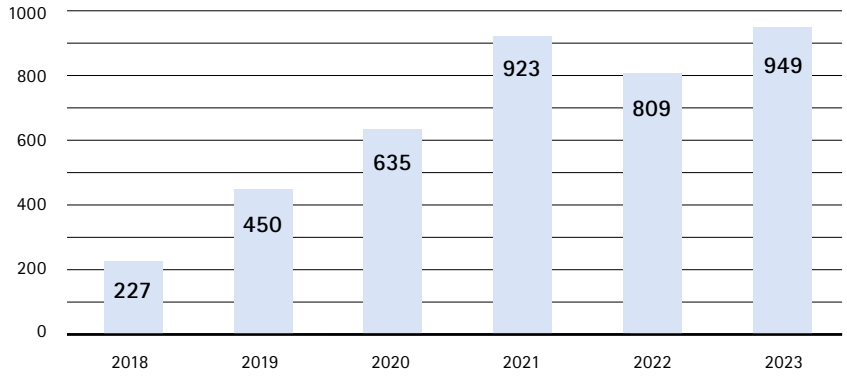
↗ Art. 33 DSGVO

Nach Art. 33 Datenschutz-Grundverordnung (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 2023 sind bei mir 949 solcher Meldungen eingegangen. Im Vergleich zum vorjährigen Berichtszeitraum 2022 mit 785 Meldungen entspricht dies einem Anstieg um ca. 20 Prozent und stellt zum Berichtszeitraum 2021 mit 923 Meldungen einen neuen Höchstwert der jährlichen Meldungen von Datenschutzverletzungen dar.

Die folgenden Fallgruppen sind im Berichtszeitraum besonders häufig gemeldet worden:

Abbildung 1:
Meldungen von Datenschutzverletzungen nach Art. 33 DSGVO



Fehlversendung

Die Fehlversendung von Unterlagen mit personenbezogenen Daten ist eine der häufigsten Ursachen für Datenschutzverletzungen. Diese resultiert oft aus einer falschen Zuordnung von Dokumenten, fehlerhafter maschineller Kuvertierung, ungenauen Adressdaten oder simplen Namensverwechslungen. Obgleich das Risiko für die betroffenen Personen in der Regel als nicht hoch eingestuft wird, da in diesem Fall die Datenschutzverletzung dem Verantwortlichen durch den/die Empfänger/in der Fehlsendung gemeldet wird, erfordert dies dennoch umgehende datenschutzrechtliche Maßnahmen. Dazu gehören unter anderem die Löschung der übermittelten Daten, die Rücksendung der Dokumente, die Behebung der Fehlerursache sowie die erneute, korrekte Versendung – alles Maßnahmen, die der Verantwortliche in die Wege leiten kann.

Offener E-Mail-Verteiler

Ebenso gehört der sogenannte offene E-Mail-Verteiler zu den häufigen Ursachen für Datenschutzverletzungen, die mir regelmäßig gemeldet werden. In diesem Kontext werden E-Mail-Adressen versehentlich nicht im Blindkopie-Feld (Bcc), sondern üblicherweise im Kopie-Feld (Cc) eingetragen. Dies stellt eine typische Fallgruppe dar, die als meldepflichtig einzustufen ist, wenn der/die E-Mail-Inhaber/in nicht ausdrücklich der öffentlichen Verbreitung der E-Mail-Adresse zugestimmt hat. In solchen Fällen fehlt es an einer rechtlichen Grundlage für die Verarbeitung personenbezogener Daten. Die Verwendung eines offenen E-Mail-Verteilers resultiert in der Regel aus einem Versehen der Absenderin bzw. des Absenders. Daher ist es besonders wichtig, in dieser Fallgruppe wiederholte Sensibilisierungsmaßnahmen zu implementieren. Dies dient nicht nur der Prävention solcher Fehler, sondern auch der allgemeinen Sensibilisierung für den verantwortungsbewussten Umgang mit personenbezogenen Daten in der E-Mail-Kommunikation.

Verlust auf dem Postweg

Neben der Fehlversendung stellen auch Vorfälle des Verlusts von Unterlagen mit personenbezogenen Daten auf dem Postweg regelmäßige Meldefälle dar. Der wesentliche Unterschied zur Fehlversendung liegt in der Tatsache, dass beim Verlust der Unterlagen der Verbleib unklar bleibt. Dieser Umstand führt dazu, dass das Risiko für die betroffenen Personen in der Regel höher eingestuft wird als im Vergleich zur Fehlversendung. Bei Letzterer kann durch die Meldung der Empfängerin bzw. des Empfängers der Fehlsendung eine abschließende Bewertung des Risikos vorgenommen werden, da dieser Umstand eine unmittelbare Reaktion und Klärung seitens des Verantwortlichen ermöglicht. Die Unsicherheit über den Verbleib der verlorenen Unterlagen auf dem Postweg schafft eine zusätzliche Herausforderung, da eine potenzielle unrechtmäßige Nutzung oder unbefugter Zugriff nicht ausgeschlossen werden kann. Diese Ungewissheit erfordert verstärkte Aufmerksamkeit und proaktive Maßnahmen seitens des Verantwortlichen, um das Risiko für die betroffenen Personen zu minimieren. Daher ist eine sorgfältige Überwachung und ein effizientes Reaktionsmanagement im Falle von Unterlagenverlusten auf dem Postweg von entscheidender Bedeutung.

Einbruch und Diebstahl

Datenschutzverletzungen im Zusammenhang mit Diebstählen und Einbrüchen stellen auch im aktuellen Berichtszeitraum eine gängige Fallgruppe dar, die mir gemeldet wurde. Auffällig ist dabei, dass die kriminellen Aktivitäten nicht zwangsläufig darauf abzielen, die personenbezogenen Daten direkt zu erlangen. Vielmehr konzentrieren sie sich auf die Gegenstände, auf denen die personenbezogenen Daten gespeichert sind, wie beispielsweise Digitalkameras, Laptops usw. Es ist jedoch wichtig zu betonen, dass dies nicht dazu führt, das verbundene Risiko solcher Beschaffungskriminalität für die Betroffenen als gering einzustufen. In der Regel kann nämlich nicht ausgeschlossen werden, dass im Nachhinein die kriminellen Täter/innen auch auf die personen-

bezogenen Daten zugreifen, um hieraus einen finanziellen Vorteil zu erlangen. Gerade in dieser Fallgruppe ist es daher ratsam, den Anreiz für Diebstähle so gering wie möglich zu halten. Dies kann durch die sachgemäße Aufbewahrung technischer Geräte – ohne diese unbeaufsichtigt zu lassen – sowie durch die Verschlüsselung der auf den Geräten gespeicherten personenbezogenen Daten, regelmäßige Backups und die Einrichtung eines sicheren Passwortschutzes erreicht werden.

Cyberkriminalität

Wie schon in den vorangegangenen Berichtszeiträumen deutlich wurde, stellen Meldungen im Zusammenhang mit Cyberkriminalität weiterhin eine bedeutende Kategorie von Datenschutzverletzungen dar. Diese umfassen grundsätzlich sämtliche Handlungen oder Straftaten, die mithilfe von Kommunikations- und Informationstechnologien begangen werden. Ein herausforderndes Element besteht darin, dass solche Aktivitäten nahezu von jedem Ort der Welt aus durchgeführt werden können und ihre Spuren oft effektiv verschleiert werden können. Typische Beispiele im Bereich der Cyberkriminalität sind Spam- und Phishing-Mails, die Verschlüsselung von Systemen mittels Ransomware oder generell die Verwendung von Schadsoftware (Malware) sowie das Ausnutzen von Schwachstellen. Diese Formen von Angriffen stellen besondere Herausforderungen dar, da sie nicht nur vielfältig und raffiniert sind, sondern auch eine globale Reichweite haben und die Identifizierung der Täter/innen erschweren. Daher ist es von entscheidender Bedeutung, proaktiv die Sicherheitsmaßnahmen zu stärken und eine kontinuierliche Überwachung auf mögliche Bedrohungen zu gewährleisten. Dies ermöglicht eine schnelle Reaktion durch wirksame Gegenmaßnahmen, um die Auswirkungen solcher Cyberangriffe zu minimieren.

Was ist zu tun?
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 4.4.5.

4.4.4 Ausgewählte Meldungen von Datenschutzverletzungen

↗ Art. 9 DSGVO

Neben den typischen Fallgruppen der gemeldeten Datenschutzverletzungen (siehe 4.4.3) sind folgende zwei Meldungen erwähnenswert:

Fehlversendete Entgeltdokumente aufgrund fehlerhafter Kuvertierung

Eine typische Datenschutzverletzung, die der Fallgruppe der Fehlversendung zugeordnet werden kann, betraf personenbezogene Daten im Zusammenhang mit Entgeltabrechnungen. Der Verantwortliche teilte mir mit, dass bei den versandten Entgeltabrechnungen versehentlich auch Entgeltabrechnung von anderen Beschäftigten enthalten waren, sodass Dritte unberechtigt von personenbezogenen Daten Kenntnis erhielten und den Betroffenen selbst keine Entgeltabrechnungen zur Verfügung gestellt wurden. Der Verantwortliche teilte mir mit, dass die betroffenen Personen informiert wurden und die Datenschutzverletzung ausgewertet werde und anschließend entsprechende Maßnahmen getroffen werden. Auf meine Nachfrage hin, was die Fehleranalyse ergeben habe und welche Maßnahmen daraus hervorgegangen sind, teilte mir der Verantwortliche mit, dass es mit dem auftragsverarbeitenden Dienstleister mehrere Auswertungstermine gegeben habe. Im Rahmen der Fehleranalyse wurde festgestellt, dass aufgrund fehlender technischer Einstellungen die Merkmale zur Dokumententrennung nicht eindeutig markiert waren und diese deshalb bei der Sendungsbündelung falsch zugeordnet wurden. Weiterhin wurde für die Dauer der Fehleranalyse und der anschließenden Testphase die Sendungsbündelung zunächst ausgesetzt. Anschließend wurde mit dem auftragsverarbeitenden Dienstleister festgelegt, dass es eine nachfolgende Überwachung und Dokumentation der Vorgänge geben wird, um eine erneute Datenschutzverletzung zu verhindern.

Vertrauliche Gesundheitsdaten auf Retour- und Weiterverkaufswegen

Eine kuriose Datenschutzverletzung mit zugleich hohem Risikopotenzial meldete mir ein Verantwortlicher im Zusammenhang mit der Verarbeitung von personenbezogenen Daten im Homeoffice. Bei den zu verarbeitenden Daten handelte es sich um hoch vertrauliche, unter anderem aus dem Gesundheitsbereich, sodass diese als besondere Kategorien personenbezogener Daten gemäß Art. 9 Datenschutz-Grundverordnung einzustufen waren. Zwar war die Verarbeitung dieser Daten im Homeoffice grundsätzlich genehmigt und die Mitnahme der Unterlagen autorisiert, problematisch war allerdings, dass entgegen der technisch-organisatorischen Regelungen des Verantwortlichen die Unterlagen nicht in einem geschlossenen Transportmedium ins Homeoffice mitgenommen wurden, sondern lediglich in einem Rucksack. Bei der gemeldeten Datenschutzverletzung realisierte sich jedoch nicht das Risiko, welches auf dem Transportweg gegeben war, sondern die Verwahrung der Unterlagen im Homeoffice. Die Unterlagen verblieben im Rucksack, welcher – und dies macht die Datenschutzverletzung so kurios – an den ursprünglichen Verkäufer des Rucksacks retourgesandt wurde, einschließlich der vertraulichen Unterlagen. Beim erneuten Verkauf des Rucksacks gelangten die Unterlagen in die Hände einer dritten Person, welche die Unterlagen nunmehr entdeckte. Glücklicherweise und damit risikomindernd meldete sich die dritte Person, sodass die vertraulichen Unterlagen schlussendlich durch den Verantwortlichen wieder zurückgeholt werden konnten. Der Verantwortliche hat neben mir als Aufsichtsbehörde sämtliche betroffene Personen über die Datenschutzverletzung informiert. Zugleich wurde nochmals der gesamte Prozess der datenschutzkonformen Verwendung von personenbezogenen Daten im Homeoffice überprüft. Des Weiteren wurde die Datenschutzverletzung zum Anlass genommen, alle Beteiligten hinsichtlich der technisch-organisatorischen Anforderungen bei der Verarbeitung von personenbezogenen Daten im Homeoffice zu sensibilisieren.

4.4.5 Vorbeugende Maßnahmen

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

- Daten sichern! Die Daten von Firmen und Organisationen müssen unbedingt gesichert sein. Diese Back-ups 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 Mitarbeiter/innen, Unternehmensleitung und Kunden/Kundinnen zu informieren sind.
- Reservetechnik vorhalten! Eine dringende Empfehlung ist zudem, Reservetechnik vorzuhalten. Ermittler/innen 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 personenbezogenen Daten betroffen sind.
- Weiterbildung! IT-Verantwortliche und all jene, die in Unternehmen und Organisationen für die IT-Sicherheit zuständig sind, benötigen regelmäßig Weiterbildung.

4.5 Datenschutzbeauftragte/r

4.5.1 Datenschutzbeauftragte/r als Vertragsgestalter/in

↗ Art. 37, 39 Abs. 1 Buchst. a DSGVO

Immer wieder erreichen mich Anfragen zum Aufgabenumfang von gemäß Art. 37 Datenschutz-Grundverordnung (DSGVO) benannten Datenschutzbeauftragten, inwieweit diese im Zuge von Vertragsentwicklungen sowie -verhandlungen rechtliche Regelungen selbst bzw. mit zu gestalten haben.

Ich weise die Anfragenden darauf hin, dass gemäß Art. 39 Abs. 1 Buchst. a DSGVO Datenschutzbeauftragte (DSB) die Aufgabe der Beratung des Verantwortlichen haben. In diesem Zusammenhang führt Erwägungsgrund 77 aus, dass der Datenschutzbeauftragte gegenüber dem Verantwortlichen hinsichtlich der Durchführung geeigneter Maßnahmen und Einhaltung der Anforderungen der DSGVO Hinweise geben könne. Ich kann dem keine Pflicht zur Mitgestaltung von rechtlichen Regelungen im Zuge von Vertragsentwicklungen sowie -verhandlungen entnehmen. Zweckmäßig dürfte es jedoch sein, eventuell bestehende Datenschutzbedenken gegen entsprechende Entwürfe vorzutragen.

In diesem Zusammenhang weise ich zudem auf die Ausführungen im Kurzpapier Nr. 12 „Datenschutzbeauftragte bei Verantwortlichen und Auftragsverarbeitern" der DSK hin: „Die DSGVO stellt in Art. 24 Abs. 1 DSGVO ausdrücklich klar, dass es die Pflicht des Verantwortlichen bzw. des Auftragsverarbeiters – und nicht die des DSB – bleibt, sicherzustellen und nachzuweisen, dass die Datenverarbeitungen im Einklang mit den Regelungen der DSGVO stehen."

Kurzpapier der Datenschutzkonferenz „Datenschutzbeauftragte bei Verantwortlichen und Auftragsverarbeitern":
↗ sdb.de/tb2306

Was ist zu tun?
Es ist sicherzustellen, dass benannte Datenschutzbeauftragte keine zusätzlichen Aufgaben in dieser Funktion bekommen.

5 Internationaler Datenverkehr

5.1 Datenschutzkonferenz veröffentlicht Anwendungshinweise zum EU-US Data-Privacy-Framework

↗ DSGVO

Am 4. September 2023 hat die Datenschutzkonferenz (DSK) Anwendungshinweise zum Angemessenheitsbeschluss der Europäischen Kommission zum Datenschutzrahmen EU-USA (EU-US Data Privacy Framework) vom 10. Juli 2023 veröffentlicht, abrufbar unter sdb.de/tb2304.
Die Aufsichtsbehörde wurde im Rahmen der Beratung von Verantwortlichen immer wieder gefragt, was sich konkret ändert und worauf zu achten ist. Neben den in den Anwendungshinweisen genannten Prüfschritten und Pflichten des Verantwortlichen sind es in der Praxis vor allem die folgenden Punkte, die Gründe für Nachfragen seitens der Aufsicht bieten:

Rechtsgrundlage und Auftragsverarbeitung

Für eine Übermittlung muss eine ausreichende Rechtsgrundlage vorhanden sein. Problematisch beim Transfer in andere Wirtschaftsräume ist oftmals ein grundlegend anderes Verständnis von personenbezogenen Daten und eine Nutzung von Daten für eigene Geschäftszwecke des Transferpartners. Solche weiteren Verarbeitungen müssen von der Rechtsgrundlage für eine Übermittlung mit abgedeckt werden. Werden Daten für solche Zwecke mit unklarer Bestimmung

oder Verwendungsdauer verarbeitet, scheidet Art. 6 Abs. 1 Buchst. f Datenschutz-Grundverordnung (DSGVO, berechtigtes Interesse) in aller Regel als Rechtsgrundlage aus, weil eine Abwägung des Risikos für Betroffene schlicht unmöglich ist. Öffentliche Stellen haben hingegen gar keine Rechtsgrundlage für einen Export von Daten, wenn diese für ein „berechtigtes Interesse" des Transferpartners genutzt werden sollen. Es muss jedem Verantwortlichen klar sein, dass dieser den Prüfpflichten der DSGVO weiterhin unterliegt und die Existenz eines Transferabkommens nicht das Ende der Prüfung bedeutet. Beispielhaft sei auf den Prüfbericht der DSK zu den „Microsoft-Onlinediensten" verwiesen, der rechtliche Fallstricke verdeutlicht.

Prüfbericht der DSK zu „Microsoft-Onlinediensten – Bewertung der aktuellen Vereinbarung zur Auftragsverarbeitung":
↗ sdb.de/tb2305

Übermittlung in weitere Drittstaaten

Auch wenn der Angemessenheitsbeschluss für die USA gilt, verwenden internationale Unternehmen oftmals internationale Cloud-Strukturen mit Niederlassungen/Rechenzentren in einer Vielzahl von Ländern. Wenn in diesen Ländern personenbezogene Daten verarbeitet werden und kein Angemessenheitsbeschluss vorliegt, ist eine Datenübermittlung nur nach den Maßgaben des Art. 46 DSGVO möglich. Dies gilt zum Beispiel bei der Nutzung von Google-Diensten (siehe 4.1.1).

Übersicht zu Angemessenheitsbeschlüssen der EU:
↗ sdb.de/tb2309

Was ist zu tun?
Verantwortliche müssen auch bei einem Angemessenheitsbeschluss Rechtsgrundlagen und Verträge genau prüfen und gegenüber der Aufsichtsbehörde darlegen können.

5.2 Cloud-Computing in der Schule

Mich erreichten zahlreiche Anfragen zur Zulässigkeit der Nutzung von Software in Schulen, die die Speicherung in einer Cloud erfordern. In meinem Tätigkeitsbericht 2021 (1.3, Seite 44) hatte ich dazu auf Ziff. III Nr. 12 Buchst. a der Verwaltungsvorschrift (VwV) Schuldatenschutz hingewiesen: „Es sind nur solche Cloud-Computing-Dienste zulässig, auf die das Recht der EU Anwendung findet." Daraus hatte ich gefolgert, dass Datentransfers in das Nicht-EU-Ausland zu unterbleiben haben.

Tätigkeitsbericht 2021:
↗ sdb.de/tb2021

Ich habe das EU-US Data Privacy Framework (siehe 5.1) zum Anlass genommen, in dieser Frage erneut auf das Sächsische Staatsministerium für Kultus (SMK) zuzugehen, da die bisherige Interpretation auch beispielsweise dazu geführt hätte, dass Cloud-Anbieter aus der Schweiz nicht genutzt werden dürfen.

Im Ergebnis legt das SMK ebenso wie ich künftig Ziff. III Nr. 12 Buchst. a VwV Schuldatenschutz so aus, dass Cloud-Dienste außerhalb der EU auch (und nur) in Ländern zulässig sein sollen, für die nach Art. 45 DSGVO ein Angemessenheitsbeschluss vorliegt, da dann die DSGVO wegen eines „angemessenen Schutzniveaus" faktisch Anwendung findet. Eine Prüfung der entsprechenden Drittstaaten können Verantwortliche auf der Website der EU-Kommission (Kurzlink: sdb.de/tb2306) bzw. für die USA auf dataprivacyframework.gov vornehmen.

Dies bedeutet jedoch nicht, dass eine entsprechende Verarbeitung in der Cloud damit in jedem Fall datenschutzrechtlich zulässig ist. Wie in meinem oben erwähnten Beitrag aus dem Tätigkeitsbericht 2021 dargestellt, ist Tracking (und sei es zur Produktverbesserung) oder Werbung, welche das Verhalten von Nutzerinnen und Nutzern im Internet nachverfolgt, in aller Regel nicht mit dem Bildungsauftrag oder dem Beschäftigtendatenschutz vereinbar.

Im Übrigen weise ich auf das Risiko hin, dass bei einer (erneuten) Feststellung der Unwirksamkeit des Angemessenheitsbeschlusses für die USA durch den EuGH die Datenverarbeitung rechtswidrig und damit sanktionierbar wird.

Was ist zu tun?

Schulen sollten weiterhin von ihnen genutzte Software kritisch prüfen. Geprüft sind über Schullogin bzw. VIDIS (sdb.de/tb2307) angebundene digitale Bildungsangebote. Generell empfiehlt sich die Anwendung der dort verwendeten Prüfkriterien (sdb.de/tb2308).

6 Sächsische Datenschutzbeauftragte

6.1 Zuständigkeit und Anforderungen an Beschwerden

6.1.1 Der Anspruch betroffener Personen auf das Ergebnis der Beschwerdebearbeitung beim Vorliegen einer Kameraattrappe

↗ Art. 2 Abs. 2 Buchst. c DSGVO, Art. 77 Abs. 2 DGSVO

Bemerkt jemand auf dem Weg zur Arbeit oder beim abendlichen Spaziergang eine Videokamera in seiner Nachbarschaft und zeigt die Videokamera noch dazu in Richtung öffentlicher Straße, macht sich gleich ein Unbehagen breit. Da liegt die Vermutung nahe, dass der/die Kamerabetreiber/in die Kamera womöglich dazu nutzt, um zu beobachten, wer sich vor seinem/ihrem Grundstück bewegt und dort entlangläuft. In welcher Weise dies geschieht, also ob nur Livebilder gesichtet werden oder auch Videoaufzeichnungen gefertigt werden, lässt sich der Kamera zwar nicht ansehen, regt jedoch die Vorstellungskraft an. So erstaunt es nicht, dass in der Mehrzahl der Eingaben vom schlimmsten Fall ausgegangen wird, also sowohl ein Monitoring als auch die Speicherung von Videosequenzen unterstellt werden. Kein Wunder, bieten doch die heutigen Videokameras eine Fülle an technischen Merkmalen und Einstellmöglichkeiten. Da liegt es auf der Hand, dass diese auch im festgestellten Fall vollständig ausgeschöpft werden oder zumindest zum größten Teil zum Einsatz kommen.

Allerdings stelle ich in der täglichen Beschwerdebearbeitung immer wieder fest, dass nicht jede bei mir gemeldete Video-

kamera auch tatsächlich an eine Stromquelle angeschlossen oder ins heimische Funknetzwerk oder Internet eingebunden ist. Oder aber es stellt sich heraus, dass es sich nur um eine Kameraattrappe handelt. Damit die datenschutzrechtlichen Vorschriften zur Anwendung kommen, muss tatsächlich eine Verarbeitung personenbezogener Daten stattfinden (Art. 2 Abs. 1 Datenschutz-Grundverordnung [DSGVO]). Ist eine Videokamera stromlos oder ist eine „echte" Kameraattrappe (leeres Gehäuse) angebracht, habe ich folglich keine Kontrollzuständigkeit. Kommen die Datenschutzvorschriften nicht zur Anwendung, kann demzufolge auch kein Datenschutzverstoß vorliegen.

Doch warum finden sich überhaupt so viele Kameraattrappen oder stromlose Videokameras im Einsatz? Der Grund dafür liegt darin, dass die Betreiber/innen damit einen Abschreckungseffekt erzielen möchten, indem sie eine (vermeintliche) Videoüberwachung vortäuschen, um so bei betroffenen Personen einen Anpassungs- und Überwachungsdruck auszulösen. Dies birgt für den/die Grundstückseigentümer/in allerdings das Risiko einer zivilrechtlichen Auseinandersetzung, oder es kommt gar zu einem Prozess vor den Zivilgerichten. Denn nur auf privatrechtlichem Weg können sich Betroffene in diesen Fällen zur Wehr setzen.

Aus diesem Grund lege ich dem/der Kamerabetreiber/in regelmäßig eine Demontage von Kameraattrappen nahe, wenn sich herausstellt, dass die festgestellten Kameras nicht dem Datenschutzrecht unterfallen. Sollte dies für den/die Betreiber/in nicht in Betracht kommen, rate ich dazu, die Kameraattrappen zumindest so auszurichten, dass für Außenstehende erst gar nicht der Eindruck entsteht, als würden öffentliche Bereiche mitüberwacht. Zeigen Kameraattrappen auf nachbarliche Grundstücke, dann verfahre ich in gleicher Weise.

Ungeachtet dessen schließt sich bei der Beschwerdebearbeitung die Frage an, ob und in welchem Umfang ich den/die Beschwerdeführer/in mit der abschließenden Mitteilung hierüber informieren darf. Die Datenschutzvorschriften legen mir auf, jedem/jeder Beschwerdeführer/in eine abschließende Infor-

mation mit dem Ergebnis meiner Prüfung zu geben (siehe Art. 77 Abs. 2 DSGVO). Die Grundstückseigentümer/innen bevorzugen es selbstverständlich, den Umstand geheim zu halten, dass die angebrachten Videokameras nicht beobachten oder aufzeichnen, ansonsten wären diese wirkungslos. Dies stellt meine Behörde vor ein Dilemma. Auf der einen Seite sehe ich das berechtigte Interesse der Kamerabetreiberin/des Kamerabetreibers daran, ihr/sein Grundstück mit einer Attrappe oder nicht aktivierten Videokamera zu schützen. Auf der anderen Seite verpflichten mich – wie dargestellt – die Datenschutzvorschriften dazu, den/die Beschwerdeführer/in glaubhaft und nachvollziehbar über das Ergebnis meiner Prüfung zu unterrichten.

Welche Informationen ich dem/der Beschwerdeführer/in nach Abschluss des Aufsichtsverfahrens gebe, hängt damit maßgeblich vom zu entscheidenden Einzelfall ab, insbesondere von den örtlichen Verhältnissen. Dabei haben sich zwei denkbare Konstellationen herauskristallisiert.

Im ersten Fall ist die Kameraattrappe oder die zu Abschreckungszwecken angebrachte abgeschaltete bzw. stromlose Videokamera so nah oder unmittelbar an der Grenze zum öffentlichen Verkehrsraum oder auch nachbarlichen Grundstücken installiert, dass selbst bei einem hypothetischen Kamerabetrieb keine legale Videoüberwachung denkbar wäre. In dieser Konstellation komme ich nicht umhin, dem/der Beschwerdeführer/in gegenüber offenzulegen, dass keine Videoüberwachung stattfindet, es sich also nicht um eine aktiv betriebene Videokamera handelt. Wäre jedoch im zweiten Fall aufgrund des Anbringungsorts sowie der örtlichen Umstände ein gesetzeskonformer Betrieb grundsätzlich vorstellbar, schließe ich den Aufsichtsvorgang mit der Feststellung, dass keine unzulässige Videoüberwachung – über die Grenze des privaten Grundstücks hinaus – festgestellt werden konnte.

Bevor ich betroffene Personen aber über Kameraattrappen oder in der Funktion einer Attrappe eingesetzte stromlose Videokameras informiere, gebe ich dem betreibenden Verantwortlichen im Regelfall die Möglichkeit, mir Einwände zu

Was ist zu beachten?
Selbstbetroffene Beschwerdeführer/innen haben auch dann Anspruch darauf, das Ergebnis meiner Prüftätigkeit zu erfahren, wenn Kameraattrappen oder nicht aktive Videokameras eingesetzt werden. Der/Die Betreiber/in hat es in der Hand, stichhaltige Argumente zu liefern, die gegen eine Offenlegung sprechen. Hierzu kann auch eine andere Kameraausrichtung oder ein geänderter Anbringungsort beitragen.

nennen, die dem entgegenstehen. Daneben liegt es aber auch in der Hand des Verantwortlichen, durch eine geänderte Anbringung oder Ausrichtung dem Eindruck entgegenzuwirken, als würde die vermeintliche Videokamera unrechtmäßig betrieben. Ergibt sich schließlich, dass ich nachvollziehbar begründen kann, weshalb keine Datenschutzvorschriften verletzt sind, lege ich die Kameraattrappe respektive die Funktion einer deaktivierten Videokamera nicht offen.

6.1.2 Umgang mit unsinnigen Petitionen – geltend gemachter Auskunftsanspruch gegen ein „Königreich Deutschland"

↗ Art. 15 Abs. 1 und 3 DSGVO

Zuweilen erreichen meine Behörde auch befremdliche Anfragen bzw. Eingaben.
Ein Beschwerdeführer forderte tatsächlich gemäß Art. 15 Datenschutz-Grundverordnung Auskunft vom „Königreich Deutschland"; in concreto schrieb er dieses „Königreich" nach seinen eigenen Angaben unter einer konkreten Anschrift an und forderte unter anderem „... im Rahmen des Beweissicherungsinteresses gemäß Art. 17 Abs. 3 e Datenschutzgrundverordnung, um Auskunft aus dem Betriebsregister – Meldeamt, des Gemeinwohlstaates Königreich Deutschland ...". Der Petent forderte – sinngemäß – von meiner Behörde, dass, wenn dieser (vermeintliche) Auskunftsanspruch nicht erfüllt werde, meine Behörde ein aufsichtsrechtliches Verfahren gegen den genannten Adressaten, eine nicht existente Körperschaft, einleiten solle.
Nun, wer auch immer hier geschädigt worden sein mag, meine Behörde verzeichnet einen zahlenmäßig erheblichen Geschäftsanfall, sodass meine Mitarbeiterinnen und Mitarbeiter derartige mutwillige oder offensichtlich unbegründete vorgetragene Begehren kurz und schmerzlos beantworten, um sich den tatsächlich berechtigten Beschwerden oder Kontrollanregungen der Bürger/innen in datenschutzrechtlichen Fragen widmen zu können.

Meine Behörde wies den Petenten darauf hin, dass sein Auskunftsersuchen an das „Königreich Deutschland" an eine nicht existente juristische Person erfolgte und daher abgewiesen werde.
Zudem war der Petent darauf hinzuweisen, dass sich der Sitz des Adressaten nicht in Sachsen befindet und meine Behörde örtlich unzuständig ist. Eine Abgabe seitens meiner Behörde unterblieb gleichwohl. Denn auch die Datenschutzaufsichtsbehörden der anderen Bundesländer sind ausreichend beschäftigt, und es reicht aus, wenn sich die Datenschutzbehörde eines Bundeslandes mit derartigen Eingaben auseinanderzusetzen hat.

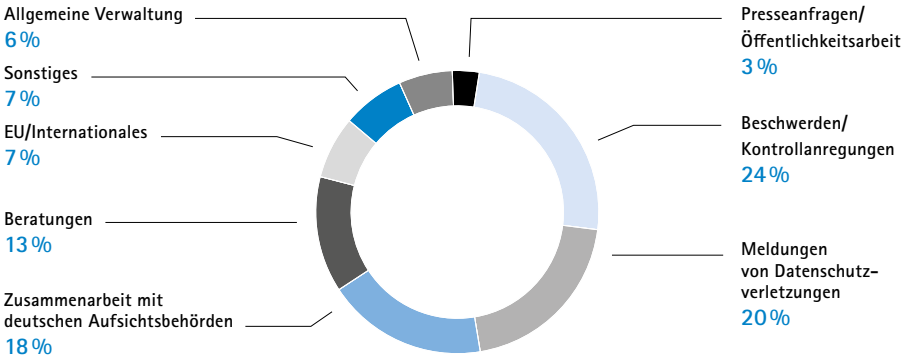
Was ist zu tun?
Ein datenschutzrechtlicher Auskunftsanspruch gemäß Art. 15 DSGVO kann grundsätzlich nur von einer existenten juristischen (oder natürlichen) Person als Verantwortlichem gefordert werden.

6.2 Zahlen und Daten zu den Tätigkeiten 2023

6.2.1 Überblick zu den Arbeitsschwerpunkten

Analog zu den Vorjahren verzeichnete meine Dienststelle 2023 bei Beschwerden/Kontrollanregungen die meisten Vorgänge, dicht gefolgt von gemeldeten Datenschutzverletzungen nach Art. 33 Datenschutz-Grundverordnung. Auch die Zusammenarbeit bzw. Abstimmung mit anderen deutschen Aufsichtsbehörden stellt weiterhin einen Tätigkeitsschwerpunkt dar.

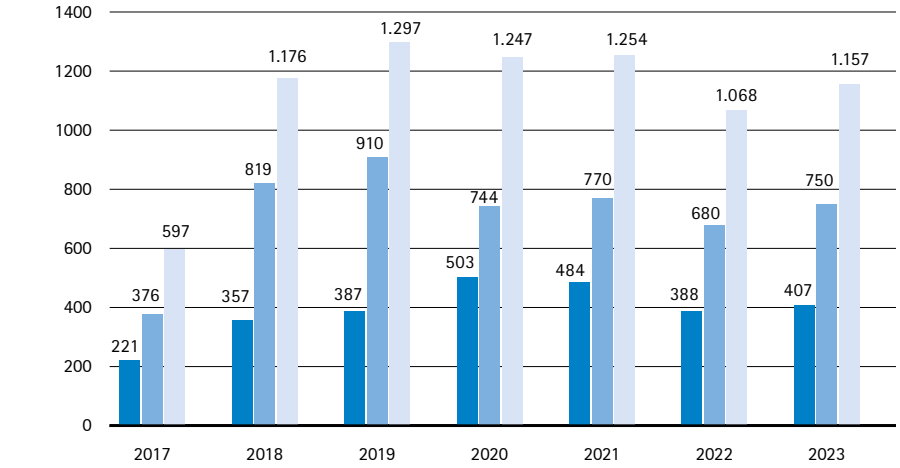
Abbildung 2:
Arbeitsschwerpunkte nach Anzahl der Vorgänge



6.2.2 Beschwerden und Kontrollanregungen

Meine Behörde erreichten im Berichtszeitraum insgesamt 1.157 Eingaben von Personen, die entweder von einem potenziellen Datenschutzverstoß betroffen waren oder als Nichtbetroffene darauf hinwiesen. Das Aufkommen lag über dem des Vorjahres (1.068), jedoch weiterhin unter dem durchschnittlichen Aufkommen der Jahre 2018 bis 2021. Der Zuwachs zum Vorjahr betraf vor allem den nichtöffentlichen Bereich (+10 Prozent).

Abbildung 3:
Beschwerden und Kontrollanregungen



6.2.3 Beratungen

Beratungen umfassen alle schriftlichen datenschutzrechtlichen Auskünfte gegenüber privaten und öffentlichen Stellen. Mit 593 Anfragen lag die Anzahl auf dem Niveau von 2019 und somit deutlich unter dem Niveau der Corona-Jahre 2020 bis 2022. Unabhängig davon beantwortete meine Behörde auch 2023 wieder eine Vielzahl von Datenschutzfragen per Telefon. Diese Anfragen werden statistisch nicht erfasst. Der Rückgang bei den Beratungen betraf in erster Linie den nichtöffentlichen Bereich.

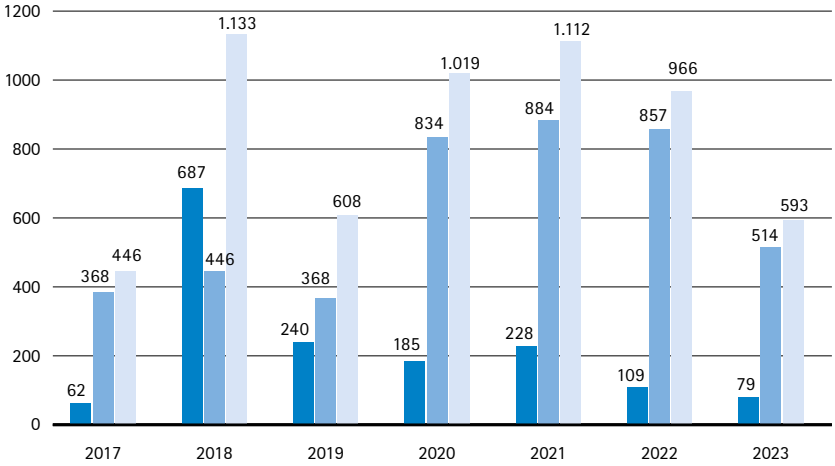


Abbildung 4:
Beratungen

- öffentlicher Bereich
- nichtöffentlicher Bereich
- Beratungen gesamt

6.2.4 Meldungen von Datenpannen

2023 meldeten Verantwortliche 949 Datenschutzverletzungen – ein Plus von 17 Prozent gegenüber dem Vorjahr und zugleich ein neuer Höchststand. Zum Vergleich: 2022 gingen 809 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 liefert der Beitrag 4.4.3.

6.2.5 Abhilfemaßnahmen

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

Warnungen	7
Verwarnungen	11
Anweisungen und Anordnungen	12
Geldbußen (nur nach DSGVO)	9
Widerruf von Zertifizierungen	0

6.2.6 Zusammenarbeit mit europäischen Aufsichtsbehörden – Internal Market Information System

↗ Art. 4, 56–65 DSGVO

Der Europäische Datenschutzausschuss (EDSA) besteht aus den Aufsichtsbehörden der 27 EU-Mitgliedsstaaten (für Deutschland nehmen der Bundesbeauftragte und ein Ländervertreter an den Sitzungen teil) sowie dem Europäischen Datenschutzbeauftragten (EDSB). Hinzu kommen die Aufsichtsbehörden Islands, Liechtensteins und Norwegens (nicht jedoch der Schweiz) als Mitgliedsstaaten des Europäischen Wirtschaftsraums (EWR); sie habe jedoch kein Stimmrecht und dürfen nicht zum Vorsitz gewählt werden.

In der Kommunikationsplattform der europäischen Datenschutzaufsichtsbehörden, dem Internal Market Information System (IMI), haben diese Aufsichtsbehörden jedoch alle das gleiche Gewicht. Ein sächsischer Einspruch kann genauso ein Streitbeilegungsverfahren gemäß Art. 65 Absatz 1 Buchst. a Datenschutz-Grundverordnung (DSGVO) auslösen wie ein französischer oder ein slowakischer. Norwegen hat sogar die erste Dringlichkeitsentscheidung des EDSA herbeigeführt,

welche die irische Aufsichtsbehörde anwies, Meta die Datenverarbeitung zum Zwecke der personalisierten Werbung zu untersagen, sofern als Rechtsgrundlage (fälschlicherweise) ein berechtigtes Interesse und vertragliche Vereinbarungen dienen sollen.

Jede Woche erstelle ich eine Übersicht über die neuen Verfahren in IMI, von denen ich durch notifications benachrichtigt wurde. Sie bildet nicht nur die Grundlage meiner innerbehördlichen Abstimmung über sächsische Eintragungen im IMI, sondern informiert auch über ein sich langsam konsolidierendes Fallrecht der europäischen Aufsichtsbehörden. Die Anzahl der neuen Verfahren variiert: In der ersten Januarwoche des Berichtszeitraums waren es zehn neue Verfahren, in der 36. Kalenderwoche 71. Insgesamt waren es im Berichtszeitraum 2.094 Verfahren, das heißt etwa 40 neue Verfahren je Woche.

Die meisten meiner Eintragungen im IMI stellten klar, dass ich keine betroffene Aufsichtsbehörde bin und deshalb an weiteren Verfahren zur Entscheidung über eine Beschwerde nicht mitwirken darf. Gemäß Art. 4 Nr. 22 DSGVO ist eine Aufsichtsbehörde eine „betroffene Aufsichtsbehörde", wenn entweder der Verantwortliche (in der Regel ein Unternehmen) oder der Auftragsverarbeiter in ihrem Hoheitsgebiet niedergelassen ist oder die Verarbeitung erhebliche Auswirkungen auf betroffene Personen mit Wohnsitz im Mitgliedsstaat dieser Aufsichtsbörde hat oder eine Beschwerde bei dieser Aufsichtsbehörde eingereicht wurde.

Da einige Aufsichtsbehörden im IMI in den Verfahren nach Art. 56 DSGVO zur Ermittlung der federführenden und betroffenen Aufsichtsbehörden angeben, dass alle Aufsichtsbehörden betroffen seien, sind mitunter Klarstellungen erforderlich, dass ich nicht betroffen bin. So konnte ich etwa vermeiden, dass ich an zwei Verfahren gegen französische Hellseherplattformen beteiligt wurde. Insgesamt habe ich im Berichtszeitraum 91 solcher Erklärungen abgegeben. In 13 Verfahren meldete ich mich als betroffene Aufsichtsbehörde, in der Regel, weil in sächsischen Zweigniederlassungen des Verantwortlichen eine Datenverarbeitung erfolgt, die auch

Gegenstand der Beschwerde ist. Im Berichtszeitraum habe ich mich allerdings nicht als federführende Aufsichtsbehörde gemäß Art. 56 Abs. 1 Satz1 DSGVO im IMI gemeldet, da in keinem Verfahren der Beschwerdegegner seine einzige oder Hauptniederlassung in Sachsen hatte.

In sieben IMI-Verfahren stimmte ich im Berichtszeitraum der Billigung von Verhaltensregeln eines Unternehmens gemäß Art. 64 Abs. 1 Buchst. b DSGVO zu.

Nicht immer im Zusammenhang mit konkreten grenzüberschreitenden Fällen stehen informelle Anfragen an die übrigen Aufsichtsbehörden in Verfahren der freiwilligen Amtshilfe nach Art. 61 DSGVO. Häufig möchten andere Aufsichtsbehörden wissen, ob die Datenpanne eines Großunternehmens auch bei einer anderen Aufsichtsbehörde gemeldet wurde oder ob andere schon in Kontakt mit einem Unternehmen getreten sind, welches keine Niederlassung in der EU hat und keinen Vertreter gemäß Art. 27 DSGVO benannt hat. Manchmal werden auch allgemeine Rechtsfragen gestellt, die nicht vom Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) einem Arbeitskreis der Datenschutzkonferenz zugewiesen werden, sondern von allen deutschen Aufsichtsbehörden beantwortet werden können. Eine solche Anfrage nach der Umsetzung und den Erfahrungen des Open Data Act habe ich unter Verweis auf das Bundesgesetz für die Nutzung von Daten des öffentlichen Sektors (Datennutzungsgesetz) 16. Juli 2021 (Bundesgesetzblatt I, 2941, 2942, 4114) abschlägig beantwortet. In einem Verfahren war ich die einzige deutsche Aufsichtsbehörde, die sich zu Konsultationen bei Datenschutz-Folgenabschätzungen gemäß Art. 36 DSGVO äußerte. Insgesamt beantwortete ich im Berichtszeitraum sechs solcher Anfragen.

Eine Beratung durch die Zentrale Anlaufstelle (ZAST) beim BfDI nahm ich gelegentlich bei schwierigen Fragen in Anspruch. Erfreulicherweise wurde eine IMI-Anfängerschulung und ein IMI-Workshop in Bonn und Wiesbaden angeboten und von einigen meiner Mitarbeiter mit Gewinn besucht.

Im nächsten Jahr sollen die fünf Fälle, in denen ich federführende Aufsichtsbehörde bin, abgeschlossen werden.

6.2.7 Register der benannten Datenschutzbeauftragten

↗ Art. 37 Abs. 1 und 7 DSGVO

Im Berichtszeitraum gingen 1.029 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 Datenschutz-Grundverordnung (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.

6.2.8 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.

Üblicherweise steigt die Anzahl der Rechtsetzungsvorhaben, wenn sich Legislaturperioden dem Ende nähern. So war das auch im Berichtszeitraum, in dem ich von der sächsischen Staatsregierung häufiger als noch im Vorjahr konsultiert wurde. Weiterhin beteiligten mich die Landtagsfraktionen regelmäßig bei der Erarbeitung von Gesetzentwürfen und Änderungsanträgen. Hinzu kamen Stellungnahmen zu verschiedenen Vorhaben, die im Zusammenhang mit der Bundes-

gesetzgebung standen und mit denen sich auch die Datenschutzkonferenz befasste.

Die wichtigsten im Jahr 2023 abgegebenen Stellungnahmen:

- Agrarstrukturgesetz
- Änderung der sächsischen Vollzugsgesetze
- Integrations- und Teilhabegesetz
- Gleichstellungsgesetz
- Verwaltungsvollstreckungsgesetz
- Bundesreisekostengesetz
- Personalvertretungsgesetz
- Gesetz zur Neuregelung des Nachrichtendienstgesetzes
- Gesetz über den Schutz der Versammlungsfreiheit
- Gesetz zur Regelung berufsanerkennungsrechtlicher Verfahren
- Gesetz zur Anpassung des Rechts über den öffentlichen Gesundheitsdienst im Freistaat Sachsen
- Gesetz zur Reform des Sächsischen Heimrechts
- Sächsisches Gesetz zur Durchführung des Vierzehnten Buches Sozialgesetzbuch und weiterer Sozialer Entschädigungsgesetze (SächsDGSGB XIV)

Wie erwähnt werde ich in vielen Fällen bereits auf der Arbeitsebene der Ministerien in die Erarbeitung von Rechtsregelungen einbezogen. Das 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.

6.2.9 Ressourcen

Im sechsten Jahr der Datenschutz-Grundverordnung lag das Arbeitsaufkommen bei Beschwerden, Beratungen und Datenpannen-Meldungen weiterhin auf hohem Niveau.

Die für die Erfüllung meiner Aufgaben erforderlichen Haushaltsmittel (Personal- und Sachausgaben) werden seit Inkrafttreten des Sächsischen Datenschutzdurchführungsgesetzes (SächsDSDG) vom 26. April 2018 im Einzelplan 13 des jeweiligen Staatshaushaltsplanes abgebildet. Im Haushaltsjahr 2023 standen mir insgesamt 41 Stellen zur Verfügung.
Die Erfüllung meiner Aufgaben als Sächsische Datenschutzbeauftragte ist nach wie vor herausfordernd. Die Kapazitäten meiner Behörde werden größtenteils durch reaktive Tätigkeiten absorbiert – die Bearbeitung von Beschwerden, die Begleitung von Rechtssetzungsvorhaben, die Koordinierung mit den übrigen Aufsichtsbehörden in der Europäischen Union und so weiter. Für meine für eine Aufsichtsbehörde zwingend erforderliche Fähigkeit, proaktiv zu kontrollieren und zu beraten, bleiben nach wie vor zu wenige Kapazitäten übrig.
Hinzu kommt, dass ich seit dem 1. Januar 2023 als Transparenzbeauftragte weitere Aufgaben übernommen habe. In dieser Funktion bin ich für die Kontrolle der Einhaltung des Sächsischen Transparenzgesetzes, die Bearbeitung von Petitionen, die Beratung der transparenzpflichtigen Stellen sowie die Erstattung von Gutachten und Berichten zuständig. Wie im Tätigkeitsbericht 2022 erwähnt, wurden mir für diese Tätigkeit zwei Stellen zuerkannt.

Fortbildung von Beschäftigten

Mehrere Mitarbeiterinnen und Mitarbeiter nahmen an Veranstaltungen zur Internet- und Computersicherheit teil. Des Weiteren besuchten Bedienstete Fortbildungen unter anderem zur elektronischen Aktenführung und nahmen an Fortbildungen zum Datenwirtschaftsrecht sowie zum Informationsfreiheitsrecht teil.

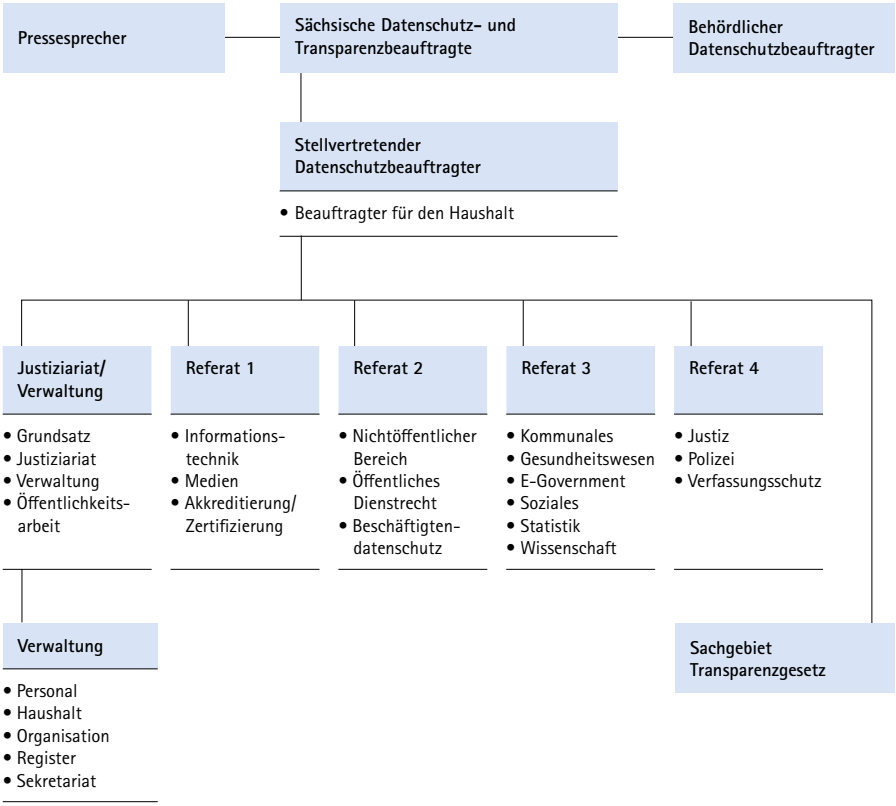


Abbildung 6:
Vereinfachtes Organigramm der Behörde (Stand: 31.12.2023)

6.3 Datenschutzaufsichtliche Befugnisse, verwaltungsrechtliche Entscheidungen

6.3.1 Zwangsgeldverfahren bei nichtöffentlichen Stellen

↗ § 19 Abs. 5 SächsVwVG, § 40 Abs. 4 BDSG, § 92 Abs. 2 VwGO, § 383 Abs. 1 ZPO, Art. 31 DSGVO

Art. 31 Datenschutz-Grundverordnung (DSGVO) regelt die Zusammenarbeit der Verantwortlichen mit der Aufsichtsbehörde. Nach dieser Vorschrift haben der Verantwortliche und der Auftragsverarbeiter und gegebenenfalls deren Vertreter

auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammenzuarbeiten. Ergänzend dazu regelt § 40 Abs. 4 Bundesdatenschutzgesetz, dass die der Aufsicht unterliegenden Stellen sowie die mit deren Leitung beauftragten Personen der Aufsichtsbehörde auf Verlangen die für die Erfüllung ihrer Aufgaben erforderlichen Auskünfte zu erteilen haben. Der Auskunftspflichtige kann die Auskunft lediglich auf solche Fragen verweigern, deren Beantwortung ihn selbst oder einen der in § 383 Abs. 1 Nr. 1 bis 3 der Zivilprozessordnung bezeichneten Angehörigen der Gefahr strafgerichtlicher Verfolgung oder eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten aussetzen würde.

Soweit Verantwortliche ihrer vorstehend dargestellten Kooperationspflicht nicht nachkommen bzw. davon ausgehen, sich durch Schweigen oder Nichtreagieren ihrer Pflicht zur Erteilung von Auskünften oder zur Bereitstellung von Unterlagen entziehen zu können, bleibt mir regelmäßig nur der Übergang ins förmliche Heranziehungsverfahren. Mit der Androhung eines Zwangsgeldes verbundene Auskunftsheranziehungsbescheide sind insoweit ein adäquates und wirksames Mittel, um von Verantwortlichen, die mindestens zwei aufsichtsbehördliche Schreiben ignoriert haben oder die Auskunftserteilung aktiv verweigern, die zur Aufgabenerfüllung erforderlichen Auskünfte zu erhalten. Spätestens nach der Festsetzung eines Zwangsgeldes reagieren dann die meisten Verantwortlichen und stellen mir die geforderten Auskünfte und Unterlagen bereit. Im Berichtszeitraum habe ich acht Zwangsgelder mit einer Gesamtsumme von 45.000 Euro (Vorjahr: 12.000 Euro) festgesetzt.

Man sollte meinen, dass sich Verantwortliche, die meine zunächst formlosen Auskunftsersuchen ignoriert und anschließend auch nicht auf einen Heranziehungsbescheid reagiert haben, sich dann aber jedenfalls nach Erhalt des darauf folgenden Zwangsgeldbescheides bei mir melden. Doch weit gefehlt. Es scheint notorische Auskunftsverweigerer zu geben, die finanziell offensichtlich auch recht gut gestellt sind und die den Zweck des Zwangsgeldverfahrens wohl noch nicht durchschaut haben und die die Angelegenheit daher

dem Anschein nach aussitzen wollen. Tatsächlich erlischt die Auskunftspflicht des Verantwortlichen mit der Zahlung eines Zwangsgeldes aber nicht. Nach § 19 Abs. 5 Sächsisches Verwaltungsvollstreckungsgesetz dürfen Zwangsmittel wiederholt und so lange angewandt werden, bis der Verantwortliche seinen Verpflichtungen nachgekommen ist. Das Zwangsverfahren wird aber eingestellt, sobald die geforderten Auskünfte vollständig erteilt worden sind.
Die von mir im Berichtszeitraum betriebenen acht Zwangsverfahren betreffen ausschließlich Videoüberwachungsfälle, dabei aber lediglich fünf Verantwortliche:

Videoüberwachung öffentlicher Verkehrsbereiche durch einen privaten Grundstückseigentümer

„Achtung Kamera! Hinweise zur Videoüberwachung für Bürgerinnen und Bürger, Wirtschaft und Verwaltung":
↗ sdb.de/achkam

Eine Privatperson hatte zur Sicherung ihres Wohngrundstücks eine Videokamera betrieben, bei der der Verdacht bestand, dass sie nicht nur die Grundstückseinfahrt, sondern auch den davor befindlichen öffentlichen Verkehrsbereich erfasste. Nachdem der Betreiber weder auf das erste formlose Anschreiben noch auf die anschließende Anhörung und auch nicht auf den folgenden Heranziehungsbescheid reagiert hatte, folgte dann eine Zwangsgeldfestsetzung in Höhe von 1.800 Euro, die auch sofort die gewünschte Wirkung zeigte. Der Adressat erwachte aus seinem Tiefschlaf und erteilte die geforderten Auskünfte. Daraufhin habe ich das Zwangsverfahren eingestellt – der Verantwortliche musste statt des Zwangsgeldes lediglich noch die Verfahrenskosten begleichen. Insoweit ein unspektakulärer, geradezu klassischer Fall, bei dem das Zwangsmittel unmittelbar seinen Zweck erfüllt hat.

Videoüberwachung öffentlicher Verkehrsbereiche durch einen Gewerbetreibenden

Der Fall ist schon etwas gravierender, unterscheidet sich vom zuvor geschilderten Fall im Ausgangspunkt aber nur insoweit, als dass es sich um einen Gewerbetreibenden handelt, der eine Videokamera an seiner Garage angebracht hatte. Auch hier zunächst der gleiche Ablauf, wobei das initial

festgesetzte Zwangsgeld hier 1.900 Euro betrug und leider nicht die beabsichtigte Wirkung zeigte. Stattdessen wurde das Zwangsgeld kommentarlos bezahlt, woraufhin das Zwangsgeld auf 3.800 Euro verdoppelt wurde. Erst das nach Zahlung auch dieses Betrags erneut festgesetzte Zwangsgeld in Höhe von 7.600 Euro führte schließlich zum Erfolg, sodass von einer weiteren Vollstreckung abgesehen werden konnte. Überraschend war dabei die Mitteilung des Verantwortlichen, dass die betreffende Kamera schon vor Längerem demontiert worden sei. Weshalb er dies nicht schon in einem früheren Verfahrensstadium mitgeteilt hatte, blieb sein Geheimnis. Jedenfalls hätte er sich dadurch die vorangegangenen Zwangsgelder sparen können.

Videoüberwachung in und außerhalb einer Spielhalle

Ausgangspunkt des betreffenden Aufsichtsverfahrens waren behördliche Feststellungen, dass eine Spielhallenbetreiberin mit ihrer Videoüberwachungsanlage auch den öffentlichen Verkehrsraum vor dem Gebäude miterfasst. Dies hatte ich zum Anlass einer Kontrolle der Videoüberwachungsanlage insgesamt genommen. Doch auch hier stieß ich bislang auf stummen Widerstand. Das Unternehmen, eine GmbH, reagiert nicht auf meine Auskunftsforderungen. Bisher wurden drei Zwangsgelder in Höhe von 3.600 Euro, 7.200 Euro und 14.400 Euro bezahlt. Ich werde im nächsten Tätigkeitsbericht über den Fortgang der Angelegenheit berichten. Ergänzend prüfe ich die parallele Einleitung eines Bußgeldverfahrens.

Videoüberwachung in einer Diskothek

Tätigkeitsbericht 2021:
↗ sdb.de/tb2022

Dies ist der bislang extremste und derzeit immer noch offene Fall – ich hatte darüber bereits im letzten Tätigkeitsbericht (6.3.1, Seite 168 ff.) informiert. Worum es dabei ging:
Nach längerem, wenig ergiebigem und von zahlreichen Anträgen auf Fristverlängerung geprägtem Schriftverkehr mit einem anwaltlich vertretenen Diskothekenbetreiber hatte ich bereits 2021 einen Auskunftsheranziehungsbescheid erlassen. Nachdem als einzige Reaktion auf diesen Bescheid ein erneuter anwaltlicher Antrag auf Fristverlängerung zu ver-

zeichnen war, hatte ich das angedrohte Zwangsgeld in Höhe von 800 Euro festgesetzt und die Vollstreckung eingeleitet. Der Verantwortliche hat das Zwangsgeld dann schließlich bezahlt, darüber hinaus aber in keiner Weise reagiert.

Folgerichtig musste ich ein weiteres, doppelt so hohes Zwangsgeld (1.600 Euro) festsetzen. Gegen den – sofort vollziehbaren – Festsetzungsbescheid hat der Bevollmächtigte des Verantwortlichen gerade noch rechtzeitig vor Eintritt der Bestandskraft Klage eingereicht und insbesondere auch Antrag auf Wiederherstellung der aufschiebenden Wirkung gestellt, verfiel danach aber wieder in sein altes Muster, indem er gegenüber dem Gericht zunächst einen Antrag auf Fristverlängerung stellte, sich danach aber nicht mehr meldete. Folgerichtig wurde der Antrag auf wiederherstellende Wirkung auch abgewiesen. Das Verwaltungsgericht hat dazu festgestellt, dass der Heranziehungsbescheid bestandskräftig, mit einer zutreffenden Rechtsmittelbelehrung versehen und auch ordnungsgemäß zugestellt worden ist. Es sei auch nicht ersichtlich, dass der Bescheid nichtig sein könnte. Das betreffende (zweite) Zwangsgeld sei unter angemessener Fristsetzung angedroht und schriftlich festgesetzt worden. Bis zum Zeitpunkt der gerichtlichen Entscheidung sei der Verantwortliche seiner Pflicht zur Vornahme der geschuldeten Handlung, nämlich der Auskunftserteilung gemäß der Regelungen im ursprünglichen Heranziehungsbescheid, nicht nachgekommen.

Auch in der Hauptsache hatte die Klage keinen Erfolg. Der Bevollmächtigte hatte – nach Aufforderung durch das Verwaltungsgericht – weder die geforderte Klagebegründung vorgelegt noch sich überhaupt gemeldet. Das Klageverfahren ist daher durch Beschluss eingestellt worden. Gemäß § 92 Abs. 2 Satz 1 Verwaltungsgerichtsordnung gilt eine Klage als zurückgenommen, wenn der Kläger das Verfahren trotz Aufforderung des Gerichts länger als zwei Monate nicht betreibt. Das Zwangsgeld hatte der Verantwortliche bereits vorher bezahlt.

Im Ergebnis blieb mir jetzt nichts weiter übrig, als nun erneut ein weiteres, wiederum doppelt so hohes Zwangsgeld (3.200 Euro) festzusetzen. Daraufhin wiederholte sich der Verfahrensablauf in bekannter Weise; es wurde lediglich kein erneuter Antrag auf Wiederherstellung der aufschiebenden Wirkung gestellt. Dies bedeutet, das Zwangsgeld wurde bezahlt, und es wurde Klage eingereicht. Die Klage wurde nicht begründet, woraufhin das Gericht das Verfahren durch Beschluss eingestellt hat.

Auch bezüglich des nun folgenden Zwangsgeldes in Höhe von 6.400 Euro folgt der Verfahrensablauf dem gleichen Muster. Das Zwangsgeld wurde bezahlt, und es wurde auch wieder Klage eingereicht, diese jedoch trotz gerichtlicher Aufforderung nicht begründet. Wiederum hat das Gericht das Verfahren durch Beschluss eingestellt. Ich habe nunmehr parallel zu diesem Aufsichtsverfahren auch ein Bußgeldverfahren wegen Verstoßes gegen die Kooperationspflicht des Art. 31 DSGVO eingeleitet. Im Rahmen der Anhörung hat sich das Unternehmen – wie anders kaum zu erwarten war – bisher nicht geäußert. Ich werde im nächsten Tätigkeitsbericht über den weiteren Fortgang berichten.

Videoüberwachung des Freisitzes eines Bistros

Der letzte hier zu beschreibende Fall ist wieder eher unspektakulär. Inhaltlich ging es um die Videoüberwachung der zu einem Bistro gehörenden Freisitzfläche, wobei auch die Videoüberwachung angrenzender öffentlicher Verkehrsbereiche im Raum stand. Zwar hatte sich der Betreiber des Gastronomiebetriebes schließlich – wenn auch erst nach Erlass eines Heranziehungsbescheides – zum Sachverhalt geäußert, dabei aber die geforderten Auskünfte nur teilweise erteilt. Auch in einem solchen Fall kann natürlich ein Zwangsgeld festgesetzt werden, wenngleich dies dann natürlich vergleichsweise gering ausfällt. Nur mit einer vollständigen Auskunftserteilung kann die Festsetzung eines Zwangsgeldes umgangen werden. Eine abschließende Information zu diesem – zum Ende des Berichtszeitraums noch offenen – Verfahren kann erst im nächsten Tätigkeitsbericht erfolgen.

Was ist zu tun?
Mit der Datenschutzaufsichtsbehörde sollte kooperiert werden, andernfalls drohen empfindliche Zwangsgelder. Mit der Zahlung eines Zwangsgeldes können sich Verantwortliche ihrer Auskunfts- oder Vorlagepflicht nicht entziehen.

6.3.2 Richterliche Überprüfung der Aufsichtstätigkeit

↗ Art. 52, 57, 58, 77, 78 DSGVO

Als Datenschutzaufsichtsbehörde steht man – jedenfalls im Zuge der Beschwerdebearbeitung – regelmäßig zwischen den Fronten: Auf der einen Seite die betroffenen Personen mit ihrem Vorwurf eines Datenschutzverstoßes, auf der anderen Seite die Verantwortlichen mit der ihrer Auffassung nach rechtmäßigen Verarbeitung personenbezogener Daten. Bejaht man den Datenschutzverstoß und zeigen sich Verantwortliche nicht einsichtig, müssen Abhilfemaßnahmen förmlich angeordnet werden, und Verantwortliche können gerichtlich dagegen vorgehen. Verneint man hingegen einen Datenschutzverstoß, haben auch betroffene Personen nach Art. 78 Abs. 1 Datenschutz-Grundverordnung (DSGVO) ein Klagerecht.

Selbst bei noch so sorgfältiger Beschwerdebearbeitung läuft man also immer Gefahr einer gerichtlichen Auseinandersetzung, wobei das Risiko einer Klage durch betroffene Personen erfahrungsgemäß größer ist. Zum einen sind die Abschlussnachrichten meist nicht so umfangreich begründet, wie etwa Verwaltungsakte gegen Verantwortliche; zum anderen lassen sich betroffene Personen mangels vertiefter Kenntnisse des Datenschutzrechts regelmäßig nicht so einfach davon überzeugen, dass sie im Unrecht sind. Oftmals reicht schon die Mitteilung eines ihnen nicht genehmen Ergebnisses zur Klageerhebung aus. Damit verbunden wird die Hoffnung, dass das Gericht die Bewertung der Aufsichtsbehörde aufhebt und durch eine eigene Entscheidung im Sinne der betroffenen Personen ersetzt.

Auch in dem in diesem Tätigkeitsbericht erwähnten Klageverfahren (siehe 2.1.3) war das im Grunde genommen so. Der Beschwerdeführer war schlichtweg mit dem mitgeteilten Ergebnis nicht einverstanden und hatte daher Klage beim Verwaltungsgericht Dresden eingereicht. Lange Zeit fehlte es dabei an einem konkreten Klageantrag, sodass nicht klar war, was – außer einem anderen Ergebnis – der Kläger kon-

kret überhaupt erreichen wollte. Letztendlich beantragte er dann mithilfe des Gerichts, dass meine Behörde verpflichtet werden solle, unter Aufhebung meines Bescheides – gemeint war meine Abschlussnachricht – über seine Beschwerde unter Beachtung der Rechtsauffassung des Gerichts neu zu entscheiden. Wie im Beitrag 2.1.3 bereits ausgeführt, hat das Gericht aber meine datenschutzrechtliche Bewertung inhaltlich mitgetragen – sie sei materiell-rechtlich nicht zu beanstanden – und die Klage abgewiesen. Meine Behörde habe die Beschwerde des Klägers umfassend geprüft, sie sei zu einem nicht zu beanstandenden Ergebnis gekommen und habe den Kläger auch rechtzeitig über den Fortgang und das Ergebnis der Untersuchung unterrichtet. Das Verwaltungsgericht hat zudem festgestellt, dass der Kläger bei festgestellten Verstößen keinen Anspruch auf bestimmte aufsichtsrechtliche Maßnahmen, sondern nur einen Anspruch auf fehlerfreie Ermessensausübung hinsichtlich der Untersuchungs- und Abhilfemaßnahmen meiner Behörde hat.

Bislang war umstritten, ob sich aus der Datenschutz-Grundverordnung für die Verwaltungsgerichte tiefergehende inhaltliche Prüfungsbefugnisse ergeben oder ob Beschwerdeverfahren eher petitionsähnlichen Grundsätzen folgen und damit Entscheidungen der Aufsichtsbehörden für die Verwaltungsgerichte nur eingeschränkt überprüfbar sind.

Der Europäische Gerichtshof hat sich in dieser Frage – ausgehend von einer Vorlagefrage des Verwaltungsgerichts Wiesbaden – jetzt klar positioniert (EuGH, Urteil vom 7. Dezember 2023 – C-26/22 –, juris, vgl. dazu Beitrag 9.3 „Scoring, Löschpflicht und Löschanspruch, EuGH-Urteile vom 07.12.2023, C-634/21 und C-26/22 bzw. C-64/22"). Ausgehend von der Formulierung in Art. 78 Abs. 1 DSGVO, wonach jede natürliche oder juristische Person das Recht auf einen „wirksamen" gerichtlichen Rechtsbehelf gegen einen sie betreffenden rechtsverbindlichen Beschluss einer Aufsichtsbehörde hat, hat der Gerichtshof festgestellt, dass ein rechtsverbindlicher Beschluss einer Aufsichtsbehörde der vollständigen inhaltlichen Überprüfung durch ein Gericht unterliegt (Randziffer 70). Bei einem Beschwerdeverfahren nach der

Datenschutz-Grundverordnung handele es sich nicht um ein petitionsähnliches Verfahren (Randziffer 58), vielmehr sei es als ein Mechanismus konzipiert worden, der geeignet ist, die Rechte und Interessen der betroffenen Personen wirksam zu wahren. Die Aufsichtsbehörde müsse eine Beschwerde mit aller gebotenen Sorgfalt bearbeiten (Randziffer 56), verfüge hinsichtlich der in Art. 58 Abs. 2 DSGVO aufgezählten Abhilfebefugnisse allerdings über ein Ermessen in Bezug auf die geeigneten und erforderlichen Mittel (Randziffer 68). Demgemäß verfüge auch das mit einem Rechtsbehelf nach Art. 78 Abs. 1 DSGVO befasste nationale Gericht zwar über eine umfassende Befugnis zur Prüfung aller Sach- und Rechtsfragen im Zusammenhang mit dem betreffenden Rechtsstreit, sei aber nicht befugt, seine Beurteilung der Wahl der geeigneten und erforderlichen Abhilfebefugnisse an die Stelle der Beurteilung der Aufsichtsbehörde zu setzen, sondern könne lediglich prüfen, ob die Aufsichtsbehörde die Grenzen ihres Ermessens eingehalten habe (Randziffer 69).

Betrachtet man die oben bzw. im Beitrag 2.1.3 erwähnte verwaltungsgerichtliche Entscheidung, erkennt man, dass diese im Wesentlichen bereits im Sinne der Entscheidung des Europäischen Gerichtshofes erfolgt ist. Grundlegende Änderungen in der Rechtsprechungspraxis sind in Sachsen insoweit also nicht zu erwarten. Die Entscheidung des Europäischen Gerichtshofes beeinträchtigt auch nicht die in Art. 52 DSGVO garantierte Unabhängigkeit der Aufsichtsbehörden, denn diese betrifft ausschließlich Beeinflussungen der Aufsichtstätigkeit jedweder Art von außen, nicht aber die gerichtliche Überprüfbarkeit materiell-rechtlicher Entscheidungen der Aufsichtsbehörde.

6.4 Geldbußen und Sanktionen, Strafanträge

6.4.1 Ordnungswidrigkeitenverfahren im öffentlichen Bereich

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

- § 38 Absatz 1 Sächsisches Datenschutzgesetz alte Fassung (§ 38 Absatz 3 Satz 1 SächsDSG alte Fassung),
- § 22 Absatz 1 Sächsisches Datenschutzdurchführungsgesetz (§ 22 Absatz 3 SächsDSDG),
- § 48 Absatz 1 Sächsisches Datenschutz-Umsetzungsgesetz (§ 48 Absatz 3 Satz 1 SächsDSUG),
- § 66 Absatz 1 Sächsisches Justizvollzugsdatenschutzgesetz (§ 66 Absatz 3 SächsJVollzDSG) und
- § 85a des Zehnten Buches Sozialgesetzbuch – Sozialverwaltungsverfahren und Sozialdatenschutz – in Verbindung mit § 41 Bundesdatenschutzgesetz, Art. 83 Absatz 5 Datenschutz-Grundverordnung (Art. 58 Absatz 2 Buchst. i DSGVO, § 14 Absatz 1 SächsDSDG).

Im Berichtszeitraum waren im öffentlichen Bereich insgesamt 60 Bußgeldverfahren anhängig. Davon wurden 15 mit einem Bußgeld abgeschlossen, wobei in drei Verfahren Einspruch gegen den erlassenen Bußgeldbescheid eingelegt worden ist. Eine Entscheidung steht jeweils noch aus. In 17 Verfahren erfolgte eine Einstellung bzw. wurde von der Verfolgung abgesehen. In einem Verfahren wurde eine Verwarnung ohne Verhängung eines Verwarnungsgeldes ausgesprochen, drei Verfahren wurden an die zuständige Behörde abgegeben. 24 Verfahren befanden sich zum Ende des Berichtszeitraumes noch in Bearbeitung.

Berichtszeitraum		01.01.–31.12.2023
anhängig gesamt		**60**
davon	Verfahren aus vorherigem Berichtszeitraum	18
	neu eingegangene Verfahren	42
abgeschlossen		**36**
davon	mit Bußgeld	15
	mit Verwarnungsgeld	0
	mit Verwarnung ohne Verwarnungsgeld	1
	eingestellt/von Verfolgung abgesehen	17
	an zuständige Behörde abgegeben	3
noch in Bearbeitung		**24**
Summe festgesetzter Buß- und Verwarnungsgelder in Euro		**28.090**

Tabelle 1:
Ordnungswidrigkeiten-verfahren im öffentlichen Bereich

Die Summe der festgesetzten Buß- und Verwarnungsgelder belief sich auf 28.090 Euro, die der rechtskräftigen auf 7.740 Euro. Gegenüber dem vergangenen Berichtszeitraum hat sich die Zahl der neu eingegangenen Ordnungswidrigkeitenverfahren mehr als verdoppelt. Auffällig war, dass die zu bearbeitenden Ordnungswidrigkeitenverfahren an Komplexität gewonnen haben und oftmals gleich eine Vielzahl von Verstößen beinhalten, was zu einem erhöhten Bearbeitungsaufwand der einzelnen Verfahren führt.

In ca. 80 Prozent der im Berichtszeitraum anhängigen Verfahren standen/stehen Bedienstete der sächsischen Polizei in Verdacht, unbefugt dienstlich erlangte personenbezogenen Daten verarbeitet zu haben (ordnungswidrig gemäß § 48 Abs. 1 Nr. 1 SächsDSUG). Des Weiteren bestand/besteht gegen Bedienstete unterschiedlichster sächsischer (Sozial-) Behörden der Verdacht, nicht offenkundige personenbezogene Daten unbefugt verarbeitet zu haben. Der hohe Anteil von Ordnungswidrigkeitenverfahren gegen Polizeibedienstete resultiert dabei zum einen aus dem überdurchschnittlichen

Anzeigeverhalten der Polizeidienststellen, welche ein datenschutzrechtliches Fehlverhalten ihrer Bediensteten konsequent verfolgen, zum anderen zeigt er, dass nach wie vor Unsicherheiten und Schwierigkeiten im Umgang mit dienstlich zur Verfügung stehenden Daten bestehen.
Bei dem Großteil der Ordnungswidrigkeitenverfahren gegen Bedienstete der sächsischen Polizei handelt es sich, wie bereits in den vergangenen Jahren, um privat motivierte Abrufe von personenbezogenen Daten aus den der Polizei zur Verfügung stehenden Datenbanken, zum Beispiel zu Freunden, Kollegen, Nachbarn, anderen Bekannten oder sich selbst. Aber auch Datenübermittlungen an Dritte oder eine privaten Zwecken dienende Speicherung von dienstlich erlangten Daten spielten im Berichtszeitraum eine Rolle. Zur Veranschaulichung der Bandbreite bearbeiteter Vorgänge werden nachfolgend drei ausgewählte Fälle vorgestellt:

Abfrage von Daten zum eigenen Fahrzeug nach Verkehrsunfall

Im vergangenen Jahr informierte mich eine Polizeidienststelle über den Verdacht einer Datenschutzverletzung in einem ungewöhnlichen Zusammenhang. Grund der Ordnungswidrigkeitenanzeige war die Abfrage eines Bediensteten in der Datenbank ZEVIS, dem Zentralen Verkehrsinformationssystem. Über das Informationssystem ZEVIS können unter anderem Daten aus dem Zentralen Fahrzeugregister, dem Fahreignungsregister und dem Fahrerlaubnisregister abgerufen werden. Datenabrufe über ZEVIS sind für Polizeibedienstete zunächst nicht ungewöhnlich; sie geschehen oftmals im Kontext der Verfolgung von Straftaten und Verkehrsordnungswidrigkeiten oder bei Verkehrskontrollen. In diesem Fall hatte die betreffende Dienststelle jedoch Grund zur Annahme, dass die Abfrage unberechtigt erfolgte.
Hintergrund des Geschehens war ein Unfall, bei welchem der Verursacher mit seinem Pkw ein anderes parkendes Fahrzeug beschädigt hatte. Der Halter des beschädigten Fahrzeuges war zu diesem Zeitpunkt nicht vor Ort. Zwei Passanten beobachteten den Verkehrsunfall und bemerkten, wie sich der

Verursacher kurze Zeit später von der Unfallstelle entfernte. Sie stellten fest, dass sich an dem geschädigten Fahrzeug weder eine Notiz befand, noch der Geschädigte zu seinem Fahrzeug zurückgekehrt war. Die beiden Zeugen erstatteten noch am selben Tag bei dem zuständigen Polizeirevier eine Anzeige wegen unerlaubten Entfernens vom Unfallort. Drei Tage nach dem Unfall erschien auf dem Revier ein Polizeibediensteter, der sich als Verursacher des Unfalls zu erkennen gab. Am selben Tag suchte der Polizeibedienstete auch den Geschädigten auf, um sich persönlich für den Vorfall zu entschuldigen.

Auch wenn der Verursacher des Unfalls gefunden war, stellte sich die Frage, weshalb der Polizeibedienstete erst drei Tage nach dem Unfallgeschehen das Polizeirevier aufsuchte und sich selbst anzeigte. Nach einer Protokolldatenauswertung wurde festgestellt, dass er kurz vor seiner Selbstanzeige in dem polizeilichen Auskunftssystem ZEVIS sein eigenes Kfz-Kennzeichen abgefragt hatte. Mit hoher Wahrscheinlichkeit stellte er dabei fest, dass eine Anzeige gegen ihn vorlag. Es war anzunehmen, dass sich der Polizeibedienstete kurz darauf als Unfallverursacher zu erkennen gab, um weitere negative Konsequenzen für sich zu vermeiden. Weiterhin war nicht auszuschließen, dass er die gewonnenen Erkenntnisse nutzte, um sein Aussageverhalten in einem gegen ihn gerichteten Strafverfahren anpassen zu können.

Bei der Frage, ob polizeiliche Datenrecherchen befugt erfolgt sind oder nicht, ist es irrelevant, ob die Daten einen Dritten oder die eigene Person betreffen (= „Selbstauskunft"). Sämtliche personenbezogenen Daten, die in den polizeilichen Datenbanken gespeichert sind, sind ausschließlich für die polizeiliche Tätigkeit bestimmt – auch bei einem Abruf von eigenen Daten braucht es einen konkreten dienstlichen Anlass. Einen solchen aber hatte der Polizeibedienstete nicht, seine Abfrage diente ganz offensichtlich allein dem privat motivierten Zweck der Prüfung, ob etwas gegen ihn vorlag.

Gegenüber dem Polizeibediensteten erging ein Bußgeldbescheid wegen der unbefugten Verarbeitung von nicht offenkundigen personenbezogenen Daten.

Wie dieser Fall zeigt, können selbst Abfragen zur eigenen Person bzw. zum eigenen Fahrzeug Erkenntnisse liefern, die den Betroffenen selbst bis dahin nicht bekannt waren.

„Abfotografieren" polizeilicher Dokumente mit privatem Smartphone

In einem anderen Fall informierte mich eine Polizeidienststelle über den Verdacht eines Datenschutzverstoßes durch einen ihrer Bediensteten. Im Rahmen eines Ermittlungsverfahrens der Staatsanwaltschaft war das Mobiltelefon des betroffenen Bediensteten beschlagnahmt und durchsucht worden. Bei der Auswertung des Mobiltelefons wurden darauf Hunderte Fotos von polizeilichen Ermittlungsakten und anderen polizeilichen Dokumenten festgestellt. Der Großteil der fotografierten Schriftstücke enthielt eine Vielzahl an personenbezogenen Daten, darunter Namen, Geburtstage, Privatadressen, Zeugenaussagen, ärztliche Untersuchungsberichte etc. Ein dienstlicher Anlass dafür, dass der Bedienstete die Fotos mit seinem privaten Telefon aufgenommen und darauf gespeichert hatte, war für mich nicht ersichtlich, weshalb ein Ordnungswidrigkeitenverfahren wegen eines Verstoßes nach dem Sächsischen Datenschutzumsetzungsgesetz gegen den Betroffenen eingeleitet wurde. Auf meinen Antrag wurden die betreffenden Dateien gesondert beschlagnahmt, da die ursprüngliche Beschlagnahme des Mobiltelefons in einem staatsanwaltschaftlichen Ermittlungsverfahren wegen des Verdachts einer anderen Straftat durchgeführt worden war und die nun relevanten Dateien nicht umfasste.

Der Bedienstete gab innerhalb des Verfahrens an, er habe die Fotos zu Beginn seiner Dienstzeit aufgenommen, um sich mit den dienstlichen Aktenstrukturen und Schreibweisen vertraut zu machen. Er erklärte, er habe die Fotos von bestimmten Akten oder Aktenteilen auf seinem Handy gespeichert, wenn sich neue oder komplizierte Fallkonstellationen ergaben. Die Fotos habe er dann beispielsweise als Vorlage oder Muster für das Erstellen von eigenen Schriftstücken genutzt. Dass der Beamte die Fotos tatsächlich aus diesen Gründen

auf seinem Mobiltelefon gespeicherte hatte, war glaubhaft, denn auf einigen der Fotos ließen sich Notizen und Markierungen erkennen, die der Beamte für sein „Selbststudium" angefertigt hatte. Unter den Fotos befanden sich mehrere Dokumente, in denen probeweise als Daten „Max Mustermann" angegeben worden war, in manchen Fällen hatte der Bedienstete seine eigenen Daten eingetragen.

Auch wenn in diesem Fall die Beweggründe des Beamten in gewissem Maß aus menschlicher Sicht nachvollziehbar waren, handelte es sich hierbei um eine unbefugte Verarbeitung von personenbezogenen Daten. Die Verarbeitung von personenbezogenen Daten ist Bediensteten der Polizei grundsätzlich nur erlaubt, wenn die Datenverarbeitung für ihre Aufgabenerfüllung erforderlich ist, das heißt, wenn die konkrete Erfüllung der Aufgabe ohne die Verarbeitung nicht möglich wäre. Auch wenn der Bedienstete die Bilder im weiteren Sinne zur Nutzung für seine polizeiliche Arbeit aufnahm, war hier das Vorliegen eines konkreten dienstlichen Anlasses zu verneinen. Hinzu kommt, dass die Speicherung von polizeilichen Dokumenten, die in diesem Fall auch eine große Zahl an sensiblen Daten Dritter enthielten, auf dem privaten Handy erfolgte, was aus datenschutzrechtlichen Gründen klar unzulässig ist. Anders als bei Diensttelefonen der Polizei, die durch entsprechende technische Maßnahmen gesichert werden, besteht bei privaten Smartphones ein erhöhtes Risiko eines (möglicherweise auch unbemerkten) Zugriffs auf personenbezogene Daten, zum Beispiel durch bestimmte Applikationen oder Schadsoftware, wodurch Daten unbefugt in die Hände von Dritten gelangen können. Die Kontrolle über die Daten und ihre Verwendung ist der verantwortlichen Stelle entzogen.

Das Verfahren endete mit dem Erlass eines Bußgeldbescheides, wobei bei der Bemessung der Höhe der Geldbuße berücksichtigt wurde, dass der Bedienstete die Verarbeitung nicht aus einem ausschließlich privaten Motiv tätigte. Der Betroffene hatte zudem versichert, dass er die Daten nicht an Dritte weitergegeben und zwischenzeitlich alle Fotos gelöscht hatte.

Nutzung dienstlich erlangter Daten für private Kontaktaufnahme

Auch in diesem Fall wurde ich durch eine Polizeidienststelle über den Verdacht einer Datenschutzverletzung durch einen Polizeibediensteten informiert. Eine Bürgerin erstattete Anzeige wegen einer Straftat auf dem Polizeirevier des betreffenden Bediensteten, der die Anzeige aufnahm und die persönlichen Daten – darunter auch die Telefonnummer – der Anzeigenerstatterin erfasste. Im Anschluss an die Anzeigenaufnahme kündigte der Bedienstete an, dass zu einem späteren Zeitpunkt eine Zeugenvernehmung anberaumt würde und dass er sich noch einmal bei ihr telefonisch oder per Nachricht melden werde – die Bürgerin zeigte sich damit einverstanden. Am Abend des Tages, an dem die Bürgerin Anzeige erstattet hatte und in den folgenden Tagen erhielt sie von dem Polizeibediensteten Nachrichten über den Messenger-Dienst WhatsApp. Die Nachrichten standen jedoch in keinem dienstlichen Kontext, sondern waren eindeutig privater Natur. Die Bürgerin ging bis dato davon aus, dass der Bedienstete sie in einem dienstlichen Zusammenhang kontaktieren würde und fühlte sich von den Nachrichten des Bediensteten bedrängt. Im Nachhinein schilderte sie den Vorgang einem anderen Bediensteten, wodurch die Polizeidienststelle Kenntnis von dem Sachverhalt erlangte.

Aufgrund der eindeutig privat motivierten Verwendung der Telefonnummer der Bürgerin habe ich ein Ordnungswidrigkeitenverfahren wegen der unbefugten Verarbeitung von personenbezogenen Daten eingeleitet. Innerhalb des Verfahrens äußerte der Bedienstete, dass sich zwischen ihm und der Anzeigenerstatterin während der Anzeigenaufnahme eine lockere und entspannte Atmosphäre entwickelt habe und auch mehrfach private Themen zwischen beiden zur Sprache kamen. Bei dem Bediensteten sei dadurch der Eindruck entstanden, dass die Bürgerin ein privates Interesse an ihm hatte. Er habe die Signale falsch interpretiert und das Gespräch irrtümlicherweise als Flirt verstanden. Als er ankündigte, dass er sie noch einmal kontaktieren werde, habe er die Zustimmung der Bürgerin als Einverständnis

gewertet, sie auch in einem privaten Kontext kontaktieren zu dürfen. Dem Bediensteten musste allerdings angesichts seiner Tätigkeit als Polizist und regelmäßig wiederkehrender Belehrungen zu Themen des Datenschutzes bewusst gewesen sein, dass keine wirksame Einwilligung vorlag. § 2 Nr. 18 SächsDSUG definiert die Einwilligung als „jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung". Der Bedienstete machte in diesem Fall nicht erkennbar, dass er beabsichtigte, die Bürgerin mit seinem privaten Handy und in einem privaten Zusammenhang zu kontaktieren. Die Ankündigung, er werde sich noch einmal bei ihr melden, erfolgte innerhalb der dienstlichen Sphäre – im Anschluss an die Anzeigenaufnahme unter Verweis auf eine spätere Zeugenvernehmung und ohne Offenlegung eines privaten Interesses. Dabei ist irrelevant, dass beide Beteiligten während der Anzeigenaufnahme auch über private Themen sprachen. Auch eine subjektiv als locker und aufgeschlossen wahrgenommene Atmosphäre berechtigte den Beamten nicht zu der Annahme, dass die Bürgerin Kontakt wünschte oder in eine private Verwendung ihrer Telefonnummer eingewilligt habe. Für die Bürgerin war in keiner Weise erkennbar, dass der Bedienstete eine private Kontaktaufnahme beabsichtigte. Gegenüber dem Bediensteten wurde letztendlich ein Bußgeld wegen der unbefugten Nutzung der Telefonnummer erlassen, da weder ein dienstlicher Anlass noch eine wirksame Einwilligung der Bürgerin zur privaten Verwendung ihrer Nummer vorlag.

Polizeibedienstete tragen eine besondere Verantwortung hinsichtlich der ausschließlich dienstlichen Verwendung personenbezogener Daten, insbesondere in Fällen, in denen sich Bürger zur Anzeige von Straftaten an die Polizei wenden. Das Vertrauen der Bürger darauf, dass ihre Daten nicht für dienstfremde Zwecke verwendet werden, ist essenziell für das Vertrauen in die Polizei als Institution.

Was ist zu tun?

Die Bediensteten der Behörden und öffentlichen Stellen in Sachsen als nach außen agierende Vertreter des Freistaats sind auch künftig zu ihrer besonderen Pflichtenwahrung und Vorbildwirkung zu ermahnen. Der Ahndung von Ordnungswidrigkeiten im öffentlichen Bereich kommt nach wie vor besondere Bedeutung zu.

6.4.2 Ordnungswidrigkeitenverfahren im nichtöffentlichen Bereich

↗ Art. 58 Abs. 2 Buchst. b, Art. 83 DSGVO

Im Berichtszeitraum hatte ich 92 neue Ordnungswidrigkeitenanzeigen zu verzeichnen – die Anzahl bewegte sich damit deutlich über dem Niveau des Vorjahres (71). Wie bereits im vergangenen Jahr bezogen sich etwa zwei Drittel der Anzeigen (61) auf die Anfertigung von Videoaufnahmen (stationäre Kameras [41], Dashcams [20]). Damit liegt der Schwerpunkt (66 Prozent) der bei mir eingegangenen Ordnungswidrigkeitenanzeigen auch weiterhin klar bei der Videoüberwachung (Vorjahr gleichfalls 66 Prozent).
Insgesamt waren damit im Berichtszeitraum 162 Ordnungswidrigkeitenverfahren bei mir anhängig. Von diesen konnte ich 69 Fälle abschließen und habe dabei in acht Verfahren neun Bußgelder festgesetzt.

Tabelle 2:
Ordnungswidrigkeitenverfahren im nichtöffentlichen Bereich

Berichtszeitraum		**01.01.2023 – 31.12.2023**
anhängig gesamt		**162**
davon	Verfahren aus vorherigem Berichtszeitraum	70
	neu eingegangene Verfahren	92
abgeschlossen		**69**
davon	mit Bußgeld	8
	eingestellt/von Verfolgung abgesehen	61
noch in Bearbeitung		**93**
Summe festgesetzte Bußgelder in Euro		**5.000**

Sieben Bußgelder habe ich wegen eines rechtswidrigen Einsatzes von Dashcams festgesetzt; ihre Höhe bewegte sich zwischen 100 Euro und 1.000 Euro. In einem dieser Fälle konnte ich feststellen, dass im Tatzeitraum beide Ehepartner

das mit einer Dashcam ausgerüstete Fahrzeug genutzt hatten. Da diese Fahrzeugnutzungen den Ehepartnern jeweils klar zugeordnet werden konnten, habe ich auch gegen beide Personen jeweils ein Bußgeld festgesetzt.

Ein weiteres Bußgeld betraf den Betrieb einer stationären Videokamera im Innenhof eines Mehrfamilienhauses. Kamerabetreiber war hier ein Mieter, der die Videokamera an einem Fenster seiner Wohnung im Obergeschoss montiert und betrieben hatte. Da sich der – polizeibekannte – Betroffene wenig kooperativ gezeigt hatte, konnte ich die entsprechenden Beweismittel (Videoaufzeichnungen) nur auf der Grundlage eines Durchsuchungs- und Beschlagnahmebeschlusses sichern. Der Betroffene hatte die Videokamera in sein WLAN eingebunden und offensichtlich über sein Smartphone Zugriff auf die Livebilder der Kamera wie auch auf die auf einer Speicherkarte in der Videokamera abgelegten Videoaufzeichnungen.

Das verbleibende Bußgeld habe ich gegen einen ehemaligen Mitarbeiter eines Sicherheitsdienstes festgesetzt. Nachdem dieser seine Tätigkeit als Kaufhausdetektiv schon länger beendet hatte, waren im Rahmen einer anderweitig begründeten polizeilichen Maßnahme auf seinem privaten Smartphone immer noch Fotos der Personalausweise von Personen, die er in seiner früheren Tätigkeit des Ladendiebstahls überführt hatte, festgestellt worden.

Neben den oben genannten Bußgeldern habe ich in 10 Fällen noch datenschutzrechtliche Verwarnungen gegenüber nichtöffentlichen Verantwortlichen ausgesprochen (vgl. Art. 58 Abs. 2 Buchst. b DSGVO).

6.4.3 Erlass eines Strafbefehls wegen Dashcam-Einsatzes

↗ §§ 74 Abs. 1, 201 Abs. 1, 205 Abs. 1 StGB; Art. 6 Abs. 1 Buchst. f DSGVO

Über die rechtlichen Beschränkungen und Risiken des Dashcam-Einsatzes habe ich in meinen Tätigkeitsberichten immer wieder berichtet, zuletzt im Tätigkeitsbericht 2020 (2.2.30, Seite 86 ff.) Dabei habe ich auch die besondere Problema-

Tätigkeitsbericht 2020:
↗ sdb.de/tb2020

tik aktivierter Audioaufnahmen – fast alle Kameratypen verfügen über ein integriertes Mikrofon – thematisiert und festgestellt, dass auch für eine gegebenenfalls erfolgende Audioaufzeichnung der geführten Gespräche keine Rechtsgrundlage ersichtlich ist. In Bezug auf den regelmäßig verfolgten Zweck der Beweissicherung bei Verkehrsunfällen fehlt es schon an der Erforderlichkeit für die Aufzeichnung von im, aus oder neben dem Fahrzeug geführten Gesprächen. Art. 6 Abs. 1 Buchst. f Datenschutz-Grundverordnung (DSGVO) scheidet also als Rechtsgrundlage aus. Der Bundesgerichtshof (Urteil vom 15.05.18, VI ZR 233/17, juris) hat diesbezüglich klar zum Ausdruck gebracht, dass das Grundgesetz davor schützt, dass Gespräche heimlich aufgenommen werden und heimliche Tonaufnahmen nicht öffentlich geführter Gespräche noch wesentlich stärker in das Persönlichkeitsrecht der betroffenen Personen eingreifen als schon heimliche Bildaufnahmen der sich in der Öffentlichkeit bewegenden Verkehrsteilnehmer. Das Recht am gesprochenen Wort gewährleistet die Selbstbestimmung über die eigene Darstellung der Person in der Kommunikation mit anderen. Dieses Selbstbestimmungsrecht findet einen Ausdruck in der Befugnis des Menschen, selbst und allein zu entscheiden, ob sein Wort auf einen Tonträger aufgenommen und damit möglicherweise Dritten zugänglich werden soll, womit Wort und Stimme der Kommunikationsteilnehmer/innen losgelöst und in einer für Dritte verfügbaren Gestalt verselbstständigt werden. Nach § 201 Abs. 1 Nr. 1 Strafgesetzbuch (StGB) ist damit sogar ein Straftatbestand erfüllt; meist fehlt es insoweit – mangels Kenntnis der betroffenen Personen – lediglich an diesbezüglichen Strafanträgen, da Verstöße gegen § 201 Abs. 1 StGB nur auf Antrag verfolgt werden (§ 205 Abs. 1 StGB).

Weitere Informationen zur datenschutzkonformen Nutzung von Dashcams:
↗ sdb.de/achkam

Dass die Strafdrohung in der Praxis Anwendung findet, zeigt ein mir von der Polizei im Berichtszeitraum übergebenes Ordnungswidrigkeitenverfahren eines Dashcam-Einsatzes. Der Betroffene hatte in diesem Fall nicht nur rechtswidrig eine Dashcam zur Überwachung des öffentlichen Verkehrsraums betrieben, sondern darüber hinaus auch das integrier-

te Mikrofon aktiviert und mittels diesem dann das mit den Polizeibeamten während einer Verkehrskontrolle geführte Gespräch aufgezeichnet. Infolge der geöffneten Fahrertür waren durch das Mikrofon der im Fahrzeuginneren befindlichen Dashcam auch die außerhalb des Fahrzeugs geführten Gespräche aufgezeichnet worden. Der betroffene Polizeibeamte hatte dies zum Anlass genommen, gegen den Betroffenen einen Strafantrag zu stellen. Die Staatsanwaltschaft hat daraufhin den Betroffenen beschuldigt, unbefugt das nichtöffentlich gesprochene Wort eines anderen auf einen Tonträger aufgezeichnet zu haben, und beim zuständigen Amtsgericht einen Strafbefehl wegen Verstoßes gegen § 201 Abs. 1 Nr. 1 StGB (Verletzung der Vertraulichkeit des Wortes) beantragt. Das Amtsgericht hat diesen Strafbefehl antragsgemäß erlassen, dabei eine Geldstrafe in Höhe von 25 Tagessätzen verhängt und zugleich nach § 74 Abs. 1 StGB auch die Einziehung der sichergestellten Dashcam einschließlich der Speicherkarte angeordnet. Der Betroffene hat kein Rechtsmittel eingelegt.

Was ist zu tun?
Die Aktivierung der Mikrofonfunktion einer Dashcam ist grundsätzlich unzulässig, sobald sich außer dem Fahrzeugführer weitere Personen im Fahrzeug befinden oder sonst die Möglichkeit besteht, dass im oder aus dem Fahrzeug heraus geführte Gespräche (zum Beispiel Telefonate) aufgezeichnet werden.

6.4.4 Verfolgungsverjährung bei Videoüberwachung

↗ § 31 OWiG

Die Verfolgungsverjährung ist das wohl praktisch wichtigste rechtliche Hindernis für die Durchführung eines Ordnungswidrigkeitenverfahrens. Ist Verjährung eingetreten, ist die Verfolgung einer Ordnungswidrigkeit gesetzlich ausgeschlossen, § 31 Abs. 1 Ordnungswidrigkeitengesetz (OWiG). Für datenschutzrechtliche Bußgeldtatbestände beträgt die Verjährungsfrist drei Jahre, § 31 Abs. 2 Nr. 1 OWiG. Nach § 31 Abs. 3 OWiG beginnt die Verjährung allerdings erst zu laufen, wenn die Handlung beendet ist.
Für Ordnungswidrigkeiten aus dem Bereich der Videoüberwachung bedeutet dies nun Folgendes:
Handelte es sich um bloßes Monitoring, kann eine rechtswidrige Videoüberwachung nach drei Jahren nicht mehr verfolgt werden. Zugegebenermaßen dürften solche Fälle prak-

tisch aber kaum auftreten, da solcherart Verstöße kaum noch rechtssicher nachgewiesen werden können dürften. Jedenfalls ist dies dann aber kein Verjährungsproblem mehr.
Anders liegt der Sachverhalt, wenn auch aufgezeichnet worden ist. In diesem Fall ist es praktisch ohne Bedeutung, welchen Ursprungsdatums die Videoaufzeichnungen sind. Da der datenschutzrechtliche Verstoß nicht nur in der Videoüberwachung als (momentane) Beobachtung als solcher, sondern auch in der Aufzeichnung liegt, ist die Tathandlung so lange nicht beendet, wie die Aufzeichnungen noch vorhanden sind – Tatbestand ist die rechtswidrige Speicherung. Dies bedeutet, dass auch unrechtmäßige Videoaufzeichnungen, die bereits älter als drei Jahre sind, als Ordnungswidrigkeit verfolgt werden können. Es ist auch nicht erforderlich, dass die Videoaufzeichnungen bis in den Dreijahreszeitraum hineinreichen – allerdings müssen sie noch innerhalb dieses Zeitraums vorhanden gewesen sein. Damit können auch Videoaufzeichnungen, die beispielsweise vor fünf Jahren über einen Zeitraum von beispielsweise einen Monat angefertigt worden sind, als Datenschutzverstoß geahndet werden. Auch hier setzt die praktische Frage der Nachweisbarkeit dann aber wieder (andere) Grenzen. Aus Beweisgründen werden wohl nur Verstöße geahndet werden, bei denen die Aufzeichnungen zum Ahndungszeitpunkt noch vorhanden sind.

Was ist zu beachten?
Solange Aufzeichnungen aus unrechtmäßigen Videoüberwachungen noch nachweisbar sind, können diese auch als Ordnungswidrigkeit verfolgt werden; das Entstehungsdatum ist insoweit nicht entscheidend, eine Verjährung tritt während des Speicherzeitraums nicht ein.

6.4.5 Videoüberwachung unter Nachbarn – Praxis der Behandlung von Ordnungswidrigkeitenanzeigen

↗ § 47 Abs. 1 OWiG; §§ 823, 1004 BGB; Art. 2 Abs. 1 DSGVO

Die Videoüberwachung ist seit Jahren ein Arbeitsschwerpunkt meiner Aufsichtstätigkeit im nichtöffentlichen Sektor. Dies gilt auch für den Ordnungswidrigkeitenbereich, wobei die mir dort von der Polizei übergebenen Verfahren fast ausschließlich Streitigkeiten unter Nachbarinnen und Nachbarn, mitunter sogar unter Familienmitgliedern betreffen. Anzeigende beklagen regelmäßig einen von Videokameras auf dem Nachbargrundstück oder in der Nachbarwohnung

ausgehenden Überwachungsdruck, weil die Kameras entweder nicht erkennen lassen, welche Bereiche sie erfassen (Domkameras) oder aber so ausgerichtet sind, dass sie eine Erfassung auch des eigenen Grundstücks oder des Zugangs zur eigenen Wohnung zumindest vermuten lassen. Eher selten sucht man in diesem Zusammenhang das Gespräch mit den Nachbarn – meist ist das Verhältnis wegen langjähriger anderweitiger Streitigkeiten so zerrüttet, dass schon lange nicht mehr miteinander gesprochen wird. Als Lösung bleibt dann vermeintlich nur eine, gegebenenfalls auch wiederholte Anzeige bei der Polizei. Diese nimmt die Vermutungen des Anzeigenden im Rahmen einer Zeugenvernehmung auf und fertigt bestenfalls noch eine Fotodokumentation der Lage vor Ort an. Nur in Ausnahmefällen befragt sie bereits die betreffenden Nachbarinnen oder Nachbarn.

Für mich stellt sich dann regelmäßig das Problem der Nachweisbarkeit einer Videoüberwachung über das eigene Grundstück oder die eigene Wohnung hinaus. Allein das Vorhandensein und die Ausrichtung einer Kamera reichen als Beweis im Ordnungswidrigkeitenverfahren nicht aus. Schließlich kann es sich auch nur um Attrappen – auch diese können übrigens blinken – oder um inaktive Kameras handeln. In diesen Fällen kann schon deshalb kein Datenschutzverstoß vorliegen, weil keine Verarbeitung personenbezogener Daten erfolgt und die Datenschutz-Grundverordnung (DSGVO) damit nicht anwendbar ist, Art. 2 Abs. 1 DSGVO. Davon abgesehen kann auch der Erfassungsbereich aktiver Kameras beispielsweise durch Schwärzungen bereits in der Kamera beschränkt werden. All dies führt dazu, dass tatsächlich rechtskonform nur das eigene Grundstück oder eben überhaupt nichts überwacht und lediglich auf den Abschreckungseffekt gesetzt wird. Von alledem hat der/die betroffene Nachbar/in aber natürlich keine Kenntnis und soll es gegebenenfalls auch gar nicht erfahren. Er/Sie sieht nur die vermeintlich auf ihn/sie gerichteten Kameras und will dagegen vorgehen.

Als Ordnungswidrigkeitenbehörde verbleibt mir zunächst allein das Mittel der Anhörung des/der Kamerabetreibenden. Doch diese/r muss sich weder selbst belasten noch über-

haupt zum Sachverhalt äußern. Mit einer Anhörung ist also nicht allzu viel gewonnen. Keinesfalls ist zu erwarten, dass man auf diese Weise zu Beweismitteln (Geständnis, Videoaufzeichnungen) gelangt, auf deren Grundlage dann ein Bußgeld festgesetzt werden könnte. Darüberhinausgehende Ermittlungsmaßnahmen – hier Durchsuchungen zur Gewinnung von Beweismitteln (Beschlagnahme von Datenträgern mit Videoaufzeichnungen) – sind zwar prinzipiell vorstellbar, stellen sich in reinen Nachbarschaftsfällen aber regelmäßig als unverhältnismäßig dar.

Schließlich ist auch noch das öffentliche Verfolgungsinteresse in Betracht zu nehmen. Soweit die betreffenden Kameras nicht auch den Verdacht nähren, dass auch angrenzende öffentliche Verkehrsbereiche mitüberwacht werden, es sich mithin allein um eine Streitigkeit unter zwei Nachbarinnen/Nachbarn handelt, die Allgemeinheit also kein nennenswertes Interesse an der Aufklärung dieser privatrechtlichen Angelegenheit hat, stehen weitergehende Ermittlungsmaßnahmen in keinem akzeptablen Verhältnis zu einem auch der Allgemeinheit dienenden Ergebnis.

In der überwiegenden Zahl der Fälle sehe ich daher von der Einleitung eines Ordnungswidrigkeitenverfahrens ab bzw. stelle dies entsprechend ein (§ 47 Abs. 1 Ordnungswidrigkeitengesetz).

Dabei ist auch noch Folgendes zu berücksichtigen. Mit einem Bußgeld würde nur das Verhalten des Betroffenen in der Vergangenheit geahndet. Eine Beendigung der rechtswidrigen Handlung ist damit nicht zwingend verbunden, auch wenn in einem solchen Fall natürlich die Möglichkeit einer erneuten Ordnungswidrigkeitenanzeige besteht. Selbst wenn sich der Betroffene einsichtig zeigt und den Betrieb der Videokameras einstellt, bedeutet das keinesfalls, dass die Kameras auch entfernt werden. Der Betroffene kann auch schlichtweg nur deren Erfassungsbereiche korrigieren. In diesen Fällen bleiben die Kameras also – zulässigerweise – an ihrem ursprünglichen Ort montiert, und damit bleibt es auch beim Überwachungsdruck für die Nachbarinnen und Nachbarn, denen damit im Ergebnis alles andere als geholfen ist.

Tätigkeitsbericht 2021:
↗ sdb.de/tb2021

Was ist zu tun?
Videoüberwachungskameras an Grundstückgrenzen sollten so ausgerichtet werden, dass gar nicht erst der Eindruck entsteht, das Nachbargrundstück würde miterfasst. Diesbezügliche Streitigkeiten unter Nachbarinnen und Nachbarn sollten auf dem Zivilrechtsweg geklärt werden; Ordnungswidrigkeitenverfahren sind an dieser Stelle wenig zielführend.

Ich empfehle den Anzeigenden daher regelmäßig, ihre Ansprüche zivilrechtlich durchzusetzen (vgl. auch Tätigkeitsbericht 2021, 6.1.4., Seite 148 ff.) Dem sich schon allein aus der Existenz einer Videokamera ergebenden Überwachungs- und Anpassungsdruck kann einzig auf dem Zivilrechtsweg wirksam begegnet werden. Kameraattrappen werden durch die Rechtsprechung kaum anders bewertet als funktionstüchtige, tatsächlich aufzeichnende Kameras. Den Betroffenen sind insoweit nach den §§ 823, 1004 Bürgerliches Gesetzbuch je nach konkreter Sachlage Entschädigungs-, Beseitigungs- oder Unterlassungsansprüche zuerkannt worden.

6.5 Öffentlichkeitsarbeit

6.5.1 Onlinekommunikation und Publikationen

Neue Website und E-Mail-Adressen

Abbildung 6:
Startseite des neuen Internetauftritts

Was ist zu tun?
Wer noch die bisherigen Kontaktangaben meiner Behörde, beispielsweise in einer Datenschutzerklärung auf einer Website veröffentlicht hat, sollte die Daten zeitnah aktualisieren.

Im Tätigkeitsbericht 2022 hatte ich auf die umfangreiche Neugestaltung meines Internetauftritts bereits hingewiesen. Seit Mai 2023 ist die Website unter www.datenschutz.sachsen.de nun online. Sie wurde inhaltlich, optisch sowie technisch überarbeitet. Jede Zielgruppe – ob Bürgerinnen und Bürger, Wirtschaft oder Verwaltung – findet dort ein auf sie zugeschnittenes Informationsangebot. Es enthält Ausführungen zu den rechtlichen Grundlagen sowie themenspezifische Inhalte, beispielsweise zum Datenschutz in der Schule, im Homeoffice, bei Videokonferenzsystemen und in vielen weiteren Bereichen.
Die Überarbeitung der Website diente auch dazu, um die Darstellung meiner Website auf mobilen Endgeräten zu verbessern und Inhalte barrierefrei präsentieren zu können. Zudem unterstützen eigens entwickelte Icons und Grafiken bei der Orientierung sowie Navigation.
Außer der Website haben sich auch die E-Mail-Adressen geändert. Statt @slt.sachsen.de heißt es nun @sdtb.sachsen.de. Das zentrale E-Mail-Postfach erreichen Sie unter post@sdtb.sachsen.de.

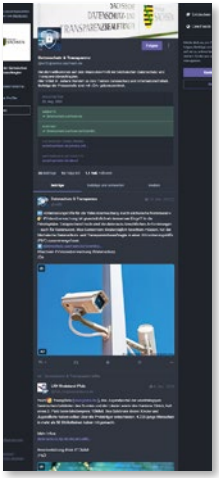


Abbildung 7:
Profil der SDTB auf Mastodon

Mastodon-Instanz für öffentliche Stellen

Im November 2022 bin ich mit meiner Behörde auf Mastodon, dem datenschutzfreundlichen Kurznachrichtendienst, gestartet. Dort informiere ich mit meiner Behörde über aktuelle Themen rund um den Datenschutz und die Transparenz bzw. Informationsfreiheit. Dafür hatte ich anfänglich die Instanz des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) genutzt. Seit September 2023 betreibt meine Behörde nunmehr einen eigenen Mastodon-Server unter social.sachsen.de. Ich freue mich, dass ich darüber auch öffentlichen Stellen aus Sachsen ein datenschutzkonformes soziales Netzwerk für ihre Öffentlichkeitsarbeit zur Verfügung stellen kann. Mastodon hatte 2023 nochmals an Popularität zugelegt. Der Kurznachrichtendienst gilt inzwischen nicht mehr nur bei IT-Expertinnen und Experten als datensparsame und nicht-kommerzielle Alternative zu Facebook und X, ehemals Twitter. Mit der Einrichtung einer eigenen Instanz auf social.sachsen.de möchte ich diese positive Entwicklung unterstützen. Öffentliche Stellen, die an einem Account auf social.sachsen.de interessiert sind, können sich gern an meine Dienststelle wenden: socialmedia@sdtb.sachsen.de

Inzwischen folgen mir unter social.sachsen.de/@sdtb etwa 1.100 Nutzerinnen und Nutzer, worüber ich mich sehr freue. Natürlich tummeln sich im Verhältnis immer noch deutlich weniger Menschen auf Mastodon als bei den kommerziellen Anbietern. Nichtsdestotrotz sehe ich öffentliche Stellen in der Pflicht, mit Bürgerinnen und Bürgern ausschließlich rechtskonform zu kommunizieren. Mastodon bietet diese Möglichkeit. Darüber hinaus kann der „News-Feed" eines (Behörden-) Profils beispielsweise auf der jeweiligen (Behörden-)Website eingebunden werden, was wiederum die Reichweite des Profils erhöht. 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.

Wer sich einen Mastodon-Account einrichten und darüber kommunizieren möchte, findet beispielsweise auf https://joinmastodon.org/servers eine Liste mit verfügbaren Instanzen. Für die Nutzung von Mastodon auf Mobilgeräten stehen in den App-Stores zahlreiche kostenfreie und oftmals quelloffene Applikationen zum Download bereit.

Aktuelle Broschüren

Abbildung 8:
2023 aktualisierte Broschüren

Für die Informationsvermittlung greife ich nicht nur auf die Möglichkeiten der Onlinekommunikation zurück, sondern nutze ebenso gedruckte Publikationen. Insbesondere für Präsenzveranstaltungen eignen sich Broschüren, um die Zielgruppen für die Themen meiner Behörde zu sensibilisieren. Wie üblich sind solche Veröffentlichungen gelegentlich zu aktualisieren. Das betraf im Berichtszeitraum – aufgrund der neuen Funktion als Sächsische Transparenzbeauftragte – zwei Publikationen: „Datenschutz und Transparenz für Sachsen – Aufgaben, Befugnisse und Rechtsstellung der Sächsischen Datenschutz- und Transparenzbeauftragten" und „Das Transparenzgesetz – Ihr Recht auf Informationszugang". Beide Broschüren sind auch in der Publikationsdatenbank des Freistaates Sachsen in der aktualisierten Fassung als PDF-Datei erhältlich: www.publikationen.sachsen.de

6.5.2 Presse- und Medienarbeit

Im Berichtszeitraum wendeten sich Journalistinnen und Journalisten etwas häufiger als in den Vorjahren an meine Behörde. Vor allem Datenschutzthemen waren von Interesse, nur verhältnismäßig wenige Anfragen betrafen mein Amt als Transparenzbeauftragte. Für Aufsehen sorgte vor allem – wie schon 2022 – das Facebook-Verfahren gegen die Sächsische Staatskanzlei. Über kein anderes Datenschutzthema in meinem Zuständigkeitsbereich berichteten Medien so umfangreich wie über die Untersagung des Fanpage-Betriebs. Bei all dem Wirbel um Facebook soll die beträchtliche Bandbreite an anderen Sachverhalten nicht unerwähnt bleiben – vor allem die zahlreichen Anfragen im Zusammenhang mit Videoüberwachung

durch Kommunen, Privatleute, die Polizei oder Fahrzeughersteller. Außerdem erkundigten sich Medienvertreter/innen bei mir unter anderem zu ChatGPT, Künstlicher Intelligenz im Sport, der Datenschutzkonformität von sozialen Medien und Apps, zur Löschung von Kundendaten im Handel sowie zum Fotografieren von Falschparkern oder zum Gemeinsamen Kompetenz- und Dienstleistungszentrum der Polizeien der Länder Berlin, Brandenburg, Sachsen, Sachsen-Anhalt und Thüringen (GKDZ) sowie zu vielen weiteren Themen.

6.5.3 Fortbildungen, Infoveranstaltungen und fachlicher Austausch

Sowohl die betroffenen Personen als auch die Verantwortlichen sind dazu aufgefordert, achtsam mit personenbezogenen Daten umzugehen – entweder mit ihren eigenen oder mit den ihnen anvertrauten. Deshalb wende ich mich in meiner Öffentlichkeitsarbeit an beide Zielgruppen. Hierbei zeigt sich: Veranstaltungen sind oftmals die wirkungsvollsten Kommunikationsinstrumente, wenn es darum geht, Erwachsene, Jugendliche und Kinder für Datenschutz zu sensibilisieren.

Abbildung 9:
SDTB vor Ort bei „Digital? Aber sicher"

Mit Hackern auf Tour

Aus diesem Grund habe ich im Herbst 2023 auch die Neuauflage der Veranstaltungsreihe „Digital? Aber sicher" unterstützt. An der Roadshow zur Cybersicherheit, die von der Sächsischen Staatskanzlei initiiert wurde, waren neben meiner Behörde unter anderem die sächsischen Volkshochschulen, die Verbraucherzentrale Sachsen und das Bundesamt für Sicherheit in der Informationstechnik (BSI) beteiligt.
Nach dem Auftakt am 16. Oktober in Dresden machte „Digital? Aber sicher!" bis 17. November Halt in zwölf sächsischen Städten. Jede Veranstaltung dauerte etwa eineinhalb bis zwei Stunden. Vor den Abendveranstaltungen für Bürgerinnen und Bürger wurden auch zielgruppenspezifische Live-Hackings und Vorträge zur Cybersicherheit für Schülerinnen und Schüler, Lehrkräfte, Auszubildende und Verwaltungsmitarbeitende vormittags und nachmittags angeboten. Meine Behörde war insgesamt in acht Orten mit einem Kurzvortrag zum digitalen Datenschutz und/oder einem Infostand vertreten.

Weitere Veranstaltungen für Bürgerinnen und Bürger

2023 nahm ich wieder am „Tag der offenen Tür des Sächsischen Landtags" teil. Am Stand meiner Behörde stellten die Bürgerinnen und Bürger nicht nur Fragen zum Datenschutz, sondern ebenso zum Sächsischen Transparenzgesetz. Beide Themenschwerpunkte behandelte auch der E-Learning-Kurs „Wer sieht mich?", der unter anderem von der Sächsischen Landeszentrale für politische Bildung organisiert wurde. Dabei drehte sich alles um den Umgang mit personenbezogenen Daten und den Zugang zu amtlichen Informationen. Im Rahmen des mehrteiligen Seminars hielt ich einen Vortrag zum Transparenzgesetz und beantwortete die Fragen aus der Teilnehmerrunde. Wie schon im vergangenen Datenschutz-Tätigkeitsbericht angedeutet, nahm mein Amt als Sächsische Transparenzbeauftragte 2023 einen beachtlichen Teil meiner Zeit in Anspruch, vielfach im Zusammenhang mit der Öffentlichkeitsarbeit, wozu auch Vorträge wie beim Dies academicus an der Universität Leipzig gehörten.

Abbildung 10:
Impressionen von „Digital? Aber sicher!“ in Dresden, Görlitz und Leipzig

Deutlich mehr Schulungen

Im aktuellen Berichtszeitraum waren Mitarbeiterinnen und Mitarbeiter meiner Dienststelle im Sinne der Prävention, trotz des stetig gestiegenen Arbeitsaufkommens, vielfältig im Bereich der Beratung bzw. Aus- und Fortbildung unterwegs. Sie hielten 36 Fortbildungsseminare und somit fast doppelt so viele wie 2022 (ca. 20). Analog zu den Vorjahren lehrten die Bediensteten an staatlichen Aus- und Fortbildungseinrichtungen wie der Hochschule Meißen und dem zugehörigen Fortbildungszentrum, dem Landesamt für Schule und Bildung, aber auch bei der Verwaltungs- und Wirtschaftsakademie Dresden. Inhaltlich handelte es sich um verschiedene Fragen

zum allgemeinen Datenschutzrecht, Datenschutz in Schulen und der Kommunalverwaltung, zur Datensicherheit im Netz oder zum Beschäftigtendatenschutz. Die Veranstaltungen fanden oftmals im Hybridformat statt, also in Präsenz- und Online-Form.

Zusammenarbeit mit Behörden und Multiplikatoren

Regelmäßig in Kontakt zu treten mit den unterschiedlichsten Behörden, Vereinigungen, Parteien, Gremien und Multiplikatoren gehört zu meinen wichtigsten Aufgaben. Am häufigsten werde ich von Mitgliedern des Landtages konsultiert. An den Sitzungen des Innenausschusses nehme ich regelmäßig teil. Auch im Plenum habe ich einen festen Platz.

Als (beratendes) Mitglied des IT-Kooperationsrates, des Statistischen Beirates und des Landespräventionsrates habe ich im Berichtszeitraum mehrere Sitzungen wahrgenommen. In der Landesrektorenkonferenz habe ich mich ebenso vorgestellt wie im GKDZ. Gerne nehme ich auch Einladungen zu Festveranstaltungen an – so war etwa die Veranstaltung zu 30 Jahren Verfassungsgerichtshof in Sachsen ein würdiger Festakt. Auch der Europäische Datenschutztag, der KI-Kongress oder die Führungskräftekonferenz der Staatskanzlei waren mir wichtige Veranstaltungen zur Vernetzung und Werbung für den Datenschutz. Oft werde ich am Rande solcher Veranstaltungen zu datenschutzrechtlichen Fragen angesprochen. Manche Sache erledigt sich schnell, aus mancher Frage entsteht aber auch ein aufsichtlicher Vorgang.

7 Zusammenarbeit der Datenschutzaufsichtsbehörden, Datenschutzkonferenz

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (kurz: Datenschutzkonferenz oder DSK) ist national wie auch international ein anerkanntes Experten- und Aufsichtsgremium. Zu den Aufgaben der DSK gehört, die Datenschutzgrundrechte zu wahren und zu schützen, eine einheitliche Anwendung des europäischen und nationalen Datenschutzrechts zu erreichen und gemeinsam für seine Fortentwicklung einzutreten. Die Führung der DSK wechselt jährlich. Im Berichtszeitraum hatte das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein den Vorsitz inne.

Abbildung 11:
106. Konferenz der DSK am 21. und 22. November 2023 in Lübeck

Über die Jahre hat sich die Zusammenarbeit innerhalb der DSK intensiviert. Seit 2021 treffen sich die Datenschutzbeauftragten der Länder und des Bundes wöchentlich in einer Videokonferenz und stimmen sich zu aktuellen Themen ab. Die regelmäßigen Besprechungen dienen vor allem der Kohärenz der Auffassungen der Datenschutzaufsichtsbehörden, auch um mit einer Stimme im Europäischen Datenschutzausschuss zu sprechen. Beschlüsse werden in diesen Kurzbesprechungen jedoch nicht gefasst. Dafür stehen vor allem die beiden Hauptkonferenzen zur Verfügung. Gelegenheit zum Austausch boten im Berichtszeitraum zudem drei Zwischen- und zwei Vorkonferenzen sowie die Kooperationen in den verschiedenen Arbeitskreisen. In diesem Zusammenhang sei erwähnt, dass meine Behörde zum Jahresanfang 2023 – gemeinsam mit der Berliner Beauftragten für Datenschutz und Informationsfreiheit – den Vorsitz des Arbeitskreises „Gesundheit und Soziales" übernommen hat. Mit meiner Behörde bereite ich die Tagungen für 2025 vor, die in Sachsen stattfinden werden.

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

Weiterentwicklung der Datenschutzkonferenz

Gemeinsam mit den Datenschutzbeauftragten der anderen Aufsichtsbehörden engagierte ich mich 2023 auch im Arbeitskreis „DSK 2.0". Dort begannen die Planungen zur Gründung einer DSK-Geschäftsstelle, unter anderem zu den Aufgaben und den erforderlichen rechtlichen Regelungen. Der weitere Fortgang hängt maßgeblich davon ab, ob die Einrichtung der Geschäftsstelle in das aktuelle Gesetzgebungsverfahren zum Bundesdatenschutzgesetz aufgenommen wird.
Weiterhin nahm im Jahr 2023 das Präsidium der DSK seine Arbeit auf. Dabei handelt es sich um ein Pilotprojekt. Das Präsidium setzt sich zusammen aus dem vorherigen, aktuellen und kommenden Vorsitz der Datenschutzkonferenz sowie den beiden Vertretern im Europäischen Datenschutzausschuss (EDSA). Das Präsidium hat die Aufgabe, den DSK-Vorsitz in operativen und strategischen Fragen zu unterstützen. Gerade vor dem Hintergrund des jährlichen Vorsitzwechsels soll durch das Präsidium Kontinuität gewährleistet werden. Die Beteiligung der Vertreter der deutschen Datenschutzaufsichtsbehör-

den im EDSA soll zudem die Schnittstelle und den Anschluss zu diesem Gremium optimieren.

7.1 Materialien der Datenschutzkonferenz – Entschließungen

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

- Datenschutz in der Forschung durch einheitliche Maßstäbe stärken (23.11.2023)
- Rahmenbedingungen und Empfehlungen für die gesetzliche Regulierung medizinischer Register (22.11.2023)
- Geplante Chatkontrolle führt zu einer unverhältnismäßigen, anlasslosen Massenüberwachung! (17.10.2023)
- Verfassungsrechtliche Anforderungen bei automatisierter Datenanalyse durch Polizei und Nachrichtendienste beachten! (11.05.2023)
- Notwendigkeit spezifischer Regelungen zum Beschäftigtendatenschutz! (11.05.2023)

7.2 Materialien der Datenschutzkonferenz – Beschlüsse

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

- Positionspapier zu cloudbasierten digitalen Gesundheitsanwendungen (06.11.2023)
- Positionspapier zur audiovisuellen Umgebungserfassung im Rahmen von Entwicklungsfahrten (27.09.2023)
- Bewertung von Pur-Abo-Modellen auf Websites (29.03.2023)

- Zur datenschutzrechtlichen Bewertung von Zugriffsmöglichkeiten öffentlicher Stellen von Drittländern auf personenbezogene Daten (03.02.2023)

7.3 Materialien der Datenschutzkonferenz – Orientierungshilfen

Anwendungshinweise sollen beim praktischen Vollzug der Datenschutz-Grundverordnung unterstützen.

- Kernelemente der Überwachungsaufgaben von Überwachungsstellen für Verhaltensregeln nach Art. 40 DSGVO
- Übermittlung personenbezogener Daten aus Europa an die USA – Anwendungshinweise zum Angemessenheitsbeschluss der Europäischen Kommission zum Datenschutzrahmen EU-USA (EU-US Data Privacy Framework) vom 10. Juli 2023

7.4 Materialien der Datenschutzkonferenz – Stellungnahmen

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

- Stellungnahme (II) zum Entwurf eines Ersten Gesetzes zur Änderung des Bundesdatenschutzgesetzes mit Stand 09.08.2023 (06.09.2023)
- Stellungnahme (I) zum Entwurf eines Ersten Gesetzes zur Änderung des Bundesdatenschutzgesetzes mit Stand 09.08.2023 (06.09.2023)
- Stellungnahme zum Entwurf der Europäischen Kommission: VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES zur Festlegung zusätzlicher Verfahrensregeln für die Durchsetzung der Verordnung (EU) 2016/679 COM(2023) 348 final) (01.09.2023)

- Stellungnahme zum Referentenentwurf des Bundesministeriums für Gesundheit: Entwurf eines Gesetzes zur verbesserten Nutzung von Gesundheitsdaten (14.08.2023)
- Stellungnahme zu Artikel 5 des Referentenentwurfs eines Gesetzes zur verbesserten Nutzung von Gesundheitsdaten (10.08.2023)
- Stellungnahme zum Referentenentwurf des BMDV zur Rechtsverordnung nach § 26 Abs. 2 TTDSG (11.07.2023)
- Stellungnahme zum politischen Targeting (21.06.2023)
- Stellungnahme zur Verbesserung bei Scoringverfahren (11.05.2023)
- Stellungnahme: Daten der Verbraucherinnen und Verbraucher beim Einsatz von Smart Meter zur Erfassung des Kaltwasserverbrauchs durch einheitliche Regelungen schützen (11.05.2023)
- Stellungnahme zum Europäischen Gesundheitsdatenraum bei der Nutzung von Gesundheitsdaten (27.03.2023)
- Stellungnahme zu Grundsatzfragen zur Sanktionierung von Datenschutzverstößen von Unternehmen – EuGH-Rechtssache C-807/21 (18.01.2023)

7.5 Materialien der Datenschutzkonferenz – weitere Dokumente

Die Datenschutzkonferenz veröffentlichte im Jahr 2023 auch folgende Dokumente.

- Gutachten: Rechtliche Möglichkeiten zur Stärkung und Institutionalisierung der Kooperation der Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK 2.0) (15.05.2023)
- Positionspapier zu Kriterien für Souveräne Clouds (11.05.2023)

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

Der Europäische Datenschutzausschuss (EDSA) verabschiedete die nachstehend aufgeführten Dokumente. Dabei handelt es sich um Aktualisierungen früherer Publikationen.

- Empfehlungen 1/2022 zur Beantragung der Genehmigung sowie über die Bestandteile und Grundsätze, die in Verbindlichen internen Datenschutzvorschriften (Art. 47 DSGVO) (20.06.2023) enthalten sind (20.06.2023) – nur in Englisch
- Leitlinien 04/2022 zur Bemessung von Geldbußen nach der DSGVO (24.05.2023) – nur in Englisch
- Leitlinien 03/2021 zur Anwendung von Artikel 65 Abs. 1 Buchst. a DSGVO (24.05.2023) – nur in Englisch
- Leitlinien 05/2022 zur Anwendung von Gesichtserkennungstechnologien im Bereich der Strafverfolgung (17.05.2023) – nur in Englisch
- Leitlinien 8/2022 für die Bestimmung der federführenden Aufsichtsbehörde eines Verantwortlichen oder Auftragsverarbeiters (17.04.2023)
- Leitlinien 01/2022 zu den Rechten betroffener Personen – Auskunftsrecht der betroffenen Person (17.04.2023) – nur in Englisch
- Leitlinien 9/2022 zur Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person nach der DSGVO (04.04.2023) – nur in Englisch
- Leitlinien 7/2022 über die Zertifizierung als Instrument für Übermittlungen (24.02.2023)
- Leitlinien 5/2021 über das Zusammenspiel zwischen der Anwendung des Artikels 3 und der Bestimmungen über internationale Übermittlungen nach Kapitel V DSGVO (24.02.2023)

- Leitlinien 3/2022 zu irreführenden Designmustern in Schnittstellen von Social-Media-Plattformen: wie man sie erkennt und vermeidet (24.02.2023) – nur in Englisch

7.7 Technische Leitlinie zur ePrivacy-Richtlinie

↗ TTDSG, DSGVO

Tätigkeitsbericht Datenschutz 2022:
↗ sdb.de/tb2022

Bereits im letzten Tätigkeitsbericht (2.1.3, Seite 36 f.) habe ich von der Arbeit an der Interpretation der ePrivacy-Richtlinie (ePD) berichtet. Diese Arbeit wurde 2023 fortgeführt und nach vielen Iterationen unter Beteiligung aller nationalen Datenschutzaufsichtsbehörden zu einem ersten Ergebnis gebracht, welches zum Jahresende der öffentlichen Konsultation vorgelegt wurde. Nach der Konsultation werden die vorgebrachten Vorschläge und Korrekturen eingebracht und voraussichtlich wird das finale Dokument im Jahr 2024 veröffentlicht werden.

Wie bereits berichtet, befasste sich in diesem Fall die Arbeitsgruppe „Expert Subgroup Technology" des Europäischen Datenschutzausschusses (EDSA) mit der Interpretation eines Satzfragments von Art. 5 Absatz 3 ePD (im Folgenden „Art. 5(3)"): „Speicherung von Informationen oder der Zugriff auf Informationen, die bereits im Endgerät eines Teilnehmers oder Nutzers gespeichert sind". Wobei die Kommunikation auf Englisch erfolgte und somit der diskutierte Text so lautete: „storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user". Dafür wurde ein kleines Team von Rapporteuren zusammengestellt und mit der Erstellung und Begleitung des Dokuments beauftragt. Sachsen war als Rapporteur beteiligt. Wieso ist dieser Satz relevant und wie interagiert er mit den Bestimmungen der DSGVO? Zunächst sei darauf hingewiesen, dass die ePD im Gegensatz zur DSGVO nicht direkte Anwendung findet, sondern in nationales Recht umgesetzt werden muss. Dies ist in Deutschland das „Telekommunikations-Telemedien-Datenschutzgesetz" (TTDSG), und Art. 5(3)

entspricht dabei § 25 TTDSG. Ein wichtiger Unterschied zwischen dem TTDSG und der DSGVO ist, dass das TTDSG nicht nur die Verarbeitung personenbezogener Daten betrifft. Tatsächlich bezieht sich § 25 TTDSG auf jegliche Daten auf dem Endgerät. Ferner bezieht er sich auch nicht auf den Prozess der Verarbeitung, sondern auf den Moment der Speicherung oder des Zugriffs. Es ist jedoch durchaus möglich und üblich, dass beide Gesetze auf einen Sachverhalt zutreffen. Ein klassisches Beispiel für einen solchen Fall stellt ein Cookie dar. Bereits das Setzen des Cookies löst § 25 TTDSG aus (Speicherung), und wenn das Cookie für den Verbindungsaufbau nicht zwingend erforderlich ist oder vom Nutzer ausdrücklich gewünscht wurde, muss eine Einwilligung erfragt werden. Das Auslesen des Cookies ist eine Verarbeitung seitens eines Verantwortlichen und müsste somit der DSGVO unterliegen, allerdings wird dadurch ebenfalls § 25 TTDSG ausgelöst (Zugriff), und in diesem Fall „übertrumpft" das TTDSG als „lex specialis" die DSGVO. Erst in der nachfolgenden Verarbeitung, wenn also beispielsweise serverseitige Datenbankeinträge zu diesem Cookie angelegt oder geändert werden, gilt die DSGVO. Das bedeutet allerdings nicht, dass man dreimal Einwilligungen erfragen muss – diese können gebündelt abgegeben werden (siehe Orientierungshilfe Telemedien).

Orientierungshilfe Telemedien der DSK:
↗ sdb.de/tb2110

Ein weiterer wichtiger Unterschied ist die Zuständigkeit der Aufsicht. Mit der DSGVO gilt das sogenannte „One-Stop-Shop" Prinzip, nach welchem diejenige Aufsichtsbehörde „federführend" ist, welche für die Hauptniederlassung des Verantwortlichen zuständig ist, unabhängig davon, wo sich die Beschwerdeführerin bzw. der Beschwerdeführer befindet. Dies gilt auch für die Hauptniederlassung von Tochterunternehmen, beispielsweise die irländischen Niederlassungen diverser US-Unternehmen. Dieser Mechanismus existiert jedoch bei der ePD nicht. Die Zuständigkeit bleibt bei der zuständigen Aufsichtsbehörde der betroffenen Person. Dies ist auch nachvollziehbar, da die DSGVO primär eine Regulierung der Verarbeitung aufseiten des Verantwortlichen ist, während die ePD primär den Schutz der Privatsphäre der oder des Einzelnen verfolgt. Ob

Was ist zu tun?
Verantwortliche müssen beachten, ob sie eine Speicherung oder einen Zugriff auf Informationen auf dem Endgerät eines Nutzers auslösen. In diesen Fällen gilt das TTDSG mit anderen Voraussetzungen für die Einwilligung. Betroffene Personen können sich bei ihrer zuständigen Aufsichtsbehörde beschweren, und diese kann selbst ein Verfahren durchführen, auch wenn sich der Verantwortliche im EU-Ausland befindet.

diese Leitlinien dazu führen, dass Aufsichtsbehörden vermehrt Verfahren gegen Unternehmen außerhalb ihrer Zuständigkeit anstrengen, bleibt abzuwarten.

7.8 Grenzüberschreitendes Verfahren gegen einen Online-Gastgeberdienst

↗ Art. 4, 56–60 DSGVO

Die polnische Aufsichtsbehörde fragte 2020 zweimal über das Internal Market Information System (IMI) in einem Verfahren der freiwilligen Amtshilfe, wer für eine Beschwerde gegen einen Online-Gastgeberdienst, bei dem ein Löschungsantrag nach Art. 17 DSGVO ignoriert worden war, zuständig sei. Daraufhin meldete ich mich als federführende Aufsichtsbehörde, da der Betreiber dieses Netzwerks in Sachsen seinen Sitz hatte. 14 weitere Aufsichtsbehörden in der EU meldeten sich als andere betroffene Aufsichtsbehörden (Art. 60 DSGVO).

Der Betreiber antwortete auf ein Schreiben mit der Information über die Beschwerde und Fragen der Aufsichtsbehörde nicht. Auch der Erlass eines Heranziehungsbescheides führte zu keiner Reaktion. Allerdings wurde im Laufe des Berichtszeitraums die Website des Online-Gastgeberdienstes zunächst abgeschaltet. Im Rahmen der Anhörung zur beabsichtigten Verwarnung und Abhilfeanordnungen wurde dem Betreiber wiederum Gelegenheit zur Äußerung gegeben. Von diesem Schreiben wurden die anderen betroffenen Aufsichtsbehörden informiert. Eine Stellungnahmefrist ließ der Betreiber fruchtlos verstreichen. Daraufhin entwarf ich eine detaillierte Verwarnung, mit der ich den Betreiber zudem verpflichtete, die Daten des Beschwerdeführers zu löschen und mir innerhalb von zwei Wochen die Löschung nachzuweisen; andernfalls drohte ich ihm ein Zwangsgeld in vierstelliger Höhe an. Meinen Entwurf habe ich den anderen betroffenen Aufsichtsbehörden in IMI erst formlos und

schließlich als Beschlussentwurf gemäß Art. 60 Abs. 3 Satz 2 DSGVO bekannt gegeben.
Alsbald wird er in IMI als endgültiger Beschluss gemäß Art. 60 Abs. 7 DSGVO erlassen werden (Stand: 15.02.2024).

7.9 Erfolgreiche Vertretung der Interessen eines Beschwerdeführers in einem Verfahren mit der spanischen Datenschutzaufsichtsbehörde

↗ Art. 4, 56–65 DSGVO

Tätigkeitsbericht Datenschutz 2022:
↗ sdb.de/tb2022

Bereits im Tätigkeitsbericht 2022 (6.2.6, Seite 162) hatte ich von einem Fall berichtet, in dem eine in Sachsen wohnhafte Person sich bei mir über ein Unternehmen mit einer einzigen Niederlassung in einem anderen Mitgliedsstaat beschwert hatte. Damals hatte ich die Beschwerde mithilfe des Internal Market Information Systems (IMI) an die federführende spanische Aufsichtsbehörde abgegeben und anschließend Einspruch gemäß Art. 60 Abs. 4 DSGVO gegen deren Entscheidungsentwurf eingelegt. Ich war nämlich – im Gegensatz zu der federführenden Behörde – der Ansicht, dass der Beschwerdegegner nicht lediglich Auftragsverarbeiter (Art. 28 Abs. 1 DSGVO), sondern Verantwortlicher (Art. 4 Nr. 7 DSGVO) war.
Im Berichtszeitraum konnte ich die federführende Behörde von meiner Rechtsauffassung überzeugen. Sie stellte daraufhin einen neuen Beschlussentwurf in IMI ein, wonach der Beschwerdegegner als Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO erkannt wurde; zugleich erhöhte sie die Geldbuße um das Fünffache. Nach Konsultation der übrigen deutschen Aufsichtsbehörden teilte ich mein Einverständnis mit dem neuen Bescheid mit.
Dennoch kam der Fall nicht zu einem schnellen Ende. Im März 2023 stellte die federführende Behörde einen überarbeiteten

Beschlussentwurf zur Eröffnung des Bußgeldverfahrens gemäß Art. 60 Absatz 3 Satz 2 DSGVO im IMI ein. Nach Konsultation der übrigen vier deutschen betroffenen Aufsichtsbehörden billigte ich den Entwurf. Da auch keine andere betroffene Aufsichtsbehörde Einspruch einlegte, wurde der Eröffnungsbescheid für die beteiligten Aufsichtsbehörden gemäß Art. 60 Absatz 6 DSGVO bindend.

Der Beschwerdegegner nahm den Eröffnungsbescheid jedoch nicht unwidersprochen hin. Er erhob Einwendungen und machte insbesondere darauf aufmerksam, dass die beabsichtigte Entscheidung wesentliche Auswirkungen auf sein bis dahin florierendes Kleinunternehmen haben würde. Die federführende Behörde änderte daraufhin ihren Bußgeldbescheid ab. Dieser Beschlussentwurf führte zu keinen Einsprüchen durch die übrigen Aufsichtsbehörden. Danach ist gemäß Art. 60 Absatz 6 DSGVO der Bußgeldbescheid bindend für die betroffenen Aufsichtsbehörden geworden. Damit habe ich mich erfolgreich für die Interessen des sächsischen Beschwerdeführers eingesetzt; der Beschwerdegegner muss seine Praxis ändern. Zumindest hat er im Februar 2024 seinen Namen geändert.

Leider ist bis zum Schluss des Berichtszeitraums der Bußgeldbescheid gemäß Art. 60 Absatz 7 DSGVO noch nicht erlassen worden. Auf Nachfrage beim zuständigen Bearbeiter bei der spanischen Aufsichtsbehörde AEPD und auf deren Website erfuhr ich, dass der die übrigen beteiligten Aufsichtsbehörden bindende Bußgeldbescheid über 100.000 Euro auf deren Website veröffentlicht war. Der Verantwortliche hatte der Entscheidung im Sommer 2023 widersprochen. Dieses Rechtsmittel wurde von der AEPD am 30.1.2024 zurückgewiesen. Der endgültige Bußgeldbescheid soll unverzüglich den übrigen Aufsichtsbehörden und dem EDSA über IMI bekannt gemacht werden.

Damit wird das Verfahren auf europäischer Verwaltungsebene beendet sein, und ich werde den sächsischen Beschwerdeführer vom erfolgreichen Ausgang seiner Beschwerde informieren. Es bleibt abzuwarten, ob der Verantwortliche in Spanien Rechtsmittel gegen den Bußgeldbescheid einlegen wird.

Der Aufwand in diesem Verfahren war für mich hoch. Ich musste mich über IMI nicht nur mit der spanischen Aufsichtsbehörde auseinandersetzen (die Kommunikation erfolgte auf Englisch), sondern meine Tätigkeit auch mit fünf anderen deutschen Datenschutzaufsichtsbehörden koordinieren: Baden-Württemberg, Bayern (BayLDA), Berlin, Hessen und Mecklenburg-Vorpommern.

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

8.1 Polizeilicher Einsatz von Drohnen bei einem Fußballspiel

↗ § 57 Abs. 1 SächsPVDG

Im Berichtszeitraum wandten sich mehrere Petenten mit der Bitte um datenschutzrechtliche Kontrolle eines polizeilichen Drohneneinsatzes während eines Fußballspiels an mich. Die Vielzahl der Beschwerden sowie der aufgeworfenen Fragen zeigen mir eine große Verunsicherung der Bürger in Hinblick auf den polizeilichen Einsatz von Drohnen zur Fertigung von Bildaufnahmen im Rahmen von Großveranstaltungen. Daher gehe ich folgend auf die dringlichsten Fragen ein:

Was war die Rechtsgrundlage für den Drohneneinsatz beim oben erwähnten Fußballspiel?

Die verantwortliche Polizeidirektion (PD) teilte auf meine Nachfrage hin mit, der Einsatz eines unbemannten Luftfahrtsystems, umgangssprachlich „Drohne", sei zur Bildübertragung auf Grundlage des § 57 Abs. 1 Sächsisches Polizeivollzugsdienstgesetz (SächsPVDG) erfolgt. Es habe sich um eine offene Maßnahme zur Lenkung und Leitung des Polizeieinsatzes bei dem betreffenden Spiel gehandelt. Störungen aus den unterschiedlichen Fanlagern hätten erfahrungsgemäß nicht ausgeschlossen werden können. Der Einsatzraum um das Stadion sei aufgrund der direkten angrenzenden Lage an einen Gartenverein sowie eine städtische Parkanlage unübersichtlich. Im Stadion selbst stehe keine Videoüberwachungsanlage zur Verfügung. Zudem sei kein polizeilicher Führungspunkt im Stadion, mit Sicht auf die unterschiedli-

chen Fanblöcke, zur Verfügung gestellt worden. Daraus habe sich die Erforderlichkeit geeigneter Mittel zur Bildübertragung an die Einsatzleitung ergeben.
Datenschutzrechtlich habe ich insoweit keine Bedenken. Für einen polizeilichen Drohneneinsatz während eines Fußballspiels kommt § 57 Abs. 1 SächsPVDG als Rechtsgrundlage in Betracht. Danach kann die Polizei bei abstrakten Gefahren im Zusammenhang mit öffentlichen Veranstaltungen oder Ansammlungen unter freiem Himmel, die nicht dem Sächsischen Versammlungsgesetz unterliegen, offen Übersichtsbildübertragungen anfertigen, wenn und soweit dies wegen der Größe der Veranstaltung oder Ansammlung oder der Unübersichtlichkeit der Lage zur Lenkung und Leitung eines Polizeieinsatzes im Einzelfall erforderlich ist. Die Voraussetzungen lagen hier offensichtlich vor. Insbesondere ist für einen Drohneneinsatz gemäß § 57 Abs. 1 SächsPVDG während eines Fußballspiels eine abstrakte Gefahr erforderlich – aber auch ausreichend –, das heißt, es muss eine Sachlage vorliegen, bei der nach allgemeiner Lebenserfahrung oder den Erkenntnissen fachkundiger Stellen mit hinreichender Wahrscheinlichkeit typischerweise Gefahren für ein polizeiliches Schutzgut (öffentliche Sicherheit und Ordnung) entstehen. Unter Berücksichtigung der von der PD vorgetragenen Gesamtumstände lag im Rahmen des Fußballspiels eine abstrakte Gefahr vor. In Kompensation der geringfügigen Eingriffsschwelle einer nur abstrakten Gefahrenlage verbietet das Gesetz eine Identifikation von Personen oder die Aufzeichnung der übertragenen Livebilder (§ 57 Abs. 1 Satz 2 SächsPVDG).

Warum wurden die Zuschauerinnen und Zuschauer nicht oder nicht ausreichend über den Einsatz informiert? Wie müsste eine datenschutzrechtlich korrekte Information erfolgen, wie oft müsste die Information erfolgen und in welcher Art und Weise? Braucht die Drohne eine Kennzeichnung und muss der Drohnenführer/die Drohnenführerin erkennbar sein?

Wie die PD erklärte, sei im Vorfeld der Spielbegegnung in der Sicherheitsberatung bei dem sächsischen Fußballverein

über den Drohneneinsatz offen kommuniziert und seien Absprachen hierzu getroffen worden. Zusätzlich sei auf Veranlassung der Polizei über Durchsagen des Stadionsprechers zum polizeilichen Drohneneinsatz informiert worden. Der Drohnenführer sei als uniformierter Polizeibeamter erkennbar und mit einem Dienstfahrzeug der Polizei am Einsatzort gewesen. Die Drohne selbst sei zum Zwecke der Erkennbarkeit mit Blinklichtern versehen gewesen. Eine zusätzliche Kenntlichmachung der Drohne mittels Aufkleber der Polizei Sachsen sei erst bei späteren Einsätzen erfolgt.

Diese Maßnahmen waren allein nicht geeignet bzw. ausreichend, um die gesetzliche Voraussetzung der Offenlegung der Fertigung und Aufzeichnung von Bildaufnahmen durch die Polizei gegenüber den Betroffenen zu erfüllen. Zuständig für die Information eines Drohneneinsatzes ist der datenschutzrechtlich Verantwortliche, vorliegend die durchführende Polizeidienststelle. § 57 Abs. 1 SächsPVDG ist technikoffen formuliert. Das heißt, dass der Einsatz von Drohnen als Kameraträger sich nach den allgemeinen für die Fertigung von Bildaufnahmen einschlägigen Vorschriften richtet, die ebenso für Bildaufnahmen mittels Handkamera, temporärer stationärer Kameras oder Aufnahmetechnik in Hubschraubern gelten. Im Vergleich der Eingriffsintensität der Varianten des Technikeinsatzes ist aufgrund der Bewegungsflexibilität, der Größe und des geringen Betriebsgeräusches von Drohnen die mit dem Drohneneinsatz verbundene subjektive Eingriffsintensität höher als die von entsprechender Technik auf einem Dach oder in einem Hubschrauber. Daher ist die im Gesetz bestimmte „Offenheit" (das heißt Erkennbarkeit) der Bildübertragung bei Drohneneinsätzen an weitergehende tatsächliche Anforderungen gebunden. Zwar trifft das Gesetz keine konkreten Bestimmungen zur Art und Weise, in der die Erkennbarkeit des Drohneneinsatzes durch die Polizei sicherzustellen ist. Dass aber Maßnahmen zur Information der von der Überwachung betroffenen Personen ergriffen werden müssen, ist aufgrund des ausdrücklichen Gebots der offenen Datenerhebung unumgänglich. Wie die Polizei die Offenkundigkeit des Drohneneinsatzes gewährleistet, hängt von den Umständen

des Einzelfalles und den jeweiligen Gegebenheiten vor Ort ab. Die leichte Erkennbarkeit bzw. auffällige Kennzeichnung der Drohne als polizeiliches Gerät kann dazu ebenso beitragen wie eine ins Auge fallende Kennzeichnung des Drohnenpiloten, etwa mittels einer Warnweste mit Aufdruck. Das Tragen einer Polizeiuniform allein wird in der Regel nicht ausreichend sein, erst recht, wenn sich der Drohnenpilot an oder in einem Polizeifahrzeug ganz am Rand des Geschehens aufhält. Darüber hinaus werden aber – gerade bei größeren Personengruppen – auch mehrere Lautsprecherdurchsagen, optische Hinweise (gegebenenfalls kurzzeitig auf Leinwänden oder Anzeigetafeln) oder Informationen der Veranstaltungsleitung erforderlich sein, um möglichst allen Betroffenen Kenntnis von der polizeilichen Maßnahme zu ermöglichen. Zu beachten ist dabei, dass die Polizei auch ohne Kooperationsbereitschaft eines Veranstalters die Erkennbarkeit des Drohneneinsatzes sicherstellen muss.
Ich habe die PD aufgefordert, dies bei künftigen Drohneneinsätzen im Rahmen von Versammlungen, Ansammlungen und (Groß-)Veranstaltungen zu beachten.

Wurden die Bilder aufgezeichnet, und, wenn ja, was passiert mit ihnen? Oder werden nur Übersichtsbilder gemacht, um den Polizeieinsatz zu steuern?

Die PD teilte mit, dass innerhalb der Stadionbereiche keine individualisierbaren Bildaufzeichnungen gefertigt oder Bildaufzeichnungen gespeichert wurden. Im Zuge der Abreisebewegungen der Fanlager sei nach Feststellung eines strafrechtlichen Sachverhaltes durch die Kräfte der Bundespolizei die Bildaufzeichnung mittels Drohne veranlasst wurden. Die Aufzeichnungen seien im Bereich eines S-Bahn-Haltepunktes zu Zwecken der Beweissicherung in den Verfahren der Bundespolizei erfolgt. Datenschutzrechtliche Fragen zur Bildaufzeichnung, deren Verwendung und gegebenenfalls Speicherung dürfen in diesem Fall nicht von mir überprüft werden, da Verantwortlicher nicht die sächsische Polizei, sondern die Bundespolizei ist, für deren Kontrolle ich nicht zuständig bin.
Wie bereits erwähnt, wäre eine Identifizierung von Perso-

nen bei Bildübertragungen nach § 57 Abs. 1 SächsPVDG ebenso unzulässig wie eine Aufzeichnung der Bilder. Aufzeichnungen sind unter den Voraussetzungen von § 57 Abs. 2 SächsPVDG erlaubt oder – zu Beweissicherungszwecken bei einem Anfangsverdacht für Straftaten – auf Grundlage strafprozessualer Vorschriften.

Die Drohne flog dauerhaft über den öffentlichen „Freiluft-Toiletten" (offene Open-Air-Pissoirs, die hinter der Tribüne im Gastrobereich stehen). Gibt es Möglichkeiten, das Beobachten dieses Bereichs zu unterbinden?

Die PD erläuterte hierzu, dass das sichtbare, übertragene Bild der Drohne in die Einsatzzentrale aufgrund des Betrachtungswinkels deutlich vom jeweiligen Standort der Drohne abweiche. Es könne eine abweichende Wahrnehmung der Betroffenen zwischen Standort der Drohne in der Luft und der tatsächlichen Bildübertragung entstehen. Toilettenbereiche seien nicht bildlich übertragen worden.

Die Drohne flog mehrmals über einen vollbesetzten Fanblock, welche Gefahren bestehen bei einem möglichen Absturz des Fluggeräts? Ist das Überfliegen von Fanblöcken gestattet?

Für die technische Umsetzung eines Drohneneinsatzes ist das Polizeiverwaltungsamt (PVA) zuständig. Auf meine Bitte um Stellungnahme zur Sicherheit eines Drohneneinsatzes teilte das PVA mit, dass auf die Sicherheit bei der eingesetzten Drohnentechnik besonders geachtet werde. Möglichen witterungsbedingten Gefahren werde durch die Einholung entsprechender Vorinformationen zur erwarteten Wetterlage Rechnung getragen. Im Einzelfall erfolge sodann kein Drohneneinsatz. Risiken durch andere Luftfahrzeuge werde bei entsprechender Notwendigkeit durch eine Anmeldung bei der Flugsicherung begegnet. Im Übrigen erfolge der Drohneneinsatz grundsätzlich im Sichtbereich des Starters. Abstandssensoren und bei Bedarf das Radarsystem würden zudem mögliche Risiken durch Hindernisse minimieren. Die

Risiken eines Technikausfalls, eines Bedienfehlers oder anderer gleichgelagerter Störungen würden durch regelmäßige Schulungen und Fortbildungen der Starter minimiert. Des Weiteren werden während eines Einsatzes die bestehenden Warneinrichtungen der Drohnensteuerung genutzt. Die Drohnen unterliegen regelmäßigen Wartungsintervallen. Die sogenannte Home-Funktion einer Drohne gewährleiste, dass technikseitig ein automatischer Rückflug der Drohne für den Fall technischer Störungen erfolge. Hinsichtlich der Gefahr eines Absturzes in voll besetzte Fanblöcke bei Fußballspielen sei konkret zu ergänzen, dass der Überflug von Menschenansammlungen – wie beispielsweise Fanblöcken bei einem Fußballspiel – bereits gemäß geltendem Betriebskonzept grundsätzlich ausgeschlossen sei. Menschenansammlungen würden grundsätzlich nicht überflogen. Ausnahmen würden sich gegebenenfalls aus entsprechenden polizeilichen Gefahrenlagen nach einer Abwägung der bestehenden Risiken ergeben.

Was ist zu tun?
Zur Information der von der Überwachung betroffenen Personen müssen seitens der verantwortlichen Polizeidienststelle Maßnahmen ergriffen werden. Wie die Polizei die Offenkundigkeit des Drohneneinsatzes gewährleistet, hängt von den Umständen des Einzelfalles und den jeweiligen Gegebenheiten vor Ort ab.

8.2 Einsatz von polizeilicher Kameratechnik (Bildübertragungswagen) oberhalb eines Busparkplatzes im Rahmen eines Fußballspiels

↗ § 57 Abs. 1 SächsPVDG

Neben den zahlreichen Beschwerden über einen polizeilichen Drohneneinsatz im Rahmen eines Fußballspiels erreichte mich auch der Hinweis eines Petenten, der beobachtet hatte, dass ein Polizeifahrzeug mit ausgefahrenem Kameramast auf der Brücke oberhalb eines Busparkplatzes geparkt und vermutlich Bildaufnahmen gefertigt habe. Das Fahrzeug sei nicht klassisch als Polizeifahrzeug gekennzeichnet, allerdings sei innerhalb der Fahrerkabine ein Polizeibeamter erkennbar gewesen. Der Petent bat mich um datenschutzrechtliche Prüfung der polizeilichen Fertigung von Bildaufnahmen und

um Einschätzung, inwieweit das Videofahrzeug der Polizei der Kennzeichnungspflicht gemäß § 57 Abs. 1 Sächsisches Polizeivollzugsdienstgesetz (SächsPVDG) unterliegt.
Die von mir um Stellungnahme gebetene Polizeidirektion (PD) bestätigte den Sachverhalt. Oberhalb des Busparkplatzes habe eine Übersichtsbildübertragung in Form einer „Livebildübertragung" in den Führungsstab zur Lenkung und Leitung stattgefunden, da auf dem Busparkplatz erheblicher Anreiseverkehr zu einem Fußballspiel stattgefunden habe. Rechtsgrundlage für die offene Bildübertragung sei § 57 Abs. 1 Satz 1 SächsPVDG gewesen. Hiernach kann die Polizei bei abstrakten Gefahren im Zusammenhang mit öffentlichen Veranstaltungen oder Ansammlungen unter freiem Himmel, die nicht dem Sächsischen Versammlungsgesetz unterliegen, offen Übersichtsbildübertragungen anfertigen, wenn und soweit dies wegen der Größe der Veranstaltung oder Ansammlung oder der Unübersichtlichkeit der Lage zur Lenkung und Leitung des Polizeieinsatzes im Einzelfall erforderlich ist.
Zum Fußballspiel habe man mit insgesamt 29.000 Zuschauern gerechnet. Aufgrund der unterschiedlichen Anreisemöglichkeiten sei bereits zu Beginn der Anreise mit einer unübersichtlichen Lage im Stadtgebiet zu rechnen gewesen. Die Größe der Veranstaltung und des möglichen Anreiseradius im kompletten Stadtgebiet habe die Übersichtsbildübertragung im Sinne des § 57 Abs. 1 SächsPVDG erforderlich gemacht. Aufgrund des Gefahrenpotenzials habe jedenfalls eine abstrakte Gefahr vorgelegen. Die eingesetzte Videotechnik sei daher erforderlich gewesen, um dieser Gefährdungslage abzuhelfen. Hinsichtlich der Voraussetzung der Offensichtlichkeit dieses Einsatzes erläuterte die PD, dass ein Polizeifahrzeug des Polizeiverwaltungsamtes (PVA) zum Einsatz gekommen sei, welches an den jeweiligen Fahrzeugseiten über eine Beschriftung mit der Aufschrift „POLIZEI" verfügt habe. Des Weiteren habe es sich um eine ausgefahrene Mastkamera auf dem Dach des Einsatzfahrzeuges (Bildübertragungswagen) gehandelt, die gut erkennbar und damit offensichtlich gewesen sei. Dieser Bildübertragungswagen habe sich zu dem Zeitpunkt auf der Brücke mit Blickrich-

tung der ausgefahrenen Mastkamera auf den Busparkplatz befunden. Des Weiteren seien auf dem Parkplatz mehrere Polizeibeamte im Einsatz gewesen, sodass hieraus ebenfalls hätte geschlussfolgert werden können, dass es sich um einen offensichtlichen und damit offenen polizeilichen Einsatz gehandelt habe. Die Beamten vor Ort seien dazu berechtigt gewesen, Auskunft auf Nachfragen hinsichtlich der Livebildübertragung zu geben, und hätten hiervon auch Gebrauch gemacht.

Das Ergebnis meiner datenschutzrechtlichen Prüfung lautete, dass der oben genannte Einsatz von Kameratechnik unter Berücksichtigung der von der PD vorgetragenen Gesamtumstände und abstrakten Gefahrenlage zwar die materiellen Voraussetzungen von § 57 Abs. 1 SächsPVDG erfüllte (siehe 8.1), allerdings entgegen dem Gesetz nicht „offen" erfolgte. § 57 SächsPVDG bestimmt den „offenen" Einsatz technischer Mittel, das heißt, der Verantwortliche ist verpflichtet, auf die Tatsache der Videoüberwachung aufmerksam zu machen, soweit diese nicht offenkundig ist. An die Annahme der Offenkundigkeit – als Ausnahme von der grundsätzlichen Hinweispflicht einerseits und als Abgrenzungskriterium zum verdeckten Einsatz andererseits – sind hohe Anforderungen zu stellen. Es sind letztlich nur solche Fälle von der Hinweispflicht ausgeschlossen, in denen der polizeiliche Einsatz von technischen Mitteln der betroffenen Person buchstäblich direkt „ins Auge fällt". Dies ist jedoch nur in solchen Fällen anzunehmen, in denen eine Verbindung zwischen der Kamera und einem Beamten auf den ersten Blick ohne Zweifel sofort erkennbar ist, etwa bei einem uniformierten Polizeibeamten, der eine Kamera (auch Stabkamera) in der Hand hält. In diesem Fall wird der Betroffene direkt von der Kamera erfasst, kann dies aber auch sofort selbst erkennen (Verwaltungsgericht Sigmaringen, Urteil vom 20.10.2020 – 14 k 7613/18). Im vorliegenden Fall sprach schon der Standort des Einsatzfahrzeugs mit Mastkamera gegen eine solche Offenkundigkeit. Überwachungsgebiet war ein Busparkplatz. Der Bildübertragungswagen stand oberhalb des Busparkplatzes auf einer den Busparkplatz überführenden Brücke,

das heißt außerhalb des überwachten Gebietes und somit außerhalb des direkten Blickfeldes der Betroffenen. Sollten die Betroffenen dennoch das Fahrzeug mit der durchaus auffälligen Mastkamera wahrgenommen haben, folgte selbst daraus keine zwingende Erkennbarkeit einer polizeilichen Videoüberwachung. Das Einsatzfahrzeug des PVA war kein Polizeifahrzeug mit typischer Farbgebung und deutlicher, großer Beschriftung, sondern ähnelte optisch einem zivilen Kleinbus und war mit eher kleinerer, farblich unauffälliger seitlicher Beschriftung versehen. Diese Beschriftung war zum einen bereits aufgrund der Entfernung Busparkplatz – Brücke nicht deutlich zu erkennen bzw. zu „entziffern", zum anderen ist davon auszugehen, dass das Brückengeländer die Beschriftung zumindest teilweise verdeckt hat. Ein erkennbares, aber farblich unauffälliges Fahrzeug mit Mastkamera ist nicht zwingend einem polizeilichen Einsatz zuzuordnen, sondern kann durchaus auch den Medien (Rundfunk, Fernsehen) zugeschrieben werden. Auch, dass auf dem Busparkplatz mehrere Polizeibeamte im Einsatz gewesen seien, sodass hieraus ebenfalls geschlussfolgert hätte werden können, dass es sich um einen polizeilichen Einsatz gehandelt habe, führt zu keinem anderen Ergebnis. Die eingesetzte Videotechnik war nur ein Teil des Polizeieinsatzes rund um ein Fußballspiel, der selbstverständlich und wie üblich auch den Einsatz von Beamten zu Fuß umfasste. Eine Verbindung zwischen der Kamera und einem Beamten kann schon allein wegen unterschiedlicher Standorte nicht auf den ersten Blick erkennbar gewesen sein. Dass die Beamten vor Ort dazu berechtigt gewesen seien, Auskunft auf Nachfragen hinsichtlich der Livebildübertragung zu geben und hiervon auch Gebrauch gemacht hätten, ist erfreulich, entbindet den Verantwortlichen (PD) allerdings keinesfalls davon, selbst proaktiv auf die nicht offenkundige Videoüberwachung hinzuweisen. Wie bereits im Beitrag zum polizeilichen Einsatz von Drohnen erläutert (vgl. 8.1), muss die Polizei sicherstellen, dass alle Betroffenen die Möglichkeit erhalten, ohne Weiteres Kenntnis von der polizeilichen Maßnahme zu erlangen. Wie die Polizei die Offenkundigkeit gewährleistet, hängt

Was ist zu tun?

An die Annahme der Offenkundigkeit von Bildübertragungen oder -aufnahmen – als Ausnahme von der grundsätzlich erforderlichen Hinweispflicht und als Abgrenzungskriterium zum verdeckten Einsatz – sind hohe Anforderungen zu stellen. Es sind letztlich nur solche Fälle von der Hinweispflicht ausgeschlossen, in denen der Einsatz von technischen Mitteln der betroffenen Person buchstäblich direkt „ins Auge fällt".

auch hier von den Umständen des Einzelfalles und den jeweiligen Gegebenheiten vor Ort ab. Die leichte Erkennbarkeit des Bildübertragungswagens als polizeiliches Fahrzeug kann dazu beitragen. Darüber hinaus werden aber – gerade bei größeren Personengruppen – auch mehrere Lautsprecherdurchsagen oder optische Hinweise erforderlich sein. Ich habe daher die PD als datenschutzrechtlicher Verantwortlicher gebeten, dies bei künftigen Einsätzen im Rahmen von Versammlungen, Ansammlungen und (Groß-)Veranstaltungen zu beachten.

8.3 Speicherung personenbezogener Daten im polizeilichen Auskunftssystem Sachsen (PASS)

↗ §§ 80, 91 SächsPVDG

Ein Petent hatte 2023 von der sächsischen Polizei auf seinen Antrag eine Auskunft über die zu seiner Person verarbeiteten Daten erhalten (§ 92 Abs. 2 Sächsisches Polizeivollzugsdienstgesetz [SächsPVDG] in Verbindung mit § 13 Sächsisches Datenschutz-Umsetzungsgesetz [SächsDSUG]). Ihm fiel auf, dass im Polizeilichen Auskunftssystem Sachsen (PASS) ein Eintrag vorhanden war, der einen gegen ihn erhobenen Vorwurf der Verbreitung, Veröffentlichung, des Erwerbs und des Besitzes kinderpornografischer Inhalte aus dem Jahr 2017 zum Inhalt hatte. Die Polizei hatte den Fall Anfang 2018 an die zuständige Staatsanwaltschaft abgegeben, diese stellte das Verfahren 2018 bzw. 2019 (hierzu liegen unterschiedliche Angaben vor) nach § 170 Abs. 2 Strafprozessordnung (StPO) ein, weil das angezeigte Verhalten keinen Straftatbestand erfüllt hatte.

Nach den gesetzlichen Vorgaben hätte die Staatsanwaltschaft nach § 482 Abs. 2 StPO die Polizei über den Ausgang des Verfahrens, also die Verfahrenseinstellung, unterrichten müssen. Die Polizei hätte daraufhin den Eintrag im PASS unverzüglich löschen müssen (§ 43 Abs. 2 Satz 2 SächsPolG

alte Fassung, dem der heutige § 80 Abs. 4 in Verbindung mit § 91 Abs. 2 SächsPVDG entspricht).

Die Aufklärungsbemühungen der Polizei förderten zutage, dass laut Registratur der Staatsanwaltschaft zwar die Versendung der Mitteilung über den Ausgang des Verfahrens an die Polizei erfolgt war, die Mitteilung der Datenstation der Polizei jedoch nicht bekannt gewesen sei. Ob und auf welchem Weg die Unterrichtung über den Ausgang des Verfahrens bei der Polizei verlustig gegangen sei, konnte nicht mehr rekonstruiert werden. Die Löschung des Datensatzes bei der Polizei erfolgte unverzüglich nach Bekanntwerden der Hintergründe.

Während in den 1990er und Anfang der 2000er Jahre die regelmäßige Rückmeldung der Verfahrensausgänge durch die Staatsanwaltschaft an die Polizei größere Schwierigkeiten bereitete und nicht einwandfrei funktionierte, scheint es sich nach der Behebung dieser Probleme (vgl. 12. TB 2005, Beitrag 5.9.4, Seite 141) im geschilderten aktuellen Fall um ein seltenes (Büro-)Versehen oder einen Verlust der Meldung auf dem Übermittlungsweg gehandelt zu haben.

12. Tätigkeitsbericht (2005) für den öffentlichen Bereich:
↗ sdb.de/tb12oeb

Allerdings kam vorliegend ein „Sicherungsmechanismus", den die Polizei für Fälle ausbleibender Mitteilungen über Verfahrensausgänge durch die Staatsanwaltschaft eingerichtet hat, nicht zur Anwendung. Nach Ablauf von polizeiintern festgelegten Prüffristen nach Abgabe des Verfahrens soll – falls bis dahin noch keine Mitteilung der Staatsanwaltschaft erfolgt sein sollte – die zuständige Polizeidienststelle bei der Staatsanwaltschaft den Verfahrensausgang aktiv erfragen (vgl. 12. Tätigkeitsbericht für den öffentlichen Bereich, a. a. O.). Die Frist endet nach meiner Kenntnis zwei Jahre nach Abgabe des Verfahrens an die Staatsanwaltschaft. Eine aktive Nachfrage der Polizei zum Verfahrensausgang hätte im vorliegenden Fall also 2020 bzw. 2021 erfolgen müssen, wurde aber offenkundig nicht gestellt.

Die Kenntnis von Verfahrensausgängen ist für die Polizei insofern wichtig, als sie wesentlichen Einfluss auf die Entscheidung über die weitere polizeiliche Speicherung der Daten der tatverdächtigen, beschuldigten oder zwischenzeitlich frei-

gesprochenen oder verurteilten Person hat. Entfällt nach der staatsanwaltschaftlichen oder gerichtlichen Entscheidung der ursprüngliche Tatverdacht, wie im vorliegenden Fall, gänzlich, ist eine Löschung der Daten im polizeilichen Informationssystem gesetzlich zwingend vorgeschrieben.

Die Aktualität, Vollständigkeit und Richtigkeit der gespeicherten Daten – oder eben ihre Löschung – sind auch für die betroffenen Personen von immenser Bedeutung. Gerade Tatvorwürfe aus Anzeigen, die gesellschaftlich besonders geächtete Delikte betreffen, sind geeignet, den Ruf der betroffenen Person nachhaltig zu schädigen. Dieser Gefahr ist mit großer Sorgfalt bei der Datenverarbeitung (einschließlich der Speicherung und Löschung) zu begegnen.

Bei Speicherungen im PASS kommt erschwerend hinzu, dass Eintragungen über beschuldigte Personen im Wege der Auskunft aus PASS praktisch sämtlichen Bediensteten des sächsischen Polizeivollzugsdienstes zugänglich sind. Zugriffsbeschränkungen im PASS sind, wie mir das Landeskriminalamt mitteilte, technisch nicht möglich.

Der geschilderte Fall gibt Anlass für grundsätzliche Überlegungen zur Verfassungskonformität des sächsischen Informationssystems der Polizei; die Kombination aus einer Erfassung im PASS, die unter relativ geringen Voraussetzungen erfolgt, und einem Zugriffsrecht sämtlicher Polizeibediensteten ist nicht nur datenschutzrechtlich, sondern auch verfassungsrechtlich hochproblematisch.

Derzeit werden die polizeiliche Informationsordnung betreffende Vorschriften des Bundeskriminalamtgesetzes (BKAG) durch das Bundesverfassungsgericht überprüft, ähnlich gelagerte gesetzliche Vorschriften des SächsPVDG stehen am Sächsischen Verfassungsgerichtshof auf dem Prüfstand.

Ich beabsichtige, die dargestellten datenschutzrechtlichen Probleme mit dem Sächsischen Staatsministerium des Innern zu erörtern, sobald die Anfang 2024 zu erwartenden Entscheidungen der Verfassungsgerichte vorliegen.

Was ist zu tun?

Die Einhaltung gesetzlicher Vorschriften zur (Weiter-)Verarbeitung personenbezogener Daten stellt nicht nur das rechtmäßige Handeln der Polizei sicher, sondern ist auch für betroffene Personen von größter Bedeutung. Aus diesem Grund sind auch dem Betroffenenschutz dienende untergesetzliche Vorgaben streng zu beachten.

8.4 Polizeiliche Identitätsfeststellung des Beifahrers im Rahmen einer allgemeinen Verkehrskontrolle

Ein Hinweisgeber wandte sich an meine Behörde und schilderte folgenden Sachverhalt: Im Rahmen einer allgemeinen Verkehrskontrolle sei er als Fahrzeugführer durch zwei Polizeibeamte angehalten und kontrolliert worden. Sein Beifahrer sei durch die Polizeibeamten ebenfalls aufgefordert worden, seinen Ausweis vorzuzeigen. Der Hinweisgeber bat mich um datenschutzrechtliche Prüfung dieser polizeilichen Identitätsfeststellung seines Beifahrers und somit Betroffenen der polizeilichen Maßnahme.

Zunächst habe ich den Hinweisgeber darauf aufmerksam gemacht, dass nur Betroffene, also diejenigen Personen, deren personenbezogene Daten verarbeitet werden (hier der Beifahrer) einen Anspruch auf Auskünfte zum datenschutzrechtlichen Prüfverfahren (zum Beispiel Ergebnismitteilung) haben. Da es mir zudem ohne ausdrückliche Einwilligung des Betroffenen nicht möglich ist, seine personenbezogenen Daten zur Aufnahme von Ermittlungen gegenüber der verantwortlichen Polizeidirektion (PD) zu verwenden, habe ich den Betroffenen gesondert angeschrieben und um Mitteilung gebeten, ob er mit der Preisgabe seiner Identität gegenüber der PD einverstanden ist. Der Betroffene erteilte sein Einverständnis.

Auf meine Bitte um Stellungnahme teilte die PD mit, dass unter Zugrundelegung der Ausführungen des bei der Verkehrskontrolle handelnden Polizeibeamten sowie rechtlicher Erwägungen hinsichtlich der konkreten Kontrollsituation und der damit verbundenen polizeilichen Maßnahmen aus ihrer Sicht kein Anlass zu etwaigen Beanstandungen im Hinblick auf datenschutzrechtliche Aspekte oder in Bezug auf die Verhältnismäßigkeit bestehe. Der die allgemeine Verkehrskontrolle und Identitätsfeststellung durchführende Polizeibeamte gab an, der Fahrzeugführer sei einer Ver-

kehrskontrolle unterzogen wurden, wobei eine Verkehrsordnungswidrigkeit gemäß § 24a Abs. 1 Straßenverkehrsgesetz (StVG, Trunkenheitsfahrt) festgestellt worden sei. Dementsprechend seien vom Beifahrer die Personalien als Zeuge im Ordnungswidrigkeitenverfahren gemäß § 46 Abs. 1 Ordnungswidrigkeitengesetz (OWiG) in Verbindung mit § 163b Abs. 2 Strafprozessordnung (StPO) erfasst worden. Er hätte als Zeuge im Ordnungswidrigkeitenverfahren be- und entlastende Beweise erbringen können.

Im Gegensatz zur verantwortlichen PD habe ich Zweifel an der Rechtmäßigkeit der polizeilichen Identitätsfeststellung. Gemäß § 36 Abs. 5 Straßenverkehrsordnung (StVO) darf nur der Fahrzeugführer im Rahmen einer allgemeinen Verkehrskontrolle kontrolliert werden. Die Identität des Beifahrers darf durch die Polizei unter den Voraussetzungen der Strafprozessordnung festgestellt werden, wenn und soweit nach § 46 Abs. 1 OWiG in Verbindung mit § 163b Abs. 2 StPO dies zur Aufklärung einer Straftat – oder vorliegend einer Ordnungswidrigkeit – geboten ist. Dies ist zum Beispiel der Fall, wenn im Zeitpunkt der Identitätsfeststellung konkrete Anhaltspunkte dafür bestehen, dass die Person als Zeuge benötigt wird. Vorliegend war zum Zeitpunkt der Identitätsfeststellung des betroffenen Beifahrers der Fahrzeugführer verdächtig, im Straßenverkehr ein Kraftfahrzeug geführt zu haben, obwohl er 0,25 mg/l oder mehr Alkohol in der Atemluft oder 0,5 Promille oder mehr Alkohol im Blut oder eine Alkoholmenge im Körper hatte, die zu einer solchen Atem- oder Blutalkoholkonzentration geführt habe, § 24a Abs. 1 StVG. Ich gehe davon aus, dass im Rahmen der Verkehrskontrolle ein Alkoholtest bei dem Fahrzeugführer durchgeführt wurde, der zu einem auffälligen Ergebnis führte. Beweismittel im Rahmen eines Verfahrens wegen Trunkenheitsfahrt gemäß § 24a Abs. 1 StVG sind eine beweissichere Atemalkoholanalyse und/oder Blutentnahme.

Fraglich ist, inwieweit bei dieser Sachlage der von der Identitätsfeststellung betroffene Beifahrer hinsichtlich einer Trunkenheitsfahrt be- oder entlastende Beweise als Zeuge hätte vorbringen können. Um den Sachverhalt abschließend

datenschutzrechtlich bewerten zu können, bat ich die PD um weitere Erläuterungen dazu, wie der Beifahrer als Zeuge zur Beweisgewinnung, -erhärtung oder -entkräftung hätte beitragen können. Bei Redaktionsschluss lag mir noch keine Erklärung der PD vor.

8.5 Weitergabe der auf beschlagnahmten Datenträgern befindlichen Daten zur Durchsicht und Auswertung an externe Stellen

↗ §§ 47, 62 BDSG; §§ 72, 78, 161a, 110, 500 StPO

Der Rechtsanwalt eines Petenten bat um eine datenschutzrechtliche Prüfung der Weitergabe von Daten von bei seinem Mandanten in einem strafprozessualen Ermittlungsverfahren beschlagnahmten Datenträgern zum Zweck der Durchsicht an eine Stelle außerhalb der Strafverfolgungsbehörden. Im Oktober 2022 sei ihm auf seinen Antrag auf Anwesenheit bei der Durchsicht der beschlagnahmten Datenträger durch die Polizei mitgeteilt worden, dass der gespiegelte Datenbestand zur Durchsicht an eine sächsische Hochschule abgegeben worden sei. Die zuständige Staatsanwaltschaft habe ihn im November 2022 darüber informiert, dass die Auswertung der gespiegelten Daten an die Hochschule ausgelagert worden sei, um aufgrund der großen Menge an verschiedensten Daten ein zeitnahes Ermittlungsergebnis zu erhalten. Dies sei kein unübliches Vorgehen, sondern entspreche bei derartigen Datenmengen der auch in anderen Verfahren geübten Praxis. Auf seine darauf ergangene Bitte um Übersendung der Verfügung der Weitergabe der Daten an die Hochschule habe ihm die Staatsanwaltschaft mitgeteilt, dass die Durchsicht der gesicherten Daten gemäß § 110 Strafprozessordnung (StPO) auf die Ermittlungspersonen übertragen worden sei und die entsprechende Zuleitungsverfügung der Polizei

zur Auswertung der gesicherten Daten durch die Hochschule Mittweida nicht vorliege. Auf den Hinweis des Anwalts darauf, dass an der Hochschule keine Ermittlungspersonen im Sinne von § 110 StPO tätig seien, und seine Bitte um Aufklärung sei ihm nochmalig Akteneinsicht gewährt und mitgeteilt worden, dass die Zuleitung der Asservate durch die Polizei an die Hochschule in Abstimmung mit der Staatsanwaltschaft anhand eines zuvor abgestimmten Umfanges und Zweckes der Auswertung erfolgt sei. Die neuerliche Akteneinsicht habe dem Anwalt allerdings keinerlei Erkenntnis darüber erbracht, wer die Zuleitung der Daten an die Hochschule verfügt hatte und auf welcher Rechtsgrundlage die Weitergabe erfolgte. Auf eine Nachfrage des Anwalts aus dem April 2023 sei nicht mehr reagiert worden.

Nachdem der Rechtsanwalt sich an mich gewandt hatte, bat ich die zuständige Staatsanwaltschaft im September 2023 unter Hinweis auf eine mögliche Auftragsverarbeitung nach § 500 StPO in Verbindung mit § 62 Bundesdatenschutzgesetz (BDSG) um Informationen zum Sachverhalt. Leider blieb diese Bitte, auch auf Erinnerung und den Hinweis auf die gesetzliche Pflicht zur Erteilung von Auskünften an mich (§ 40 Abs. 1 Sächsisches Datenschutz-Umsetzungsgesetz [SächsDSUG]), bis kurz vor Ende des Berichtszeitraums ohne Reaktion seitens der Staatsanwaltschaft. Kurz vor Ende des Kalenderjahres informierte mich die Staatsanwaltschaft dann darüber, dass die Weiterleitung der Daten an die Hochschule in der Verantwortung der Polizei gelegen habe, an die ich mich wegen der Einzelheiten der Auftragserteilung wenden möge. Die Voraussetzungen des § 500 Abs. 1 StPO lägen nach Ansicht der Staatsanwaltschaft nicht vor, da sich die Möglichkeit der Heranziehung von Dritten für die Durchsicht von Papieren und elektronischen Speichermedien nach ständiger Rechtsprechung bereits aus § 110 Abs. 1 StPO ergebe und nicht ersichtlich sei, dass der Gesetzgeber mit der erst 2019 durch Gesetz erfolgten Einführung des § 500 StPO für die strafprozessuale Erhebung, Verwendung und Verwertung personenbezogener Daten neue Anforderungen habe formulieren wollen.

Die Beschwerde und der Schriftwechsel mit der Staatsanwaltschaft geben Anlass, auf die Rechtslage hinzuweisen.
Nach meiner Beobachtung nimmt die Zahl der Beschlagnahmen von Datenträgern nach §§ 94, 98 StPO als Ermittlungsmaßnahme stetig zu. Die Maßnahme dürfte mittlerweile als Standardmaßnahme in Ermittlungsverfahren zur Anwendung kommen und zu einem großen Teil Mobiltelefone beschuldigter Personen betreffen.
In der Regel bezieht sich die Beschlagnahmeanordnung zunächst lediglich auf den Datenträger selbst, da vor einer Durchsicht nicht bekannt ist, welche der auf dem Datenträger befindlichen Daten verfahrensrelevant sind und ihrerseits als Beweismittel zu beschlagnahmen sind. Die Durchsicht der auf beschlagnahmten Datenträgern befindlichen Daten erfolgt nach § 110 StPO durch die Staatsanwaltschaft oder ihre Ermittlungspersonen.
Die Frage, ob mit der Durchsicht als eine für die Aufklärung einer Straftat zentrale Tätigkeit der Strafverfolgungsbehörden externe Stellen beauftragt werden dürfen, ist schon seit Langem gerichtlich geklärt. Es ist strafprozessual nicht unzulässig, seitens der Staatsanwaltschaft (private) Dritte zu Dienstleistungen im Ermittlungsverfahren heranzuziehen. Ist die Verantwortung für die Durchsicht durch Staatsanwälte oder Ermittlungspersonen sichergestellt, können Personen mit Spezialkenntnissen, etwa Dolmetscher, Sachverständige oder sonstige Dienstleister hinzugezogen werden. Beim Einsatz von Sachverständigen oder Dienstleistern darf es aber nicht zu einer „Privatisierung des Ermittlungsverfahrens" kommen, bei der Polizei und Staatsanwaltschaft nur noch formal in Erscheinung treten, was etwa der Fall wäre, wenn eine externe Person bei der Durchsicht selbstständig einen Rechner überprüft, alle für die weitere Untersuchung erforderlichen Feststellungen trifft und damit den weiteren Gang der Untersuchung bestimmt.
Der Gesetzgeber hat mit § 500 StPO und § 62 BDSG gesetzliche Regelungen zur Auftragsverarbeitung im Strafverfahren geschaffen, wobei strenge datenschutzrechtliche Vorgaben einzuhalten sind.

Die Weitergabe von Daten zur Durchsicht (und Auswertung) an Dritte im Ermittlungsverfahren ist im Wege der Beauftragung des Dritten als Sachverständigen (§ 161a Abs. 1 in Verbindung mit §§ 72 ff. StPO) oder der Auftragsverarbeitung denkbar (§ 500 StPO in Verbindung mit § 62 BDSG). Sachverständige gelten datenschutzrechtlich als eigene Verantwortliche im Sinne von Art. 4 Nummer 7 DSGVO und sind keine Auftragsverarbeiter im Sinne von § 62 BDSG.

Entgegen der Ansicht der Staatsanwaltschaft ist nicht § 110 StPO die rechtliche Grundlage für die Weitergabe von Daten zur Durchsicht an Dritte. § 110 StPO befugt die Staatsanwaltschaft und ihrer Ermittlungspersonen zur Durchsicht von Daten. Dass dabei auch (externe) Dritte herangezogen werden können, ist unstreitig; allerdings trifft § 110 StPO keinerlei Aussage zum Verfahren der Einbeziehung Dritter. Auf welche Art und Weise Dritte an Ermittlungen beteiligt werden, hat der Gesetzgeber etwa in §§ 72 ff. StPO (Sachverständige) oder in § 500 in Verbindung mit § 62 BDSG (Auftragsverarbeiter) bestimmt. Anlässe für die Beauftragung können vielfältig sein – die Durchsicht von Datenbeständen ist einer von vielen möglichen –, stets aber müssen die gesetzlichen Verfahrensregeln eingehalten werden. Eine der Staatsanwaltschaft möglicherweise vorschwebende „freihändige, formlose" Beauftragung externer Dritter ist nicht zulässig.

Bisweilen wirft die Abgrenzung zwischen der Tätigkeit als Sachverständiger, der über im Einzelfall für die Ermittlungen erforderliches individuelles Spezialwissen verfügt, und der eines bloßen Ermittlungshelfers (Auftragsverarbeiters), der über technische Möglichkeiten und Kapazitäten verfügt, Schwierigkeiten auf. Sie kann nicht allein anhand der Form und der Bezeichnung in der Beauftragung, sondern nur mittels Würdigung des Auftrags und der vorzunehmenden Handlungen des Dritten erfolgen und erlangt im Hinblick auf die Kostenfolgen für Beschuldigte bzw. verurteilte Täter Brisanz (Kosten für Sachverständige können dem Verurteilten gesondert auferlegt werden).

Die bloße Vornahme einer organisatorischen oder technischen Dienstleistung allein erfüllt nicht die Anforderungen an ein

Sachverständigengutachten, auch wenn hierfür umfangreiches Expertenwissen erforderlich sein mag und Ergebnisse in geeigneter Weise teils tabellarisch, teils auszugsweise sichtbar gemacht werden (vgl. Schleswig-Holsteinisches Oberlandesgericht, Beschluss vom 10. Januar 2017 – 2 Ws 441/16 (165/16) –, Rn. 11, 13 juris).

Mein Eindruck ist, dass in der Mehrheit der Fälle, in denen Strafverfolgungsbehörden (große) Datenbestände zur Durchsicht und gegebenenfalls Auswertung an externe Stellen weitergeben, Kapazitätsgründe der Ermittlungsbehörden eine zentrale Rolle spielen, weil für die – originär den Ermittlungsbehörden selbst zukommende – Aufgabe der Aufklärung des Sachverhalts behördlicherseits zu wenig Personal zur Verfügung steht. Eine Auslagerung der Durchsicht um, wie im vorliegenden Fall, aufgrund der großen Menge an verschiedensten Daten ein zeitnahes Ermittlungsergebnis zu erhalten, spricht eher für eine bloße Ermittlungshilfe bzw. Auftragsverarbeitung als für eine Sachverständigenbeauftragung.

§ 62 BDSG formuliert strenge Vorgaben für die Auftragsverarbeitung; Sinn und Zweck der Vorschrift ist unter anderem die Sicherstellung eines hohen Datenschutzniveaus auch dann, wenn Daten zu Strafverfolgungszwecken von (privaten) Stellen verarbeitet werden, die selbst nicht in den Anwendungsbereichen von Strafprozessordnung und dem 3. Teil des BDSG tätig werden. Insbesondere die Anforderungen in § 62 Abs. 5 BDSG zum Inhalt des Vertrags mit dem Auftragsverarbeiter sollen bei diesem ein Datenschutzniveau gewährleisten, das dem bei den zuständigen und verantwortlichen Strafverfolgungsbehörden entspricht. Der Vertrag ist schriftlich oder elektronisch abzufassen (§ 62 Abs. 6 BDSG).

Datenschutzrechtliche Vorgaben an Sachverständige finden sich in der Strafprozessordnung hingegen keine, was daran liegen mag, dass die Vorschriften über Sachverständige aus einer Zeit stammen, in der an Mobiltelefone und die heutige Rechentechnik noch nicht zu denken war und Sachverständige nicht mit der Durchsicht und Auswertung unter Umständen riesiger Datenmengen beauftragt wurden. Externe

Sachverständige werden in aller Regel den Vorschriften der DSGVO unterliegen und in diesem Rahmen ihre Verarbeitungshandlungen am Gutachtenauftrag ausrichten. Der den Auftrag erteilenden Stelle (Gericht, Staatsanwaltschaft, Polizei) kommt gemäß § 78 StPO eine Leitungsfunktion zu, die eine unmissverständliche Formulierung der vom Gutachter zu beantwortenden Beweisfrage erfordert. Teil der Leitungsfunktion ist die Vornahme aller gesetzlich vorgeschriebenen Belehrungen des Sachverständigen. Dies gilt sowohl im Hinblick auf vom Gutachter zu beachtende verfahrensrechtliche Vorgaben als auch bzgl. möglicher sachlich-rechtlicher Besonderheiten des Falles (vgl. BeckOK StPO/Monka, 49. Ed. 1.10.2023, StPO § 78 Rn. 3).

Im Ergebnis muss im Hinblick auf die Risiken bei der ermittlungsbehördlichen Weitergabe von großen Datenmengen an Stellen außerhalb der Staatsverwaltung und dem damit verbundenen (möglichst nur temporären) Verlust der tatsächlichen Einflussnahme auf die Verarbeitung der Daten auf dem einen wie auf dem anderen Wege sichergestellt werden, dass das für die Strafverfolgungsbehörden geltende Datenschutzniveau auch bei den externen Stellen – unabhängig davon, ob es sich um Sachverständige oder Auftragsverarbeiter handelt – eingehalten wird. Mit Blick auf die Masse und Art der personenbezogenen Daten, die heute üblicherweise etwa auf Mobiltelefonen gespeichert werden und – wie im Beschwerdefall – im Fall der Beauftragung Dritter mit der Durchsicht ungefiltert herausgegeben werden, wäre eine mit der Herausgabe verbundene Absenkung des Schutzes für die Beschuldigten und die in der Regel zahlreichen mitbetroffenen Dritten, deren Daten sich in den zu durchsuchenden Dateien befinden, mit den gesetzlichen Vorgaben von § 47 BDSG nicht in Einklang zu bringen. Mit anderen Worten: eine Arbeitsentlastung der Strafverfolgungsbehörden durch die Beauftragung externer (privater) Stellen darf nicht zulasten der (Grund-)Rechte der betroffenen Personen gehen.

In jedem Fall muss die Ausleitung von Daten an Dritte zum Zweck der Durchsicht für Ermittlungsverfahren dokumentiert werden, sei es durch einen Vertrag nach § 62 Abs. 5

Was ist zu tun?

Die Herausgabe personenbezogener Daten in Ermittlungsverfahren zur Durchsicht (und Auswertung) an externe Stellen birgt enorme datenschutzrechtliche Risiken. Sie ist im Wege der Auftragsverarbeitung oder, bei Vorliegen der Voraussetzungen, im Rahmen der Beauftragung eines Sachverständigengutachtens möglich. Die Weitergabe der Daten ist zu dokumentieren und darf nicht zur Absenkung des Datenschutzniveaus führen.

BDSG oder durch einen klar formulierten Sachverständigenauftrag einschließlich Belehrungen und Verpflichtungen. Die Beauftragung ist aktenkundig zu machen. Dass dies nach der Sachverhaltsschilderung des Rechtsanwalts vorliegend nicht der Fall war, ist ebenso bedenklich wie der Umstand, dass ihm auch seitens der Staatsanwaltschaft keine Rechtsgrundlage für die Weitergabe genannt wurde.

Ich werde mich im kommenden Berichtszeitraum an die Polizei wenden und prüfen, ob die Weitergabe des Datenbestandes zur Durchsicht und Auswertung an die Hochschule formal den gesetzlichen Anforderungen entsprach.

9 Rechtsprechung zum Datenschutz

9.1 Zum Begriff der „personenbezogenen Daten" – Urteil des EuG vom 26.04.2023, T-557/20 und EuGH vom 09.11.2023, C-319/22

↗ Art. 2 Abs. 1, 4 Nr. 1, 5 Abs. 1 DSGVO

Die Frage des relativen oder absoluten Begriffs des Personenbezugs ist eine altbekannte Kernfrage, die Datenschutzaufsichtsbehörden, Datenschutzbeauftragte, Juristinnen und Juristen beschäftigt, vgl. die Definition in Art. 4 Nr. 1 Datenschutz-Grundverordnung (DSGVO). Die absolute Theorie besagt, dass ein Datum personenbezogen sei, sobald ein Dritter – auch mittels Zusatzwissen – einen Personenbezug herstellen kann. Die relative Theorie wiederum stellt darauf ab, ob der Verantwortliche für das konkrete Datum tatsächlich und rechtlich Mittel zur Verfügung hat, die Herstellung eines Personenbezugs ermöglichen.

Die Frage ist so entscheidend, da sich mit der Bejahung des Tatbestandsmerkmals „personenbezogene Daten" erst der sachliche Anwendungsbereich der Datenschutz-Grundverordnung eröffnet, Art. 2 Abs. 1 DSGVO. In der Praxis wird meine Dienststelle dabei regelmäßig und typischerweise mit Bezügen konfrontiert, bei denen es entweder um die Speicherung vorgeblich anonymer Daten durch einen Verantwortlichen geht und um die Frage, ob ein Personenbezug nicht doch vorliegt, oder um arbeitsteilige Prozesse unter

Mitwirkung mehrerer Verantwortlicher mit Datenweitergaben, bei denen sich das Problem stellt, ob die Segmente der Datensätze, die weitergegeben bzw. empfangen werden, noch als personenbezogen einzustufen sind, bzw. auch häufig bei statistischen Fragen und Forschungsfragen. Nicht selten geht es in den beschriebenen Zusammenhängen auch um das grundlegendere Problem, ob die Daten personenbezogen überhaupt verarbeitet werden dürfen.

Ist meine Behörde in der aufsichtlichen Herangehensweise um eine objektivierte Sicht bemüht gewesen, um beide Theorien in den Entscheidungsüberlegungen zu berücksichtigen, weist die Datenschutz-Grundverordnung in den Erwägungsgründen auf einen praktischen Ansatz, was anzunehmende Mittel und Aufwand anbelangt, vgl. den Wortlaut von Erwägungsgrund 26 Satz 3 und 4 der DSGVO. Und auch zurückliegend – vor Wirksamwerden der Datenschutz-Grundverordnung – hatte sich der Europäische Gerichtshof (EuGH) im Zusammenhang mit dynamischen IP-Adressen mit der Frage auseinandergesetzt und bereits die rechtliche und praktische Durchführbarkeit der Herstellung des Personenbezugs durch den jeweiligen Verantwortlichen in den Mittelpunkt der Betrachtung gestellt, EuGH, Urteil vom 19. Oktober 2016, C 582/14.

Im letzten Berichtszeitraum zeichnete das Europäische Gericht (EuG), auch unter Bezugnahme auf die vorgenannte Entscheidung, die Rechtsgedanken unter Heranziehung des Erwägungsgrunds 16 nach, vgl. EuG, Urteil vom 26. April 2023, T-557/20, Rdnr. 91 ff. bzw. Rdnr. 87 ff. zu dem Erwägungsgrund zur Pseudonymisierung. In Bezug auf eine Entscheidung des Europäischen Datenschutzbeauftragten monierte das Gericht, dass sich die Datenschutzbehörde in ihrer Betrachtung zur Frage des Personenbezugs nicht konkret mit der Frage auseinandergesetzt habe, ob eine Rückidentifizierung durch einen Datenempfänger mit zusätzlichen Informationen des Datenübermittlers „vernünftigerweise" zur Identifizierung hätte erfolgen können bzw. „praktisch durchführbar" sein könnte, sondern einen Personenbezug der übermittelten Informationen „ungeprüft" – theoretisch – unterstellt habe, EuG, Urteil vom 26. April 2023, T-557/20, Rdnr. 103 ff. Die Entscheidung

ist noch nicht rechtskräftig. Der EuGH wird sich also mit der Frage nächstinstanzlich befassen. Eine weitergehende Klärung der Rechtsfrage ist zu erwarten.
Der EuGH hingegen hatte sich in seinem Urteil in einem Vorabentscheidungsverfahren vom 9. November 2023 - C-319/22 – schon zwischenzeitlich damit auseinanderzusetzen, ob es sich bei der Fahrzeugidentifikationsnummer (FIN) um ein personenbezogenes Datum nach der Datenschutz-Grundverordnung handelt. Der EuGH blieb aber auch in seinen Auslegungshinweisen zu der zu entscheidenden Frage gegenüber dem vorlegenden Landgericht Köln im Hinblick auf anzulegende Kriterien noch weitgehend allgemein, indem er ausführte:

> „Unter diesen Umständen handelt es sich bei der FIN um ein personenbezogenes Datum im Sinne von Art. 4 Nr. 1 DSGVO der in der Zulassungsbescheinigung ausgewiesenen Person, sofern derjenige, der Zugang zur FIN hat, über Mittel verfügen könnte, die es ihm ermöglichen, die FIN zur Identifizierung des Halters des Fahrzeugs, auf das sich die FIN bezieht, oder zur Identifizierung der Person, die aufgrund eines anderen Rechtstitels denn als Halter über das betreffende Fahrzeug verfügen kann, zu nutzen."

Was ist zu tun?
Verantwortlichen ist angesichts einer noch immer nicht eindeutigen Rechtslage anzuraten, in Zweifelsfällen zu hinterfragen, ob Mittel zur Verfügung stehen, um in Bezug auf zu verarbeitende Daten einen Personenbezug herzustellen und bestmögliche Maßnahmen durchzuführen, um den im Zweifel zu gewährleistenden Schutz der Datenschutz-Grundverordnung sicherzustellen, Art. 5 Abs. 1, insbesondere Buchst. c, e, f DSGVO. Stellt sich die grundlegendere Frage, ob die Informationen überhaupt personenbezogen verarbeitet werden dürfen, ist der/die Datenschutzbeauftragte zu beteiligen bzw. fachkundiger Rat einzuholen.

9.2 Verhängung von Bußgeldern gegen juristische Personen, EuGH – Urteil vom 05.12.2023, C-807/21

↗ Art. 58 Abs. 2 Buchst. i DSGVO, Art. 83 DSGVO

Mit Vorabentscheidungsersuchen wandte sich das in einer staatsanwaltlichen Beschwerde wegen der Zurückweisung eines Bußgeldbescheids zuständige Kammergericht Berlin an den Europäischen Gerichtshof (EuGH), der mit Urteil vom 5. Dezember 2023 entschied, Aktenzeichen C-807/21. Ausgangspunkt des Verfahrens war das von der Berliner Auf-

sichtsbehörde mit Bescheid verhängte hohe Bußgeld gegen einen Immobilienkonzern wegen der Archivierung von Mieterdaten ohne technische Vorsehung einer Löschung und mit mangelnder Überprüfung der Rechtmäßigkeit einer weitergehenden Speicherung.

Im Mittelpunkt der Vorlage stand die Rechtsfrage, ob die zuständige Datenschutzaufsichtsbehörde befugt ist, Bußgelder gegen Unternehmen zu verhängen, wenn keine konkrete natürliche Person für den Datenschutzverstoß auszumachen ist. Unter Auslegung von Art. 83 und Art. 58 Datenschutz-Grundverordnung (DSGVO) urteilte der Gerichtshof, dass der in Art. 4 Nr. 7 DSGVO definierte Begriff „Verantwortlicher" weit, „als die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet", zu verstehen sei, vgl. EuGH, Urteil vom 5. Dezember 2023, C-807/21, Rdnr. 39. Nach Wortlaut und dem Zweck von Art. 4 Nr. 7 DSGVO ergebe sich, dass der Verordnungsgeber bei der Bestimmung der Haftung nach der DSGVO nicht zwischen natürlichen und juristischen Personen unterschieden habe, da die einzige Voraussetzung für diese Haftung darin bestehe, dass jemand über Zweck und Mittel entscheide, siehe EuGH, a. a. O., Rdnr. 42. Die Zusammenschau von Art. 4 Nr. 7, Art. 83 und Art. 58 Abs. 2 Buchst. i DSGVO ergebe, „dass eine Geldbuße wegen eines Verstoßes gemäß Art. 83 Abs. 4 bis 6 DSGVO auch gegen juristische Personen verhängt werden kann, sofern sie die Eigenschaft eines Verantwortlichen haben. Dagegen gibt es in der DSGVO keine Bestimmung, die die Verhängung einer Geldbuße gegen eine juristische Person als Verantwortliche davon abhängig macht, dass zuvor festgestellt wird, dass dieser Verstoß von einer identifizierten natürlichen Person begangen wurde", vgl. EuGH, a. a. O., Rdnr. 46. Art. 58 Abs. 2 Buchst. i und Art. 83 Abs. 1 bis 6 DSGVO seien vielmehr dahin auszulegen, dass eine Geldbuße wegen eines in Art. 83 Abs. 4 bis 6 DSGVO genannten Verstoßes gegen eine juristische Person in ihrer Eigenschaft als Verantwortlicher nicht von der Feststellung eines Verstoßes einer identifizierten natürlichen Person abhängig

gemacht werden könne, vgl. EuGH, a. a. O., Rdnr. 60, 79. Auch werde, soweit es sich um eine juristische Person handele, für die Anwendung von Art. 83 DSGVO keine Handlung und nicht einmal eine Kenntnis seitens des Leitungsorgans dieser juristischen Person vorausgesetzt, vgl. EuGH, a. a. O., Rdnr. 77.

Die Entscheidung erleichtert insoweit in der Praxis nicht unwesentlich die Zurechnung eines zu sanktionierenden Verstoßes gegenüber dem Verantwortlichen, der eine juristische Person ist. Aufwendige bis hin zu nicht zu bewältigende Beweisführungen zum Ursprung des Verstoßes, einer Handlung oder eines Versäumnisses bzw. eine Zurechnung gegenüber der Geschäftsleitung sind seitens der Aufsichtsbehörde nach allem nicht verlangt, sondern eine sphärenbezogene Betrachtung kann im Einzelfall genügen.

Der Gerichtshof schränkt aber insoweit ein, dass Art. 83 DSGVO es nicht gestatte, eine Geldbuße wegen eines in Art. 83 Abs. 4 bis 6 genannten Verstoßes zu verhängen, ohne dass nachgewiesen sei, dass dieser Verstoß von dem Verantwortlichen vorsätzlich oder fahrlässig, mithin schuldhaft, begangen worden sei, vgl. EuGH, a. a. O., Rdnr. 75, 79. Eine Voraussetzung, die das Ordnungswidrigkeitenrecht ebenso festlegt.

Zur Frage des Mitarbeiterexzesses, bei dem es hingegen um die Frage der Verantwortlichkeit und Sanktionierung einzelner Beschäftigter oder Bediensteter geht: vgl. auch Tätigkeitsbericht 2021, 6.4.3., Seite 184 ff.

Tätigkeitsbericht 2021:
↗ sdb.de/tb2021

Was ist zu beachten?
Eine Bußgeldsanktionierung ist gegenüber juristischen Personen möglich, setzt jedoch Vorsatz oder Fahrlässigkeit voraus. Eine Schuldzurechnung des Verstoßes gegenüber konkreten Personen innerhalb einer Entität ist dabei nicht verlangt.

9.3 Scoring, Löschpflicht und Löschanspruch, EuGH-Urteile vom 07.12.2023, C-634/21 und C-26/22 bzw. C-64/22

↗ § 31 BDSG; Art. 5 Abs.1 Buchst. a, Art. 6 Abs. 1 Buchst. f, Art. 17, Art. 21 Abs. 1, Art. 22, Art. 78 Abs. 1 DSGVO

Der Europäische Gerichtshof (EuGH) urteilte in einer vielbeachteten Entscheidung, dass Art. 22 Abs. 1 Datenschutz-Grundverordnung (DSGVO) dahingehend auszulegen sei, dass

eine „automatisierte Entscheidung im Einzelfall" im Sinne der Vorschrift vorliege, „wenn ein auf personenbezogene Daten zu einer Person gestützter Wahrscheinlichkeitswert in Bezug auf deren Fähigkeit zur Erfüllung künftiger Zahlungsverpflichtungen durch eine Wirtschaftsauskunftei automatisiert erstellt wird, sofern von diesem Wahrscheinlichkeitswert maßgeblich abhängt, ob ein Dritter, dem dieser Wahrscheinlichkeitswert übermittelt wird, ein Vertragsverhältnis mit dieser Person begründet, durchführt oder beendet.", EuGH, Urteil vom 07.12.2023, C-634/21, Rdnr. 73 und 75.

Das vorlegende Verwaltungsgericht hatte sich mit einem Rechtsstreit wegen der Weigerung der hessischen Aufsichtsbehörde auseinanderzusetzen und dem klägerischen Begehren, gegenüber der SCHUFA Holding AG zu verfügen, dass diese der Auskunft und Löschung personenbezogener Daten nachzukommen habe, EuGH, a. a. O., Rdnr. 17 ff.

Nach der Entscheidung des Gerichtshofs ist es Unternehmen untersagt, ausschließlich auf Grundlage einer automatisierten Bewertung der Kreditwürdigkeit durch Auskunfteien zu entscheiden, ob sie Verträge mit Kundinnen oder Kunden abschließen, denn Art. 22 Abs. 1 DSGVO verleihe der betroffenen Person das „Recht", nicht „einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung" unterworfen zu werden. Diese Bestimmung stelle ein grundsätzliches Verbot auf, dessen Verletzung von betroffenen Personen nicht individuell geltend gemacht zu werden brauche, vgl. EuGH, a. a. O., Rdnr. 52.

Der Gerichtshof untersuchte auch die Vereinbarkeit von § 31 Bundesdatenschutzgesetz (BDSG) mit dem Unionsrecht und wies darauf hin, dass § 31 BDSG eine nationale Rechtsgrundlage im Sinne von Art. 22 Abs. 2 Buchst. b DSGVO darstellen könnte. Demnach müsste es sich bei § 31 aber um eine nationale Vorschrift handeln, die angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person vorsieht, wogegen der Gerichtshof „durchgreifende Bedenken" äußerte. Und, soweit die Bestimmung nicht mit der Datenschutz-Grundverordnung vereinbar sei, würde die Auskunftei „nicht nur ohne Rechts-

grundlage handeln, sondern verstieße ipso iure gegen das in Art. 22 Abs. 1 DSGVO aufgestellte Verbot", vgl. EuGH, a. a. O., Rdnr. 71. Dem vorlegenden Gericht sei insofern aufgegeben, zu prüfen, ob § 31 BDSG als Rechtsgrundlage im Sinne von Art. 22 Abs. 2 Buchst. b DSGVO qualifiziert werden könne, nach der es zulässig wäre, eine ausschließlich auf einer automatisierten Verarbeitung beruhende Entscheidung zu erlassen bzw. im Bejahensfall alle weiteren datenschutzrechtlichen Anforderungen erfüllt seien, EuGH, a. a. O., Rdnr. 72. Hinzuweisen ist im gesamten Zusammenhang auch auf den zu beachtenden ausführlichen Erwägungsgrund 71 der Verordnung.

Die Entscheidung hat nach den Ausführungen des Gerichtshofs nicht allein hohe Bedeutung für die Auskunfteien, sondern auch für Dienstleister und den Handel und deren Nutzung von Scoring-Informationen zur Entscheidungsfindung und Einschätzung von Zahlungsprognosen.

In einem weiteren Urteil vom 07. Dezember 2023, C-26/22 und C-64/22, das wiederum eine verwaltungsgerichtliche Vorlage und dieselbe Auskunftei und zwei Streitfälle mit der Datenschutzaufsichtsbehörde um Löschung von bei der Auskunftei gespeicherten Daten zu Restschuldbefreiungen zugunsten der Kläger betraf, positionierte sich der Europäische Gerichtshof grundlegend, was die Speicherung der sich existenziell auswirkenden bzw. stigmatisierenden Informationen betroffener Personen durch Auskunfteien anbelangt. Bei der Restschuldbefreiung, die den Abschluss eines Insolvenzverfahrens darstellt, werden dem Schuldner ab Entscheidungstag alle noch offenen Schulden erlassen, um einen wirtschaftlichen und sozialen Neubeginn zu eröffnen und sich erneut am Wirtschaftsleben zu beteiligen. Den Klägern wurde jeweils zurückliegend eine vorzeitige Restschuldbefreiung erteilt. Die nach den insolvenzrechtlichen Bestimmungen vorzunehmende öffentliche Bekanntmachung der gerichtlichen Beschlüsse im Internet wurde gesetzeskonform nach Ablauf von sechs Monaten, nachdem die Beschlüsse ergangen waren, gelöscht, vgl. EuGH, Urteil vom 07. Dezember 2023, C-26/22 und C-64/22, Rdnr. 25. Die Auskunftei berief sich im Hinblick auf die vorgesehene längere Speicherdauer auf gemäß Art. 40 DSGVO genehmig-

te Verhaltensregeln mit einer festgelegten Löschfrist von drei Jahren, vgl. EuGH, a. a. O., Rdnr. 44.

Der Europäische Gerichtshof untersuchte die ihm vorgelegte Kernfrage unter Zugrundelegung der für die Verarbeitung personenbezogener Daten in Betracht kommenden Rechtsgrundlage, Art. 6 Abs. 1 Buchst. f DSGVO, vgl. EuGH, a. a. O., Rdnr. 74. Nach der Bestimmung ist die Verarbeitung personenbezogener Daten nur rechtmäßig, wenn die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, vgl. den Wortlaut der Vorschrift. In der Abwägung entschied das Gericht im Ergebnis, dass Art. 5 Abs. 1 Buchst. a in Verbindung mit Art. 6 Abs. 1 Buchst. f DSGVO so auszulegen sei, dass „es einer Praxis privater Wirtschaftsauskunfteien entgegensteht, in ihren eigenen Datenbanken aus einem öffentlichen Register stammende Informationen über die Erteilung einer Restschuldbefreiung zugunsten natürlicher Personen zum Zweck der Lieferung von Auskünften über die Kreditwürdigkeit dieser Personen für einen Zeitraum zu speichern, der über die Speicherdauer der Daten im öffentlichen Register hinausgeht", vgl. EuGH, a. a. O., Rdnr. 113, 114.

Es bleibt zu ermessen, ob die Entscheidung, dass private Auskunfteien Daten zu Restschuldbefreiungen aus dem öffentlichen Register nicht länger zu speichern befugt sein sollen als die öffentlichen Bekanntmachungen, auf weitere ähnlich gelagerte Rechtsverhältnisse und Bezüge übertragbar ist.

Im Ergebnis urteilte der Gerichtshof zudem, im Hinblick auf eine der gerichtlichen Veröffentlichung entsprechende parallele – und damit die persönlichkeitsrechtliche Belastung vertiefende - Speicherung von sechs Monaten bei Auskunfteien, dass Art. 17 Abs. 1 Buchst. c DSGVO so auszulegen sei, dass die betroffene Person das Recht habe, vom Verantwortlichen die unverzügliche Löschung der sie betreffenden personenbezogenen Daten zu verlangen, wenn sie gemäß Art. 21 Abs. 1 dieser Verordnung Widerspruch gegen die Verarbeitung einlege und keine zwingenden schutzwürdigen Gründe vorliegen,

die ausnahmsweise die betreffende Verarbeitung rechtfertigen, vgl. EuGH, a. a. O., Rdnr. 109 f.
Im Übrigen – dies bezieht sich natürlich auch auf die längerdauernde Speicherung durch private Wirtschaftsauskunfteien – sei Art. 17 Abs. 1 Buchst. d DSGVO dahingehend auszulegen, dass der Verantwortliche verpflichtet sei, personenbezogene Daten, die unrechtmäßig verarbeitet wurden, unverzüglich zu löschen, vgl. EuGH, a. a. O., Rdnr. 114.
Die Kontrolle einer entsprechenden Umsetzung der Entscheidung des Europäischen Gerichtshofs bei Wirtschaftsauskunfteien in meiner datenschutzaufsichtlichen örtlichen Zuständigkeit behalte ich mir vor.
Neben den oben dargestellten grundsätzlichen und interessierenden datenschutzrechtlichen Fragen hat der Gerichtshof zudem in seinem Urteil klargestellt, dass Art. 78 Abs. 1 DSGVO dahin auszulegen sei, dass eine rechtsverbindliche Entscheidung einer Aufsichtsbehörde einer vollständigen inhaltlichen Überprüfung durch ein Gericht unterliege, EuGH, a. a. O., Rdnr. 70, 114; vgl. auch EuGH, a. a. O., Rdnr. 36. Dieser Spruchteil des Gerichtshofs wird meine Dienststelle in der verwaltungsgerichtlichen Praxis selbst unmittelbar betreffen (vgl. dazu auch 6.3.2).

Was ist zu beachten?
Unternehmen sind nicht befugt, ausschließlich auf Grundlage eines automatisierten Score-Werts zu entscheiden, ob sie Verträge mit Kunden abschließen. Entscheidungen unter Nutzung von Scoring-Berechnungen haben Anforderungen und Schranken von Art. 22 DSGVO zu genügen. Verantwortliche, private Auskunfteien, sind Daten aus den öffentlichen Bekanntmachungen zu Restschuldbefreiungen nicht länger zu speichern befugt, als die Bekanntmachung andauert. Aus einer Datenverarbeitung sich ergebende Löschvorschriften der DSGVO sind einzuhalten.

9.4 Anforderungen an nationale Regelungen zum Beschäftigtendatenschutz, EuGH, Urteil vom 30.03.2023, C-34/21

↗ § 11 Abs. 1 SächsDSG; § 26 BDSG; Art. 6 Abs. 1 Buchst. c und e, Art. 88 DSGVO

In einem Vorabentscheidungsverfahren, bei dem das Verwaltungsgericht Wiesbaden aufgrund rechtlicher Zweifel die Fragestellung der Vereinbarkeit der hessischen landesgesetzlichen Vorschrift zum Beschäftigtendatenschutz mit Art. 88 Abs. 1 Datenschutz-Grundverordnung (DSGVO) zur Vorlage gebracht hatte, entschied der Europäische Gerichtshof mit

Urteil vom 30. März 2023, C-34/21. Das Urteil hat weitergehende Bedeutung für die Rechtsetzung, auch in Sachsen, soweit es darauf hinweist, dass zu allgemein abgesetzte und auslegungsbedürftige Vorschriften des deutschen Beschäftigtendatenschutzes nicht mit den Vorgaben des Art. 88 DSGVO in Einklang zu bringen sind. Die Entscheidung in der der Vorlage zugrunde liegenden Sache unter Beachtung des genannten Verwaltungsgerichts steht noch aus.

Der Rechtsstreit entstand während der Corona-Pandemiephase im Wege der Einführung des vom zuständigen Kultusministerium verfügten Livestreamunterrichts per Videokonferenz an öffentlichen Schulen, bei der lediglich eine Einwilligung der Schülerinnen und Schüler bzw. deren Eltern, nicht aber durch die unterrichtenden Lehrerinnen und Lehrer vorgesehen war. Hiergegen erhob der Hauptpersonalrat Klage, das Verwaltungsgericht wandte sich an den EuGH, das beklagte Land berief sich auf die für den öffentlichen Dienst geltende beschäftigtendatenschutzrechtliche Vorschrift, die ähnlich wie § 11 Abs. 1 Sächsisches Datenschutzgesetz (SächsDSG) eine einwilligungsunabhängige Verarbeitung personenbezogener Daten der Bediensteten zur „Durchführung" des Beschäftigungsverhältnisses „… sowie zur Durchführung innerdienstlicher planerischer, organisatorischer, sozialer und personeller Maßnahmen …" soweit es „erforderlich" ist, erlaubt.

Die Öffnungsklausel des Art. 88 Abs. 1 DSGVO befugt die Mitgliedsstaaten „zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext" zur Gesetzgebung bereichsspezifischer Vorschriften. Anforderungen an die Rechtsetzung und die „spezifischeren Vorschriften" sind dabei in Absatz 2 festgelegt. Mit § 26 Bundesdatenschutzgesetz (BDSG) sowie den beschäftigungsrechtlichen Vorschriften der Landesdatenschutzgesetze haben deutsche Gesetzgeber die Öffnungsklausel der europarechtlichen Verordnung in Anspruch genommen.

In seiner Entscheidung stellte der Gerichtshof fest, dass nationale Vorschriften, um als „spezifischere Vorschrift" im Sinne von Art. 88 Abs. 1 DSGVO zu gelten, nicht lediglich „in

Art. 6 DSGVO genannten Bedingungen für die Rechtmäßigkeit der Verarbeitung personenbezogener Daten und der in Art. 5 DSGVO angeführten Grundsätze für diese Verarbeitung" bzw. Verweise auf diese oder um einen Verweis auf diese Bedingungen und Grundsätze enthalten dürfen, EuGH, Urteil vom 30. März 2023, C-34/21, Rdnr. 71.

Die Regeln müssten, um als „spezifischere Vorschriften" gelten zu können, die Vorgaben von Art. 88 Abs. 2 DSGVO erfüllen und sich von den „allgemeinen Vorschriften der DSGVO unterscheiden" und einen zu dem spezifischen Bereich „passenden Regelungsgehalt" aufweisen, der von dem der DSGVO zu differenzieren sei. Regeln hätten „auf den Schutz der Rechte und Freiheiten der Beschäftigten hinsichtlich der Verarbeitung ihrer personenbezogenen Daten im Beschäftigungskontext" abzuzielen, und es sei auf besondere Maßnahmen zur Grundrechtewahrung zu achten und „insbesondere Transparenz der Verarbeitung, die Übermittlung personenbezogener Daten innerhalb einer Unternehmensgruppe oder einer Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, und die Überwachungssysteme am Arbeitsplatz" zu regeln, EuGH, Urteil vom 30. März 2023, C-34/21, vgl. jeweils Rdnr. 74.

Unter Bezugnahme auf den Generalanwalt, der von keiner spezifischeren Vorschrift im Sinne von Art. 88 DSGVO ausgegangen ist, EuGH, a. a. O., Rdnr. 81, und unter Rückgriff auf den Grundsatz des Vorrangs des Unionsrechts, EuGH, a. a. O., Rdnr. 83, geht der Gerichtshof davon aus, dass die landesdatenschutzgesetzliche Bestimmung, soweit die Voraussetzungen des Art. 88 nicht als erfüllt anzusehen sind, unangewendet bleibt. Es sei dann zu prüfen, ob die landesdatenschutzgesetzliche Vorschrift insbesondere über den dann unmittelbar geltenden Art. 6 Abs. 1 Buchst. c, e DSGVO weiter anwendbar sei, Rdnr. 84 ff.

Zunächst hat die Entscheidung, die sich auf eine Vorschrift aus dem hessischen Datenschutzrecht bezieht, keine unmittelbare Tragweite für den Freistaat Sachsen. Die Vorschrift des § 11 Sächsisches Datenschutzgesetz ist anders strukturiert als die des im Verfahren gegenständliche, aber zum

Was ist zu tun?
Die Kritik des Europäischen Gerichtshofs an der Rechtsetzung kann und sollte auch der sächsische Gesetzgeber bzw. die Staatsregierung aufgreifen und als Anstoß nehmen, um sich der Thematik des Beschäftigtendatenschutzes eingehender zu widmen und entsprechende Gesetzgebung zu koordinieren und vorzubereiten.

Teil auch allgemein gehalten, vgl. insbesondere Absatz 1 des § 11 SächsDSG. Dennoch wird die Entscheidung des EuGH nach meiner Überzeugung Auswirkungen auf die Gesetzgebung haben, zumal die hessische Vorschrift zu § 26 Bundesdatenschutzgesetz (BDSG) fast inhaltsgleich ist. Und die Bundesvorschrift ist auch Grundlage der Datenverarbeitung sächsischer Arbeitgeberinnen und Arbeitgeber. So bestärkt mich die EuGH-Rechtsprechung weiter in meiner Auffassung, dass die Notwendigkeit besteht, ein bestandsfähiges Beschäftigtendatenschutzgesetz zu schaffen, was auch die Datenschutzkonferenz zuletzt wieder im April 2022 gefordert hatte.

9.5 Auslegung von Art. 15 Abs. 3 Satz 1 in Verbindung mit Art. 12 Abs. 5 und Art. 23 Abs. 1 DSGVO

Mit Urteil in der Rechtssache C-307/22 hat der Europäische Gerichtshof (EuGH) zur Auslegung des Art. 15 DSGVO Stellung bezogen:
Im zugrunde liegenden Verfahren vor dem Bundesgerichtshof (BGH) verlangt ein Patient von der ihn behandelnden Ärztin eine Kopie seiner Patientenakte zur Prüfung von Haftungsfehlern während seiner Behandlung und beruft sich dabei auf Art. 15 Abs. 3 Datenschutz-Grundverordnung (DSGVO). Die betreffende Zahnärztin forderte, dass der Patient, wie nach § 630g Bürgerliches Gesetzbuch (BGB) vorgesehen, die Kosten für die Zurverfügungstellung der Kopie der Patientenakte übernimmt.
Der BGH hatte dem EuGH bezüglich der Reichweite des unionsrechtlichen Anspruchs des Patienten gegen den behandelnden Arzt auf kostenfreie Zurverfügungstellung einer ersten Kopie seiner in der Patientenakte verarbeiteten personenbezogenen Daten nach Art. 15 Abs. 3 DSGVO sowie der Möglichkeit einer Beschränkung dieses Anspruchs durch

§ 630g Abs. 2 Satz 2 BGB mit Beschluss vom 29.3.2022 unter anderem folgende Fragen zur Entscheidung vorgelegt:

- Ist Art. 15 Abs. 3 Satz 1 in Verbindung mit Art. 12 Abs. 5 DSGVO dahingehend auszulegen, dass der Verantwortliche (hier: der behandelnde Arzt) nicht verpflichtet ist, dem Betroffenen (hier: dem Patienten) eine erste Kopie seiner vom Verantwortlichen verarbeiteten personenbezogenen Daten unentgeltlich zur Verfügung zu stellen, wenn der Betroffene die Kopie nicht zur Verfolgung der in Erwägungsgrund 63 Satz 1 zur DSGVO genannten Zwecke begehrt, sondern einen anderen - datenschutzfremden, aber legitimen – Zweck, hier: die Prüfung des Bestehens arzthaftungsrechtlicher Ansprüche, verfolgt?
- Ist Art. 23 Abs. 1 Buchst. i DSGVO dahingehend auszulegen, dass die dort genannten Rechte und Freiheiten anderer Personen auch deren Interesse an der Entlastung von mit der Erteilung einer Datenkopie nach Art. 15 Abs. 3 Satz 1 DSGVO verbundenen Kosten und sonstigem durch die Zurverfügungstellung der Kopie verursachten Aufwand umfassen?
- Umfasst der Anspruch aus Art. 15 Abs. 3 Satz 1 DSGVO im Arzt-Patienten-Verhältnis einen Anspruch auf Überlassung von Kopien aller die personenbezogenen Daten des Patienten enthaltenden Teile der Patientenakte oder ist er nur auf Herausgabe einer Kopie der personenbezogenen Daten des Patienten als solche gerichtet, wobei es dem datenverarbeitenden Arzt überlassen bleibt, in welcher Weise er dem betroffenen Patienten die Daten zusammenstellt?

Hierzu hat der EuGH mit Urteil vom 26.10.2023 wie folgt entschieden:

1. Art. 12 Abs. 5 sowie Art. 15 Abs. 1 und 3 DSGVO sind dahin auszulegen, dass die Verpflichtung des Verantwortlichen, der betroffenen Person unentgeltlich eine erste Kopie ihrer personenbezogenen Daten, die Gegenstand einer Verarbeitung sind, zur Verfügung

zu stellen, auch dann gilt, wenn der betreffende Antrag mit einem anderen als den in Satz 1 des 63. Erwägungsgrundes der DSGVO genannten Zwecken begründet wird.

2. Art. 23 Abs. 1 Buchst. i DSGVO ist dahin auszulegen, dass eine nationale Regelung, die vor dem Inkrafttreten dieser Verordnung erlassen wurde, in den Anwendungsbereich dieser Bestimmung fallen kann. Eine solche Möglichkeit erlaubt es jedoch nicht, eine nationale Regelung zu erlassen, die der betroffenen Person zum Schutz der wirtschaftlichen Interessen des Verantwortlichen die Kosten für eine erste Kopie ihrer personenbezogenen Daten, die Gegenstand der Verarbeitung durch den Verantwortlichen sind, auferlegt.
3. Art. 15 Abs. 3 Satz 1 DSGVO ist dahin auszulegen, dass im Rahmen eines Arzt-Patienten-Verhältnisses das Recht auf Erhalt einer Kopie der personenbezogenen Daten, die Gegenstand einer Verarbeitung sind, umfasst, dass der betroffenen Person eine originalgetreue und verständliche Reproduktion aller dieser Daten überlassen wird. Dieses Recht setzt voraus, eine vollständige Kopie der Dokumente zu erhalten, die sich in der Patientenakte befinden und unter anderem diese Daten enthalten, wenn die Zurverfügungstellung einer solchen Kopie erforderlich ist, um der betroffenen Person die Überprüfung der Richtigkeit und Vollständigkeit der Daten zu ermöglichen und die Verständlichkeit der Daten zu gewährleisten. In Bezug auf die Gesundheitsdaten der betroffenen Person schließt dieses Recht jedenfalls das Recht ein, eine Kopie der Daten aus ihrer Patientenakte zu erhalten, die Informationen wie beispielsweise Diagnosen, Untersuchungsergebnisse, Befunde der behandelnden Ärzte und Angaben zu an ihr vorgenommenen Behandlungen oder Eingriffen umfasst.

Zusammengefasst kommt der EuGH somit zu folgendem Ergebnis:
Gemäß Art. 15 Abs. 3 DSGVO hat ein Patient das Recht, eine erste Kopie seiner Patientenakte vom behandelnden Arzt zu erhalten, und zwar grundsätzlich ohne dass ihm hierdurch Kosten entstehen. Selbst mit Blick auf den Schutz der wirtschaftlichen Interessen der Behandelnden dürfen die nationalen Regelungen dem Patienten nicht die Kosten einer ersten Kopie seiner Patientenakte auferlegen. Der Verantwortliche (Arzt) kann ein solches Entgelt nur dann verlangen, wenn der Patient eine erste Kopie seiner Daten bereits unentgeltlich erhalten hat und erneut einen Antrag auf diese stellt.
Der Patient ist nicht verpflichtet, seinen Antrag zu begründen, also die Motive für sein Auskunftsbegehren offenzulegen.
Der Patient hat das Recht, eine vollständige, originalgetreue Kopie der Dokumente zu erhalten, die sich in seiner Patientenakte befinden, wenn dies zum Verständnis der in diesen Dokumenten enthaltenen personenbezogenen Daten erforderlich ist. Dies schließt Daten aus der Patientenakte ein, die Informationen wie beispielsweise Diagnosen, Untersuchungsergebnisse, Befunde der behandelnden Ärzte und Angaben zu Behandlungen oder Eingriffen enthalten.

Was ist zu tun?
Patientinnen und Patienten haben grundsätzlich das Recht – kostenlos und ohne dies näher begründen zu müssen –, eine Kopie ihrer medizinischen Akte zu bekommen.

9.6 Rücknahme der Klage gegen meine Anordnung auf Erteilung einer kostenlosen Kopie der Patientenakte nach Art. 15 Abs. 3 DSGVO

↗ § 630g BGB; Art. 15, Art. 58 Abs. 1 Buchst. c DSGVO

Im Rahmen einer Petition wurde Anfang 2019 gerügt, dass ein Klinikum dem Antrag der Petenten nach Art. 15 Abs. 3 Datenschutz-Grundverordnung (DSGVO) auf Erteilung einer kostenlosen Kopie der Patientenakte der Mutter und der ihres

Kindes nicht nachkomme. Das Klinikum war leider auch nach mehrmaligen Aufforderungen nicht bereit, eine kostenlose Kopie der beiden Patientenakten zur Verfügung zu stellen.

Das Klinikum ordnete den Anspruch der Petenten § 630g Bürgerliches Gesetzbuch (BGB) zu. Zur Begründung wurde angeführt, dass zwischen Art. 15 Abs. 3 DSGVO und § 630g BGB differenziert werden müsse. Ausschlaggebend sei der Normzweck. Die Petenten begehrten aus Sicht des Klinikums in der Sache keine Datenüberlassung zum Zwecke der Prüfung der ordnungsgemäßen Datenverarbeitung. Sie forderten eine Kopie der Patientenakte. Diesem Zweck trage gerade und ausschließlich § 630g BGB Rechnung. Es solle dem Patienten das Recht zustehen, Kopien seiner vollständigen Patientenakte kostenpflichtig zu erlangen. Art. 15 DSGVO hingegen verfolge den Zweck, dass dem Patienten ermöglicht werden soll, die Richtigkeit der Verarbeitung seiner Daten zu überprüfen. Es sei das Begehr des Patienten zu prüfen und danach zu differenzieren. Da die Petenten zur Sicherung der weiteren Behandlung jeweils eine Kopie der Patientenakte erhalten möchten, falle dieses Begehr unter § 630g BGB. Weiter führte das Klinikum aus, dass Art. 15 Abs. 4 DSGVO darüber hinaus die Bedingung stelle, dass keine Rechte Dritter beeinträchtigt werden dürfen. Unabhängig vom Datenschutzrecht seien auch die Bestimmungen des § 203 Strafgesetzbuch (StGB) von Belang. Dies stünde der Überlassung einer Kopie der beiden Patientenakten entgegen. Die Herausgabe würde auch die Rechte von Erfüllungsgehilfen des Arztes berühren zum Beispiel bei Medikamentengaben in den Pflegedokumenten durch Personen des Pflegebereichs.

Nach der rechtlichen Einschätzung des Klinikums konkretisiert Art. 15 Abs. 3 lediglich Art. 15 Abs. 1 DSGVO in der Gestalt, dass der Auskunftsanspruch durch die Überlassung der Daten in Form einer Kopie erfüllt werden soll, so dies möglich ist. Art. 15 Abs. 1 DSGVO lege den Umfang des Anspruchs abschließend fest. Hinzu käme, dass das Klinikum tagtäglich eine enorme Daten- und Informationsmenge, insbesondere Patientendaten, verarbeite. Zur Wahrnehmung des Auskunftsanspruchs werde beim Klinikum zusätzliches Per-

sonal benötigt. Dies stelle aufgrund eines enorm komplexen Krankenhausinformationssystems und einer Vielzahl von unterschiedlich verarbeiteten Daten und Verarbeitungsstellen einen hohen Zeitaufwand dar. Weiter wurde dargelegt, dass der Aufwand für einen Anspruch gemäß § 630g BGB ähnlich hoch sein könne, allerdings würde hier eine Abgeltung durch Aufwandsentschädigung erfolgen und dem dadurch entstandenen Aufwand Rechnung getragen werden.

Mit einer Anordnung nach Art. 58 Abs. 1 Buchst. c DSGVO wurde das Klinikum angewiesen, dem Antrag der Petenten auf Gewährung einer kostenlosen Kopie der beiden Patientenakten nach Art. 15 DSGVO nachzukommen. Die vorgenannten Argumente des Klinikums wurden von mir wie folgt zurückgewiesen:

Nach Art. 15 Abs. 3 DSGVO stellt der Verantwortliche eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung. In Bezug auf die personenbezogenen Daten, die Gegenstand des Art. 15 Abs. 3 DSGVO sind, besteht bei der Patientenakte die Besonderheit, dass alle Daten, nicht nur die Stammdaten der Patientenakte, personenbezogen sind, da sich diese – hier die Informationen über die Gesundheit – auf den betroffenen Patienten beziehen. Es handelt sich damit um einen Anspruch auf eine vollständige Kopie der Patientenakte.

Dem Patienten ist, wenn er seinen Antrag auf Art. 15 Abs. 3 DSGVO stützt, eine vollständige Kopie seiner Patientenakte zu gewähren.

Art. 15 Abs. 4 DSGVO steht nicht entgegen. Die beiden Patientenakten betreffen die Mutter und ihr Kind. Rechte und Freiheiten anderer Personen im Sinne des Erwägungsgrunds 63, Satz 7 zur DSGVO, der zum Beispiel Geschäftsgeheimnisse anführt, sind dadurch nicht beeinträchtigt. Art. 15 Abs. 4 DSGVO liegt hier nicht vor. § 203 StGB liegt ebenfalls nicht vor.

Gegen die Anordnung hat das Klinikum im Juli 2021 Klage beim Verwaltungsgericht Dresden erhoben.

Nach richterlichem Hinweis auf die Entscheidung des EuGH vom 26. Oktober 2023, Az.: C-307/22, (siehe dazu auch 9.5) hat das Klinikum Ende November 2023 die Klage zurückge-

Was ist zu tun?
Einer Patientin oder einem Patienten ist bei einem Antrag nach Art. 15 Abs. 3 DSGVO eine kostenlose Kopie der vollständigen Patientenakte zu erteilen.

nommen. Das Verwaltungsgericht Dresden hat hierauf mit Beschluss vom 15. Dezember 2023 das Verfahren eingestellt. Es ist zu hoffen, dass das Klinikum nunmehr zeitnah seiner Verpflichtung nachkommt und den Petenten die streitgegenständlichen Patientendokumente in Kopie übermittelt. Ich werde dies weiter kritisch verfolgen.

Notizen

Herausgeberin
Sächsische Datenschutz- und Transparenzbeauftragte
Dr. Juliane Hundert
Devrientstraße 5, 01067 Dresden

Kontakt
Postanschrift: Postfach 11 01 32, 01330 Dresden
Telefon 0351 85471-101
Telefax 0351 85471-109
post@sdtb.sachsen.de
www.datenschutz.sachsen.de
Folgen Sie der SDTB auch auf Mastodon: social.sachsen.de/@sdtb

Fotos
© peshkova – stock.adobe.com
Weitere Fotos: ronaldbonss.com (Seite 5), SDTB (Seite 231), Jan Ziegler (Seite 233)

Druck
siblog – Gesellschaft für Dialogmarketing, Fulfillment & Lettershop mbH

Auflage
1.500 Exemplare

Veröffentlichung
April 2024

Bezug
kostenlos
Zentraler Broschürenversand der Sächsischen Staatsregierung
Hammerweg 30, 01127 Dresden
Telefon: 0351 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 Kandidaten oder 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.