Tätigkeitsbericht Datenschutz

Berichtszeitraum:
1. Januar bis 31. Dezember 2024

Meine Daten.
Meine Freiheit.

SÄCHSISCHE
DATENSCHUTZ- UND
TRANSPARENZBEAUFTRAGTE

Freistaat
SACHSEN

Tätigkeitsbericht Datenschutz 2024 der Sächsischen Datenschutz- und Transparenzbeauftragten

Berichtszeitraum:
1. Januar bis 31. Dezember 2024

Rechtsstand: 31. Dezember 2024

Liebe Leserinnen und Leser,

Datenschutz ist eine Aufgabe, bei der es auch darum geht, die Zukunft zu gestalten. Die heute verarbeiteten personenbezogenen Daten werden vielleicht morgen schon für andere Zwecke verwendet – mit unüberschaubaren Folgen für betroffene Personen. Besonders gut sichtbar wird das bei disruptiven Technologien wie der Künstlichen Intelligenz. Sie birgt enorme Chancen für Wirtschaft und Gesellschaft. Ohne Kontrolle verfügt sie jedoch über ein ebenso hohes Risiko für unsere Freiheitsrechte. Im Jahr 2024 war ich daher nicht nur als Mitglied der Datenschutzkonferenz grundlegend mit den aktuellen Entwicklungen rund um KI befasst: So zum Beispiel mit der KI-Verordnung, die die EU-Mitgliedstaaten beschlossen haben, oder mit der Nutzung von KI in den sächsischen Schulen (1.3) und der Verwaltung (1.2).

In Europa leben wir glücklicherweise mit der Errungenschaft, dass Datenschutz in der EU-Grundrechtecharta verankert ist. Er darf damit nicht einfach übergangen und somit den KI-Unternehmen oder der Datenökonomie überlassen werden – selbst wenn die uneingeschränkte Verwertung und der Handel mit unseren persönlichen Informationen sehr lukrativ erscheint. Umso wichtiger ist es, dass der Rechtsrahmen von KI weiter konkretisiert wird, damit Verantwortliche und Betroffene die Möglichkeiten und Grenzen kennen.

Mit der KI-Verordnung, dem weltweit ersten Gesetz zur KI-Regulierung, hat Europa eine essenzielle Grundlage für den grundrechtsorientierten Umgang mit dieser Schlüsseltechnologie geschaffen. Für Deutschland gilt es nun, diese Verordnung in nationales Recht zu überführen und damit unter anderem auch die Frage der Aufsicht zu klären. Die Datenschutzkonferenz hatte sich frühzeitig mit einem Vorschlag eingebracht, der die Bündelung von KI- und Datenschutzaufsicht beinhaltete. Zudem hat sie eine Orientierungshilfe zur datenschutzkonformen Nutzung herausgegeben, an deren Erstellung ich mit meiner Behörde ebenfalls mitgewirkt habe (7.3).

Mit Künstlicher Intelligenz habe ich mich also ausgiebig befasst, und dieses Thema wird alle Datenschutzaufsichtsbehörden weiterhin beschäftigen – zumal sich durch den technischen Fortschritt neue Einsatzmöglichkeiten ergeben, beispielsweise für die Arbeit der sächsischen Polizei. Im Berichtszeitraum sorgte die automatisierte Gesichtserkennung in Strafverfahren für Aufsehen. Das Personen-Identifikations-System PerIS ermöglicht der Polizei einen biometrischen Liveabgleich der Aufnahmen mit Referenzbildern. Meine kritische Einschätzung und was nun zu tun ist, finden Sie gleich zu Beginn meines Berichts (1.1).

Keinesfalls weniger relevant – gemessen an der Anzahl der Betroffenen – ist Tracking im Internet. Oftmals im Verborgenen, von Nutzerinnen und Nutzern unbemerkt, werden die eigenen Daten beim Aufruf von Websiten an Drittanbieter übermittelt bzw. Cookies zur Nachverfolgung gesetzt. Was mit den Daten passiert, bleibt in der Regel nebulös. Ein häufiges Szenario: Unternehmen verketten die Informationen zu digitalen Personenakten, die nach und nach immer genauere virtuelle Abbilder unserer Persönlichkeit ergeben. Auch hierbei kommt mittlerweile KI-Technologie zum Einsatz. Anschließend verkaufen Datenbroker diese Profile an Dritte. In verhältnismäßig harmlosen Fällen erhalten wir „nur" auf uns zugeschnittene Werbung. Im schlimmsten Fall missbrauchen Kriminelle die virtuellen Profile für Straftaten.

Um einen Überblick zu erhalten, wie es um den Datenschutz auf sächsischen Websites bestellt ist, habe ich mehr als 30.000 Internetauftritte überprüft – und eine Vielzahl an Verstößen festgestellt. Die gute Nachricht: Sehr viele Website-Betreiber/innen betreiben ihre Website datenschutzkonform oder haben nach meiner Intervention nachgebessert (1.4, 1.5).

Darüber hinaus verzeichnete ich 2024 eine Reihe an weiteren, bemerkenswerten Vorgängen, die im Zusammenhang mit Internetdiensten standen. Dazu gehörte unter anderem die anlasslose Prüfung eines Onlinehändlers für Consumer-Elektronik (4.1.1), der rechtskonforme Umgang mit Gastzugängen im E-Commerce (4.1.2) oder die Veröffentlichung von Übersichtsbildern von Ansammlungen auf Social-Media-Kanälen der Polizei (8.6).

Obwohl Onlinedienste recht häufig eine Rolle bei Eingaben spielen, soll keinesfalls der Eindruck entstehen, dass sich in der „Offline-Welt" weniger Datenschutzverstöße ereignen. Nach wie vor begegnen mir in vielfältiger Ausprägung auch die „Klassiker". Zu denen zählt der Beschäftigtendatenschutz, etwa, wenn in Belegschaftsversammlungen das Management über Kündigungsgründe oder ärztliche Diagnosen von Angestellten spricht (1.6). Ein Dauerbrenner im kommunalen Datenschutz ist der Umgang mit personenbezogenen Daten durch Gemeinderätinnen und -räte im Rahmen ihrer Ratsarbeit (2.1.17). Weiterhin ebbten die Vorgänge zu Videoüberwachungen nicht ab. Sowohl bei öffentlichen Stellen (2.1.9) als auch im privatwirtschaftlichen Bereich (6.4.2) versprechen sich Verantwortliche mehr Sicherheit durch Kameras und verletzen mitunter die Persönlichkeitsrechte der Betroffenen.

Ob online oder offline: Datenschutz schützt keine Daten, sondern Menschen, und wenn es um Menschen geht, ist immer Bewegung drin. Ich hoffe, dass auch dieser Tätigkeitsbericht einen wertvollen Beitrag dazu leistet, das Recht auf informationelle Selbstbestimmung zu bewahren. Mit den nachfolgend veröffentlichten Beiträgen möchte ich Ihnen, liebe Leserinnen und Leser, nicht nur einen Eindruck von meiner Arbeit vermitteln, sondern auch auf Fehler, Schwachstellen und Lösungen im Umgang mit personenbezogenen Daten hinweisen.

Weitere Informationen erhalten Sie ebenso auf datenschutz.sachsen.de sowie auf meinem Profil beim Kurznachrichtendienst Mastodon unter social.sachsen.de/@sdtb. Die Instanz social.sachsen.de stelle ich auch anderen öffentlichen Stellen für ihre Öffentlichkeitsarbeit zur Verfügung (6.5.1). Wer sich privat ein Mastodon-Profil einrichten und darüber kommunizieren möchte, kann dafür eine der zahlreichen freien Instanzen nutzen.

Ich wünsche Ihnen eine aufschlussreiche Lektüre.

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

AO	Abgabenordnung
BDSG	Bundesdatenschutzgesetz
BGB	Bürgerliches Gesetzbuch
BKA	Bundeskriminalamt
BKAG	Bundeskriminalamtgesetz
DSGVO	Datenschutz-Grundverordnung
EFZG	Entgeltfortzahlungsgesetz
EG	Erwägungsgrund
GG	Grundgesetz für die Bundesrepublik Deutschland
IfSG	Infektionsschutzgesetz
MStV	Medienstaatsvertrag
OWiG	Gesetz über Ordnungswidrigkeiten
PAuswG	Personalausweisgesetz
SächsBG	Sächsisches Beamtengesetz
SächsBO	Sächsische Bauordnung
SächsDG	Sächsisches Disziplinargesetz
SächsDSDG	Sächsisches Datenschutzdurchführungsgesetz
SächsDSG	Sächsisches Datenschutzgesetz
SächsDSUG	Sächsisches Datenschutz-Umsetzungsgesetz
SächsEGovG	Sächsisches E-Government-Gesetz
SächsGemO	Sächsische Gemeindeordnung
SächsHSG	Sächsisches Hochschulgesetz
SächsLKrO	Sächsische Landkreisordnung
SächsPVDG	Sächsisches Polizeivollzugsdienstgesetz
SächsStVollzG	Sächsisches Strafvollzugsgesetz
SächsVerf	Verfassung des Freistaates Sachsen
SächsVermKatG	Sächsisches Vermessungs- und Katastergesetz
SächsVersG	Sächsisches Versammlungsgesetz

SächsVSG	Sächsisches Verfassungsschutzgesetz
SGB	Sozialgesetzbuch
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
TDDDG	Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz
TTDSG	Telekommunikation-Telemedien-Datenschutz-Gesetz
UAusschG	Untersuchungsausschußgesetz
UhVorschG	Unterhaltsvorschussgesetz
UWG	Gesetz gegen den unlauteren Wettbewerb
VwGO	Verwaltungsgerichtsordnung
VwVfG	Verwaltungsverfahrensgesetz
ZPO	Zivilprozessordnung

Sonstiges

a. a. O.	am angegebenen Ort
Abs.	Absatz
AIS	Adaptives Intelligentes System (AIS)
Alt.	Alternative
Art.	Artikel
Az.	Aktenzeichen
BGH	Bundesgerichtshof
BLAG	Bund-Länder-Arbeitsgruppe
BT-Drs.	Bundestagsdrucksache
Buchst.	Buchstabe
BVerfG	Bundesverfassungsgericht
BVerfGE	Bundesverfassungsgerichtsentscheidung
BVerwG	Bundesverwaltungsgericht
BVerwGE	Bundesverwaltungsgerichtsentscheidung
DAD	DNA-Analyse-Datei
DPC	Data Protection Commission
DSK	Konferenz der unabhängigen Datenschutzbeauftragten des Bundes und der Länder – Datenschutzkonferenz
EDSA	Europäischer Datenschutzausschuss
EU	Europäische Union
EuGH	Europäischer Gerichtshof
IMI	Internal Market Information System
ITS	Intelligentes Tutorielles System

JVA	Justizvollzugsanstalt
KI	Künstliche Intelligenz
LaSuB	Landesamt für Schule und Bildung
LfV	Landesamt für Verfassungsschutz
LG	Landgericht
LPP	Landespolizeipräsidium
LT-Drs.	Landtagsdrucksache
NPS	Neue psychoaktive Substanzen
OLG	Oberlandesgericht
OVG	Oberverwaltungsgericht
PD	Polizeidirektion
PerIS	Personen-Identifikations-System
Rn.	Randnummer
SächsVerfGH	Sächsischer Verfassungsgerichtshof
SMI	Sächsisches Staatsministerium des Innern
VerfGH NRW	Verfassungsgerichtshof für das Land Nordrhein-Westfalen
VG	Verwaltungsgericht
VwV	Verwaltungsvorschrift
ZASt	Zentrale Anlaufstelle

Sachgebietsregister

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

Handel, Dienstleistungen, Gewerbe, Industrie	
• Auskunfteien, Inkassodienstleister, Detekteien	
• Banken, Finanzwirtschaft	
• Handel, siehe auch Internet/E-Commerce	2.1.6
• Handwerk, Gewerbe, Industrie	
• Hotel und Gastronomie, Freizeit, Tourismus, Sport	vgl. 6.4.2
• Versicherungen; siehe ggf. Sozialwesen, Leistungsträger	
• Werbung, Markt- und Meinungsforschung	vgl. 4.1.2
• Sonstiges, Allgemeines	5.1
Infrastruktureller Sektor	
• Energie-, Wasser- und Versorgungswirtschaft	2.1.13
• Verkehrs- und Beförderungswesen	
• Wohnungswirtschaft, Immobilienverwaltung	2.1.1, 2.1.2, 4.1.5
• Rechenzentren	
• Sonstiges, Allgemeines	
Internet, Medien, Kommunikation	
• E-Mail, Telekommunikationsvorgänge, Post	4.1.5
• E-Commerce	1.4, 1.5, 2.2.2, 4.1.1, 4.1.2, 4.1.3, 4.1.6, 9.5
• Social Media, digitale Dienste	1.4, 1.5, 2.1.16, 2.2.1, 4.1.1, 4.1.3, 6.1.1, vgl. 6.5.1, 7.7, 8.6
• Sonstiges, Allgemeines	5.1
Kammern, berufsständische Körperschaften d. ö. R.*	
Meldung von Datenschutzverletzungen, Artikel 33	4.4.1, 4.4.2, 4.4.3, 4.4.3.1, 4.4.3.2, 4.4.3.3
Ordnungswidrigkeiten – Sächsische Datenschutzbeauf.	6.4.1, 6.4.2, vgl. 9.3
Religionsgemeinschaften	

Verzeichnis von Verarbeitungstätigkeiten, Kooperationspflicht	vgl. 6.4.2
Videografie und Bildverarbeitung	
• Behördliche Überwachung/Verarbeitung*	1.1, 2.1.7, 2.1.8, 2.1.9, 8.4
• Beschäftigte, vgl. ansonsten Beschäftigtendatenschutz	
• Dashcam, Drohnen	2.1.16
• Handel, Gewerbe	2.1.6
• Wohnbereiche	7.8
• Sonstiges, Allgemeines	2.1.7, 2.2.1, vgl. 6.4.2, vgl. 6.5.1, 8.6
Wahlrecht*	vgl. 6.5.1
Zertifizierung, Akkreditierungen, Prüfsiegel	

Richtlinie (EU) 2016/680

Polizei*	2.1.14, 3.2.1, 6.4.1, 8.1, 8.2, 8.6
Ordnungswidrigkeitenbehörden*	8.4
Strafverfolgung*	1.1, 8.3
Straf- und Justizvollzug*	8.5

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

Sächsischer Landtag als Parlament	6.3.1
Verfassungsschutz	8.7
Weitere datenverarbeitende Stellen	

1 Datenschutz im Freistaat Sachsen

1.1 Polizeilicher Einsatz automatisierter Gesichtserkennung in Strafverfahren

↗ § 48 BDSG; §§ 98a, 100h, 163f, 163g stopp; Art. 5 KI-Verordnung

Anfang Mai 2024 berichteten verschiedene Medien über den polizeilichen Einsatz eines Systems zur Gesichtserkennung und zum Gesichtsabgleich in Echtzeit in einem Ermittlungsverfahren der Strafverfolgungsbehörden eines anderen Bundeslandes. Das Personen-Identifikations-System („PerIS“) war dort in Amtshilfe von sächsischen Polizeibeamten zur Anwendung gebracht worden. Die Berichte legten nahe, dass auch bei der Nutzung des Systems im Freistaat Sachsen Bildabgleiche unter Verarbeitung biometrischer Daten in Echtzeit vorgenommen werden.

Tätigkeitsbericht Datenschutz 2022:
↗ sdb.de/tb2022

Dass eine sächsische Polizeidirektion (PD) das System PerIS beschafft hatte und nutzt, war mir seit längerer Zeit bekannt (vgl. Tätigkeitsbericht 2022, Seite 220); ebenso war bekannt, dass das System einen biometrischen Liveabgleich der Aufnahmen mit Referenzbildern ermöglicht. Im Hinblick auf die polizeiliche Befugnis des im Jahr 2020 eingeführten mittlerweile außer Kraft getretenen § 59 Sächsisches Polizeivollzugsdienstgesetz (SächsPVDG) war die Funktion auch durchaus erforderlich. Hinsichtlich des konkreten polizeilichen Einsatzes des Systems in strafprozessualen Ermittlungsverfahren offenbarten sich Informationslücken, die infolge meiner durch die Medienberichterstattung veranlassten Nachfragen im konstruktiven Dialog mit der PD

geschlossen werden konnten. Im Ergebnis erhielt ich anhand der Angaben der PD einen präzisen Überblick über das Verfahren und konnte darauf meine Bewertung stützen.

Verfahren

Das System PerIS vereinigt die Fertigung hochauflösender Bildaufzeichnungen und die Möglichkeit, Bilder bzw. Bildausschnitte aus den Aufnahmen mit zuvor hinterlegten Referenzbildern automatisiert abzugleichen, wobei beide Verfahrensschritte nicht zwingend gemeinsam vorgenommen werden müssen. Der automatisierte Abgleich kann in Echtzeit erfolgen, zeitlich versetzt (retrograd) vorgenommen werden oder ganz unterbleiben. In der Praxis kommt auch eine nichtautomatisierte (händische) Auswertung einzelner Sequenzen der Bildaufzeichnungen zur Anwendung.

Kameras, die von der Polizeidirektion gegebenenfalls für strafprozessuale Maßnahmen genutzt werden, befinden sich in den von der PD betriebenen Kamerasäulen (Kamerastandorte, die präventiv oder ausschließlich strafprozessual betrieben werden) oder in PerIS-Fahrzeugen. Für strafprozessuale Aufzeichnungen werden gegebenenfalls auch Kameras bzw. Kamerasäulen genutzt, mit denen grundsätzlich nach § 57 Abs. 3 Nr. 2 SächsPVDG öffentlicher Raum präventiv videoüberwacht wird.

Für die Bildaufzeichnung an den betreffenden Straßenabschnitten (aus Sicht der PD eine Maßnahme nach §§ 100h, 163f Strafprozessordnung [StPO]) und für den biometrischen automatisierten Abgleich (aus Sicht der Polizei eine Maßnahme nach § 98a StPO) werden richterliche Anordnungen durch die zuständige verfahrensleitende Staatsanwaltschaft zumeist zugleich beantragt; die richterlichen Beschlüsse ergehen in der Regel gesondert. Seitens der PD werden Aufzeichnungsintervalle täglich auf Zeitfenster beschränkt, in denen nach Anhaltspunkten im konkreten Verfahren und/oder nach kriminalistischer Erfahrung mit verfahrensrelevanten Aufnahmen zu rechnen ist. Hochauflösende Bildaufzeichnungen von Kameras an Kriminalitätsschwerpunkten, die nach § 57 Abs. 3 Nr. 2 SächsPVDG gefertigt werden, wer-

den nach § 57 Abs. 10 SächsPVDG in strafprozessualen Ermittlungsverfahren genutzt und ausgewertet, wenn tatsächliche Anhaltspunkte für ermittlungsrelevante Erkenntnisse vorliegen. Aufzeichnungen nach § 57 Abs. 3 Nr. 2 SächsPVDG unterliegen keinem Richtervorbehalt; sollen solche Bildaufnahmen strafprozessual genutzt und einem automatisierten biometrischen Abgleich unterzogen werden, erfolgt das auf richterliche Anordnung (§§ 98a, 98b StPO). In konkreten Ermittlungsverfahren wird aus den Rohdaten der Kamerastandorte der Datenbestand zur Recherche herangezogen, der von der richterlichen Anordnung zum Abgleich (nach § 98a StPO) umfasst ist; in der Regel gilt diese nicht für alle Kamerasäulen, sondern nur für ermittlungsrelevante Standorte.

In Verfahren mit bekannten Verdächtigen/Beschuldigten und entsprechenden Referenzbildern wird der gesamte Teil des Rohdatenbestandes, der von der konkreten Anordnung umfasst ist (zum Beispiel „Kamerastandorte x, y und z"), biometrisch mit den Referenzbildern abgeglichen, wenn eine richterliche Anordnung zum biometrischen Abgleich vorliegt (§§ 98a, 98b StPO). Fehlt eine richterliche Anordnung des automatisierten Abgleichs, findet auch in Verfahren mit bekannten Verdächtigen und Referenzbildern lediglich ein händischer Abgleich statt. Bei automatisierten biometrischen Abgleichen erfolgt keine Vorauswahl bestimmter Aufnahmesequenzen oder eine sonstige Reduzierung/Filterung der Bildaufzeichnungen; abgeglichen wird der aus dem gesamten Rohdatenbestand entnommene und danach nicht weiter gefilterte Datenbestand, der nach der richterlichen Observationsanordnung erhoben wurde. Die PD führt die biometrischen Abgleiche bis spätestens 95 Stunden nach Aufnahme durch. Ermittlungsrelevante Bilder/Treffer werden in die Ermittlungsakte überführt; das restliche, verfahrensirrelevante Bildmaterial wird mittels eines Lösch-Tools sofort nach Feststellung der Verfahrensirrelevanz (auf händischen Befehl) oder automatisch nach voreingestellten Fristen – je nach Delikt zwischen 240 und 2.000 Stunden – gelöscht. Eine unverzügliche automatisierte Löschung von „Nicht-Treffer-Bildsequenzen" unmittelbar nach dem Abgleich erfolgt nicht.

Strafprozessuale biometrische Liveabgleiche (Echtzeit, Aufnahmezeitpunkt ist auch Abgleichzeitpunkt) hat die PD in Sachsen nicht durchgeführt.

Aus dieser Verfahrensbeschreibung folgt, dass jede Person, die von einer nach Observationsbeschluss betriebenen Kamera erfasst wird und von der hochauflösende Bilder gefertigt wurden, in Verfahren mit angeordneten biometrischen Abgleichen und Rasterfahndungsbeschluss auch einem biometrischen Abgleich unterzogen wird. Die Zahl der Betroffenen bei einem retrograden Abgleich ist in Ermangelung einer vorherigen Aussonderung/Filterung von Aufnahmesequenzen genauso hoch wie bei einem Liveabgleich. Je nach angeordneter Dauer der Überwachung bestimmter (mehrerer) Straßenabschnitte – richterliche Anordnungen umfassen regelmäßig einen Zeitraum von bis zu drei Monaten (§ 163 Abs. 3 in Verbindung mit § 100e Abs. 1 Satz 4 StPO) – werden hochauflösende Bilder von hunderten, eher aber tausenden Personen gefertigt, die biometrisch verarbeitet, temporär gespeichert und automatisiert mit Referenzbildern abgeglichen werden, wobei nahezu sämtliche Betroffene in keinerlei Zusammenhang mit den aufzuklärenden Straftaten stehen.

Bewertung

Ich bin nicht für die Kontrolle von Gerichten zuständig, die im Rahmen ihrer justiziellen Tätigkeit handeln (§ 37 Abs. 2 Sächsisches Datenschutz-Umsetzungsgesetz [SächsDSUG]). Damit sind auch konkrete richterliche Entscheidungen über Bildaufzeichnungen an Straßenabschnitten und automatisierte biometrische Abgleiche mit Referenzbildern meiner Bewertung entzogen; ich verfüge praktisch über keine Interventionsmöglichkeit bei polizeilichen Maßnahmen, die richterlich angeordnet wurden. Insofern sind auch keine (Untersagungs-)Anordnungen (§ 40 Abs. 2 Satz 5 SächsDSUG) gegen polizeiliche Datenverarbeitungen opportun, die die Polizei aufgrund richterlicher Beschlüsse durchführt. Der Richtervorbehalt und damit die gerichtliche Überprüfung einer Ermittlungsmaßnahme vor ihrer Anwendung implizieren –

so die rechtliche Konzeption – die Prüfung, ob die Maßnahme auf eine gesetzliche Grundlage gestützt werden kann und im Einzelfall verhältnismäßig ist.

Abstrakt allerdings und unabhängig von konkreten Ermittlungsverfahren sehe ich im Rahmen einer grundsätzlichen Einschätzung des Vorgehens der PD bereits Bildaufzeichnungen von Abschnitten öffentlicher Straßen als grundrechtsbeeinträchtigende Maßnahmen, die nahezu ausschließlich unbeteiligte Dritte in großer Zahl betreffen, äußerst kritisch. Hochauflösende (gleichzeitige) Bildaufzeichnungen an (verschiedenen) Abschnitten öffentlicher Straßen, denen aufgrund ihrer Fertigungsorte in der Nähe von Brücken kaum ausgewichen werden kann, greifen in Rechte sehr vieler Betroffener ein. Die §§ 100h, 163f StPO sind nach meiner Überzeugung keine Rechtsgrundlagen, auf die ein derartiges „Scannen" des öffentlichen Straßenverkehrs gestützt werden kann. Beide Beobachtungsbefugnisse dürfen zwar auch angewandt werden, wenn Dritte unvermeidbar (mit-)betroffen werden (§ 100h Abs. 3, § 163f Abs. 2 Satz 1 StPO); sie sind aber ganz offenkundig nicht für Einsätze geschaffen worden, in denen von vornherein feststeht, dass bei einer nur gewissen bzw. geringen Wahrscheinlichkeit, ermittlungsrelevante Erkenntnisse zu erlangen, von hunderten oder tausenden unbeteiligten Dritten hochauflösende Bilder gefertigt werden. Insofern habe ich bereits im Tätigkeitsbericht 2022 (Seite 220) erhebliche Bedenken geäußert.

Diese Bedenken hinsichtlich der Verhältnismäßigkeit des Vorgehens verstärken sich massiv, wenn sich an derartige Bildaufzeichnungen eine biometrische Weiterverarbeitung der erhobenen Daten anschließt und von den Kameras erfasste Personen einem biometrischen Abgleich ihrer Gesichter mit Referenzbildern unterzogen werden. Dies gilt umso mehr, als die PD – bei Vorliegen richterlicher Anordnungen für den biometrischen Abgleich aufgezeichneter Bilder mit Referenzbildern – den Bilddatenbestand aus den Aufzeichnungen vor dem biometrischen Abgleich nicht reduziert oder nach wie auch immer gearteten Kriterien filtert. Dadurch werden auch biometrische Daten von Personen verarbeitet,

die – im Widerspruch zum Wortlaut von § 98a Abs. 1 Satz 1 StPO – „bestimmte, auf den Täter vermutlich zutreffende Prüfungsmerkmale" gerade nicht erfüllen (Beispiel: Die Referenzbilder zeigen männliche Beschuldigte oder Tatverdächtige, vom biometrischen Abgleich sind aber sämtliche im Aufzeichnungszeitraum erfasste Personen betroffen, darunter auch Frauen und Kinder).

Biometrische Daten natürlicher Personen sind eine besondere Kategorie personenbezogener Daten (§ 500 Abs. 1 StPO in Verbindung mit § 46 Nr. 12, 14 Bundesdatenschutzgesetz [BDSG]) und dürfen nur verarbeitet werden, soweit dies zur Aufgabenerfüllung unbedingt erforderlich ist (§ 500 Abs. 1 StPO in Verbindung mit § 48 Abs. 1 BDSG). Unter welchen Umständen vor diesem Hintergrund der Einsatz von Gesichtserkennungssoftware in strafprozessualen Ermittlungsverfahren aus meiner Sicht angemessen und verhältnismäßig sein kann, habe ich im Tätigkeitsbericht 2021 auf Seite 199, ausgeführt.

Tätigkeitsbericht Datenschutz 2021:
↗ sdb.de/tb2021

In meinen Zweifeln an der Verhältnismäßigkeit der Maßnahme(n) sehe ich mich – wie schon im Tätigkeitsbericht 2022 erwähnt – durch die Rechtsprechung des Bundesverfassungsgerichts (BVerfG) zu präventiven Maßnahmen des automatisierten Kfz-Kennzeichenabgleichs auf landespolizeirechtlicher Grundlage bestätigt (vgl. insbesondere BVerfG, Beschluss vom 18. Dezember 2018 – 1 BvR 142/15 –, BVerfGE 150, 244-309, Rn. 96 bis 98 nach juris).

Auch der Bundesgesetzgeber hat in der Begründung der neu geschaffenen Befugnis zum automatisierten Kfz-Kennzeichenabgleich im Strafverfahren in § 163g StPO ausdrücklich auf erhebliche Zweifel daran hingewiesen, dass Bildaufnahmen von Kfz-Kennzeichen des passierenden öffentlichen Straßenverkehrs und deren Abgleich mit Referenzdaten auf bereits bestehende Rechtsgrundlagen (etwa § 100h und § 98c StPO) gestützt werden könnten (BT-Drs. 19/27654, S. 84). Dieser zunächst „nur" Kfz-Kennzeichen betreffende Befund kann auf die Fertigung hochauflösender (Personen-)Bilder des öffentlichen Straßenverkehrs mit nahezu ausschließlich unbeteiligten Dritten (siehe oben) übertragen werden. Erst

recht müssen die Ausführungen des Bundesgesetzgebers für derartige Bildaufzeichnungen mit sofortigem biometrischem Abgleich mit Referenzbildern in Echtzeit gelten.

Aber auch für nachträgliche biometrische Abgleiche der Bildaufzeichnungen aus der Überwachung öffentlicher Straßen mit Referenzbildern kann nichts anderes gelten, insbesondere wenn der Bilddatenbestand vor dem Abgleich nicht reduziert oder gefiltert wird. In diesen Fällen tritt – gewissermaßen „in Verschlimmerung" gegenüber automatisierten Kennzeichenerkennungssystemen – zum Eingriff der Aufzeichnung noch der Eingriff der Speicherung der Aufnahmen bis zum Abgleich und der erst danach händisch anzuordnenden Löschung hinzu.

Jedenfalls für Echtzeit-Abgleiche biometrischer personenbezogener Daten in Strafverfahren ergeben sich aus der im Berichtszeitraum verabschiedeten Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (KI-Verordnung) neue Anforderungen und die zwingende Notwendigkeit der Schaffung einer Rechtsgrundlage durch den Bundesgesetzgeber (Art. 5 Abs. 2, 3, 4 und 5 der KI-Verordnung). Die §§ 100h, 163f in Verbindung mit § 98a StPO sind danach als Grundlage für biometrische Liveabgleiche nicht mehr ausreichend.

Auch wenn die KI-Verordnung detaillierte Bestimmungen nur für die biometrische Echtzeit-Fernidentifizierung trifft, muss nach meiner Überzeugung angesichts ihrer Eingriffstiefe aber auch für sonstige Maßnahmen, bei denen im Wege der Überwachung öffentlichen Raums hochauflösende (Gesichts-)Bilder an Abschnitten öffentlicher Straßen gefertigt und ggf. für zeitlich verzögerte biometrische Abgleiche mit Referenzbildern genutzt werden, eine tragfähige eigene gesetzliche Grundlage geschaffen werden, die Schutzvorkehrungen für die dabei erfassten zahlreichen unbeteiligten Dritten enthält (wie etwa in § 163g Abs. 2 Satz 3, 4, Abs. 3 und 4 StPO). Auch Systeme zur „lediglich" nachträglichen biometrischen Fernidentifizierung sind Hochrisiko-KI-Systeme im Sinne der KI-Verordnung. In den Erwägungsgründen (EG) der KI-Verordnung wird auf die Eingriffstiefe auch von Systemen zur nachträglichen biometrischen Fernidentifizie-

rung hingewiesen. Eine Verarbeitung biometrischer Daten soll nur dann erlaubt sein, „wenn sie unbedingt erforderlich ist, vorbehaltlich angemessener Vorkehrungen für den Schutz der Rechte und Freiheiten der betroffenen Person, und sofern sie nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zulässig ist" (EG 94); „die Bedingungen für die nachträgliche biometrische Fernidentifizierung sollten keinesfalls eine Grundlage dafür bieten, die Bedingungen des Verbots und der strengen Ausnahmen für biometrische Echtzeit-Fernidentifizierung zu umgehen" (EG 95).

Insbesondere in Fallkonstellationen, in denen ein sehr großer Datenbestand aus der Überwachung öffentlicher Straßenabschnitte vor einer nachträglichen biometrischen Fernidentifizierung nicht ausgedünnt bzw. gefiltert wird und ein Abgleich sich somit auf sämtliche im Rahmen der Überwachung erfasste Personen erstreckt – so in dem durch die PD angewandten Verfahren –, ist die Intensität des Grundrechtseingriffs vergleichbar mit derjenigen bei einer biometrischen Echtzeit-Fernidentifizierung. Verzögerungen des Abgleichs von 30 Minuten bis 95 Stunden nach Fertigung der Bildaufzeichnungen sorgen zwar für eine „Nachträglichkeit" der biometrischen Fernidentifizierung, mildern bei Beibehaltung des Umfangs des Datensatzes den Eingriff in das Grundrecht der betroffenen Personen aber nicht ab, sondern verstärken ihn aufgrund der zwischenzeitlichen Speicherung der Daten.

Vor diesem Hintergrund – sowohl mit Blick auf das EU-Recht als auch auf nationales (Verfassungs-)Recht – erscheint die Schaffung einer hinreichend bestimmten, normenklaren und Schutzvorkehrungen festlegenden Rechtsgrundlage für die strafprozessuale Überwachung öffentlichen Raums mit einem anschließenden automatisierten biometrischen Abgleich der Aufnahmen mit Referenzbildern zwingend geboten, sofern der Gesetzgeber Bedarf sieht, die Strafverfolgungsbehörden mit einer derartigen Befugnis auszustatten. Dies gilt sowohl für retrograde Abgleiche als auch für Abgleiche in Echtzeit. Für Letztere ergibt sich die Notwendigkeit einer speziellen und normenklaren Rechtsgrundlage bereits unmittelbar aus der KI-Verordnung.

Was ist zu tun?
Für automatisierte biometrische Abgleiche von Personenbildern aus dem öffentlichen Raum mit Referenzbildern in Echtzeit gibt es mit Inkrafttreten der EU-KI-Verordnung keine Rechtsgrundlage. Aber auch für biometrische Abgleiche von einer Vielzahl im öffentlichen Raum erfasster Personenaufnahmen ohne Echtzeit bedarf es einer normenklaren gesetzlichen Grundlage, die grundrechtsschonende Vorgaben enthält.

Das Sächsische Staatsministerium der Justiz und für Demokratie, Europa und Gleichstellung und das Sächsische Staatsministerium des Innern habe ich über meine Auffassung in Kenntnis gesetzt.

1.2 KI in der sächsischen Verwaltung

↗ DSGVO, SächsDSDG

Das Thema künstliche Intelligenz (KI) ist nicht nur in der Bevölkerung und Privatwirtschaft von großem Interesse, sondern auch in der öffentlichen Verwaltung. Durch einen verstärkten Einsatz von KI erhofft man sich eine effizientere Verwaltung, reduzierte Kosten und eine Entspannung des Fachkräftemangels, der derzeit alle Bereiche der öffentlichen Verwaltung betrifft. Diesem Ziel stehe ich nicht im Weg, aber eine nachhaltige Entwicklung in diesem Bereich kann nur möglich sein, wenn die Umsetzung rechtskonform erfolgt. Die Datenschutz-Grundverordnung (DSGVO) setzt hierbei für öffentliche Stellen auch teilweise andere Voraussetzungen voraus als im nichtöffentlichen Bereich, insbesondere ist eine Verarbeitung auf Grundlage eines berechtigten Interesses (Art. 6 Abs. 1 Buchstabe f DSGVO) nicht möglich. Aus diesem Grund habe ich im Vorjahr vor dem Einsatz von ChatGPT in der öffentlichen Verwaltung gewarnt, bis diese Fragen geklärt sind.

Im letzten Jahr haben die sächsischen Staatsministerien und die Staatskanzlei beschlossen, eine Richtlinie zu erarbeiten, auf deren Grundlage sie KI einsetzen. Ich wurde eingeladen, an der Erstellung dieser Richtlinie mitzuwirken, und diese Einladung habe ich gerne angenommen. Diese Richtlinie soll primär als Leitfaden für geltendes Recht dienen, und diese Aufgabe erfüllt sie aus meiner Sicht. Sowohl dem Dienstherrn als auch den Mitarbeitenden der Staatsministerien werden umfangreiche und nachvollziehbare Anhaltspunkte für die Arbeit mit KI gegeben. Die weitaus größere Aufgabe wird sicherlich sein, adäquate Anwendungsbereiche für KI

im öffentlichen Bereich und die entsprechenden Applikationen zu entwickeln, aber ein wichtiger erster Schritt wurde in Sachsen nun getan.
Aus datenschutzrechtlicher Sicht sind folgende Punkte besonders wichtig:

- Personenbezogene Daten dürfen von KI-Systemen verarbeitet werden, wenn alle Vorgaben der DSGVO erfüllt sind. Das beinhaltet neben Informations- und Dokumentationspflichten insbesondere eine gültige Rechtsgrundlage, wobei die Rechtsgrundlage der Einwilligung im Regelfall ausgeschlossen wird. Eine Verarbeitung auf Grundlage von Artikel 6 Abs. 1 Buchstabe e DSGVO in Verbindung mit § 3 SächsDSDG, also die Verarbeitung zur Erfüllung einer öffentlichen Aufgabe, bedarf nach meiner Auffassung einer Begründung der Erforderlichkeit.
- Das KI-System muss rechtskonform zustande gekommen sein, und es muss sichergestellt sein, dass es selbst keine personenbezogenen Daten ausgeben kann, für welche keine Rechtsgrundlage vorliegt. Darüber hinaus sind Betroffene eindeutig und zweifelsfrei zu informieren, sobald eine KI zum Einsatz kommt, und der Einsatz darf nur unter menschlicher Aufsicht erfolgen und muss stets einem Menschen zugeordnet werden können. Es ist unter diesen Voraussetzungen dann beispielsweise denkbar, dass eine KI automatisch ein Antwortschreiben zu einem bestimmten personenbezogenen Sachverhalt verfasst, oder dass Anträge vor Prüfung durch einen Sachbearbeiter durch ein KI-System beurteilt werden.

Was ist zu beachten?
Die sächsischen Staatsministerien haben eine gute Grundlage für die Verwendung von KI in der öffentlichen Verwaltung geschaffen. Ich unterstütze diese Richtlinie und hoffe, dass die Umsetzung für Sachsen ein Erfolg wird.

1.3 Künstliche Intelligenz in der Schule

↗ DSGVO

Tätigkeitsbericht Datenschutz 2021:
↗ sdb.de/tb2021

Bereits in meinem Tätigkeitsbericht 2021 berichtete ich im Abschnitt „2.1.2 Künstliche Intelligenz in der Schule: Area9 Rhapsode" (Seite 48 ff.) über die geplante Testung eines intelligenten tutoriellen Systems durch die sächsische Kultusverwaltung und die verbesserungswürdige Einbindung meiner Behörde.

Daraus resultierte zwischenzeitlich ein länderübergreifendes Vorhaben der Kultusministerkonferenz „Intelligentes Tutorielles System (ITS)" unter sächsischer Federführung, in das ich umfangreich eingebunden wurde. Mittlerweile wurde dieses jedoch mit dem Projekt „Adaptive Learning Cloud (ALC)" zu „Adaptives Intelligentes System (AIS)" unter Federführung von Hamburg zusammengeführt.

Mit „AIS" ist, anknüpfend an das Projekt ITS, eine digitale Lernumgebung geplant, die ihrem Grundgedanken nach darauf abzielt, im schulischen Unterricht eine individuellere Förderung von Schülerinnen und Schülern zu ermöglichen. Der Einsatz der Software ist nicht nur in Präsenzumgebungen mit innovativen Lehr- und Lernformaten geplant, sondern auch beim Distanzlernen und hybriden Lernen. AIS soll auf Grundlage der Bearbeitung von Lernaufgaben der Schülerinnen und Schüler Lerninhalte individuell anpassen, wobei entsprechende Zuweisungen des Systems kontinuierlich überprüft werden. Teil des Vorhabens ist zudem die Integration einer KI-Chatbot-Oberfläche.

Letztere steht für sächsische Lehrkräfte bereits jetzt zur Verfügung. Im Berichtszeitraum habe ich einen datenschutzkonformen Zugang zu Künstlicher Intelligenz begleitet. Der durch die Kultusverwaltung kostenfrei zur Verfügung gestellte Assistent KAI nutzt dabei Schnittstellen zu Anbietern von generativer KI. Zum einen können dabei jedoch von den externen Anbietern (wie OpenAI) die von den Nutzenden eingegebenen Daten nicht einzelnen Nutzenden zugeordnet werden. Zum anderen schließen die genutzten Schnittstellen und Verträge

aus, dass die externen Anbieter die eingegebenen Daten zum weiteren Training ihrer KI-Modelle verwenden.

Für Lehrkräfte besteht somit eine datenschutzkonforme Möglichkeit, für Aufgaben aus dem pädagogischen Alltag auf KI-Unterstützung zurückzugreifen. So können beispielsweise zielgruppenorientierte Lehrtexte erstellt, kreative Unterrichtsideen entwickelt, Aufgaben, Quiz und Bilder generiert werden.

Was ist zu beachten?
Wenn Schulen KI-Werkzeuge verwenden wollen, haben sie mit dem Assistenten KAI eine kostenfreie und datenschutzgerechte Möglichkeit.

1.4 Kontrolle von über 30.000 Websites sächsischer Verantwortlicher

↗ § 25 TDDDG sowie die Art. 6 Abs. 1 DSGVO

2023 hat meine Behörde damit begonnen, eine Laborumgebung für die automatisierte Prüfung von Apps und Websites aufzubauen. Ziel war es, einerseits bei Beschwerden Detaillierungsgrad und Prüftiefe zu erhöhen, andererseits auch anlassunabhängig ein Monitoring der von sächsischen Verantwortlichen betriebenen Websites zu ermöglichen. Mitte 2024 waren die Entwicklungsarbeiten für ein Werkzeug zur Massenprüfung fertiggestellt, und eine erste Prüfung wurde durchgeführt. Geprüft wurden die Adressen von 32.981 Websites von sächsischen Unternehmen, Vereinen und Behörden. Die Adressen der Websites wurden über öffentlich zugängliche Quellen vorab ermittelt, mit dem Ziel, einen möglichst umfassenden Überblick über sächsische Verantwortliche zu erlangen.

Analysiert wurde dabei der initiale Aufruf der Website ohne jegliche Einwilligung oder weitere Interaktionen. Eventuell vorhandene Cookie-Banner wurden nicht berücksichtigt, die Websites wurden also besucht, ohne dass eine Einwilligung erteilt wurde. Schon dieser einfache Aufruf zeigte eine Vielzahl datenschutzrechtlich nicht zulässiger Website-Umsetzungen.

Insgesamt 21.834 (66,2 %) der Websites führten im initialen Aufruf (ohne Einwilligung) Netzwerkanfragen an Drittanbie-

ter durch. Im Durchschnitt waren dies rund drei Drittanbieteranfragen pro Website.

Die Verknüpfung der angefragten Drittanbieter-Domains zum entsprechenden Unternehmen ergab, dass von den meisten Websites Verbindungen zu Google LLC aufgebaut wurden. Dies betraf insgesamt 9.925 Websites (30,9 %). Diese Verbindungen wurden initiiert durch die Einbettung von diversen Google-Diensten wie beispielsweise Google Fonts, Google Tag Manager, Google Maps, Google Analytics oder Youtube. In Tabelle 1 werden die Top 10 der Verbindungen zu Google-Diensten nach Vorkommen in den Websites gelistet.

Tabelle 1:
Die häufigsten Verbindungen zu Google-Diensten

Domain	Anzahl Websites
fonts.gstatic.com	4.849 (14,7 %)
fonts.googleapis.com	4.524 (13,7 %)
www.googletagmanager.com	3.010 (9,1 %)
www.google.com	2.512 (7,6 %)
www.gstatic.com	1.672 (5,0 %)
www.google-analytics.com	1.614 (4,9 %)
maps.googleapis.com	1.482 (4,5 %)
region1.google-analytics.com	1.475 (4,5 %)
ajax.googleapis.com	995 (3,0 %)
maps.gstatic.com	931 (2,8 %)

Zusammengestellt nach kontaktierten Unternehmen folgen, bezogen auf Drittanbieterverbindungen, Amazon (1.256, 3,81 %), Cloudflare (1.248, 3,78 %) und Facebook (888, 2,69 %) sowie die Consent-Management-Anbieter Usercentrics (1.193, 3,62 %), eRecht24 (686, 2,08 %) und Cybot (678, 2,06 %). Abbildung 1 zeigt die Top 20 Drittanbieterverbindungen nach Vorkommen in Websites.

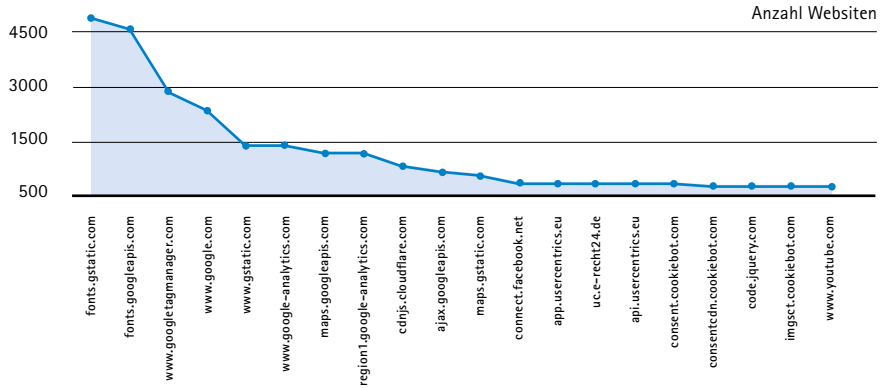


Abbildung 1:
Häufigkeit von Drittanbieterverbindungen

Knapp die Hälfte (16.627, 50,4 %) der Websites speicherten im initialen Aufruf auch Cookies. In 23,9 % (7.888) der Websites wurden dabei auch Cookies von Drittanbietern gespeichert. Insgesamt wurden 57.362 Cookies gesetzt, im Durchschnitt also rund zwei Cookies pro Website.

Tabelle 2:
Meistgesetzte Cookies

Cookie-Name	Anzahl Websites	Vermutlicher Service
PHPSESSID	3.159 (9,6 %)	PHP
_ga	1.744 (5,3 %)	Google Analytics
_gid	1.207 (3,7 %)	Google Analytics
__cf_bm	721 (2,2 %)	Cloudflare
CookieConsent	676 (2,0 %)	CookieBot
XSRF-Token	633 (1,9 %)	
_gat	601 (1,8 %)	Google Analytics
YSC	573 (1,7 %)	Youtube
VISITOR_PRIVACY_METADATA	572 (1,7 %)	Youtube
VISITOR_INFO1_LIVE	571 (1,7 %)	Youtube

Die meisten Drittanbieter-Cookies wurden gesetzt von den Domains youtube.com (573, 1,7 %), cnd.website-start.de (460, 1,4 %), panorama.wixapps.net, (454, 1,4 %), www.google.com (400, 1,2 %), und strato-editor.com (318, 1,0 %). 6.043 Websites (18,3 %) speicherten zudem Daten im Local Storage des Endgeräts.

Tabelle 3:
Meistgesetzte Local-Storage-Einträge

Local Storage Key	Anzahl Websites	Vermutlicher Service
elementor	1.179 (3,6 %)	Elementor Wordpress Plugin
uc_settings	928 (2,8 %)	Usercentrics
uc_user_interaction	927 (2,8 %)	Usercentrics
uc_ui_version	850 (2,5 %)	Usercentrics
snowplowOutQueue_snowplow_cf	447 (1,4 %)	Snowplow
debug	444 (1,4 %)	–
fedops.logger.sessionId	444 (1,4 %)	Wix.com
_grecaptcha	386 (1,2 %)	Google reCAPTCHA
lastExternalReferrer-Time	289 (0,9 %)	Meta
LastExternalReferrer	289 (0,9 %)	Meta

Gehosted wurden die Seiten dabei insbesondere bei IONOS SE (5.376, 16,3 %), Strato AG (4.517, 13,7 %), Neue Medien Münnich GmbH (4.245, 14,9 %) sowie Hetzner Online GmbH (3.937, 11,9 %).

Nicht jede der Drittverbindungen und nicht jeder Cookie stellt ohne Einwilligung automatisch einen Datenschutzverstoß dar. Die Datenschutzaufsichtsbehörden legen an die Auslegung der Normen des Artikels 6 Abs. 1 DSGVO sowie des § 25 Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG) allerdings strenge Maßstäbe an, welche von den Gerichten in der Rechtsprechung auch weitgehend akzeptiert werden. Zu einzelnen Themen (Google Analytics,

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

Google Fonts, Google Tag Manager, Zahlungsdienste) habe ich mich bereits in früheren Tätigkeitsberichten geäußert und klargestellt, dass ein Betrieb oder ein Einbinden in die eigene Website nicht ohne ausdrückliche Zustimmung erfolgen darf. Da das Monitoring der Websites sächsischer Verantwortlicher keinen Selbstzweck darstellen soll, wurde daher in der Folge überlegt, wie aus der Vielzahl an Daten und Informationen ein zielgerichtetes Vorgehen zur Verbesserung des Datenschutzniveaus erreicht werden kann. Ich habe mich für die Massenprüfung eines klar festzustellenden Verstoßes entschieden, über die Durchführung und Erkenntnisse einer ersten Prüfung soll im folgenden Beitrag berichtet werden.

1.5 Massenprüfung sächsischer Verantwortlicher zum Einsatz von Google Analytics ohne Einwilligung

↗ § 25 TDDDG, Art. 6 Abs. 1 DSGVO

Im vorhergehenden Beitrag wurde über den Aufbau einer Laborumgebung und die Prüfung von über 30.000 sächsischen Websites berichtet. Aus den Erkenntnissen der Prüfung wurde ein erstes Massenverfahren entwickelt und durchgeführt. Auffällig im Gesamtdatenset war die hohe Quantität der Einbindungen von Google-Diensten ohne Einwilligung. Das US-amerikanische Unternehmen Google LLC gehört weltweit zu den größten Datenerfassern. Das Geschäftsmodell und damit das Eigeninteresse von Google besteht in der kommerziellen Verwertung von personenbezogenen Daten (siehe policies.google.com/privacy). Hervorzuheben ist dabei insbesondere der Dienst Google Analytics, ein Trackingtool, das der Datenverkehrsanalyse von Websites dient. Diesen Dienst auf der Grundlage eines berechtigten Interesses des Website-Betreibers einzubinden, ist aus Sicht der Aufsichtsbehörde nicht möglich. Wer mit diesem Trackingwerkzeug auf seiner Website das Nutzerverhalten überwachen möchte,

benötigt also von den Besucherinnen und Besuchern der Seite zuvor eine freiwillige und eindeutige Einwilligung.
In 2.304 (~7 %) der Websites wurde dieser Pflicht nicht in ausreichender Form nachgekommen. Das heißt, es wurden mit diesem Webanalyse-Dienst Daten gesammelt, ohne dass die Besucherinnen und Besucher zuvor eingewilligt hatten: in das Setzen von Analytics-Cookies (_ga) und/oder den Aufbau von Verbindungen zu Google Analytics (www.google-analytics.com, region1.google-analytics.com, region1.analytics.google.com). Darunter befanden sich sowohl Unternehmen und Vereine als auch öffentliche Stellen. Alle Verantwortlichen wurden daraufhin am 12. Juni 2024 postalisch aufgefordert, den Datenschutzverstoß zu beseitigen und alle rechtswidrig erhobenen Daten zu löschen. Zudem wurden die Betreiberinnen und Betreiber der Websites auch aufgefordert, ihre Seiten auf andere einwilligungsbedürftige Inhalte zu prüfen.
Die Vorbereitung bis zum Versand der Briefe bedeutete für meine Behörde einigen Aufwand. Alle Verantwortlichen wurden vor Versand hinsichtlich der automatisiert erhobenen Angaben in der Datenschutzerklärung bzw. dem Impressum im Hinblick auf korrekte Anschrift und Sitz in Sachsen hin händisch überprüft. Die automatisiert erhobenen Messergebnisse hinsichtlich des Einsatzes von Google Analytics wurden ebenfalls manuell verifiziert.
Mit rund 1.000 schriftlichen Rückmeldungen sowie ca. 250 Anrufen verzeichnete ich eine große Resonanz der Verantwortlichen. Zum Teil handelte es sich um mehrfache Rückmeldungen bzw. Beratungen, im Schnitt haben sich ca. 20 Prozent der Verantwortlichen im Zusammenhang mit dem Schreiben an die SDTB gewandt. Vor allem kleinere Unternehmen und Vereine benötigten Hilfestellung bei der Umsetzung der rechtlichen Anforderungen. In den Anfragen ging es nicht nur um Google Analytics, sondern beispielsweise auch um die richtige Einbindung von Zahlungsdienstleistern bei Onlineshops und die Einbettung von Videos aus sozialen Netzwerken. In den Beratungsgesprächen stellte sich des Weiteren heraus, dass oftmals eine erhebliche Zahl von Einwilligungsbannern nicht das taten, was die Einstellungen

den Nutzerinnen und Nutzern versprachen. Zum Teil wurden Dienste ausgeführt und Cookies gesetzt, obwohl die Einstellungen »aus« signalisierten. Das war vielen Verantwortlichen nicht bewusst, gleichwohl ist es ein ernst zu nehmendes Problem, da auch Besucherinnen und Besucher über eine vermeintlich datenschutzgerechte Einstellung getäuscht werden. Ich forderte die betroffenen Website-Betreiberinnen und -Betreiber daher auf, diese Fehler umgehend zu beheben.

Verbindung	Juni	Oktober	Rückgang
_ga	1.744 (75,7 %)	591 (25,7 %)	1.153 (66,1 %)
www.google-analytics.com	1.614 (70,1 %)	544 (23,6 %)	1.070 (66,3 %)
region1.google-analytics.com	1.475 (64 %)	413 (17,9 %)	1.062 (72 %)
region1.analytics.google.com	280 (12,2 %)	89 (3,9 %)	191 (68,2 %)
Analytics gesamt	**2.304 (100 %)**	**803 (34,9 %)**	**1.501 (65,2 %)**
Google gesamt (Fonts, Maps, Analytics, Youtube, Tagmanager, ...)	2.304 (100 %)	1.325 (57,5 %)	979 (42,5 %)

Tabelle 4:
Nachuntersuchung belegt Rückgang bei Google-Verbindungen

Im Oktober 2024 folgte eine Nachuntersuchung der 2.304 Websites. Diese ergab einen Rückgang der rechtswidrigen Verarbeitung beim Einsatz von Google Analytics bei 65,2 % (1.501) der Websites. Die Tabelle zeigt dabei den Rückgang bei den einzelnen Kriterien.

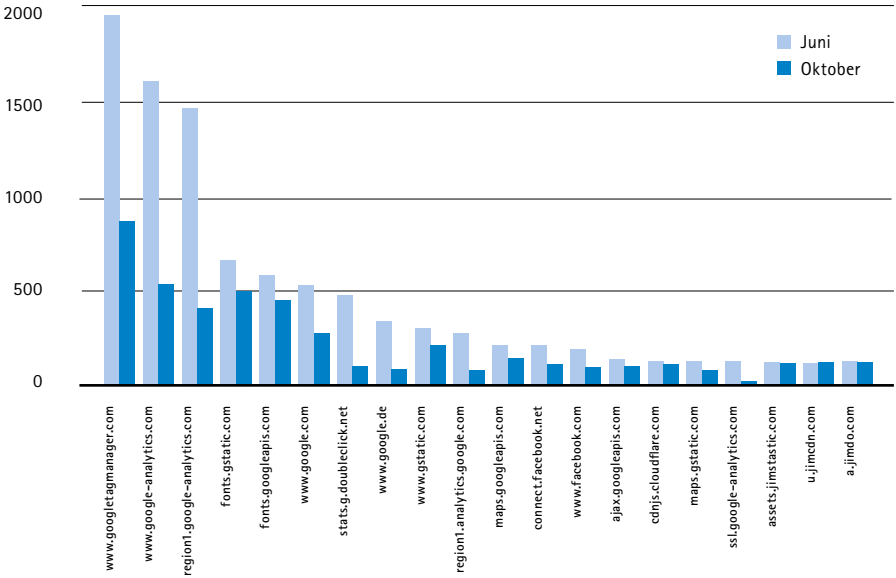
Auch bei anderen einwilligungsbedürftigen Verbindungen zu Drittanbietern sowie der Speicherung von Cookies werden Nutzerinnen und Nutzer nun seltener übergangen, sondern vorher um ihre Einwilligung gebeten. Dies zeigt sich beispielsweise überblicksmäßig in den Tabellen sowie Abbildungen 2 und 3, in denen die Verteilung der Top 20 Drittanbieterverbindungen und Cookies zwischen Juni und Oktober unter den 2.304 angeschriebenen Websites verglichen werden.

Eigenschaft	Juni	Oktober	Rückgang
Websites mit 3rd Party Requests	2.304 (100 %)	1.964 (85,9 %)	340 (14,8 %)
Cookies gesamt	14.683 (100 %)	7.815 (53,2 %)	6.868 (46,8 %)
Websites mit Cookies	2.165 (94 %)	1.579 (69 %)	586 (27 %)
Websites mit 3rd Party Cookies	1.716 (74,5 %)	944 (41,3 %)	772 (44,9 %)

Tabelle 5:
Weniger Cookies bei Nachuntersuchung

So erfreulich der starke Rückgang beim Einsatz von Tracking ohne Einwilligung auch ist, bleibt dennoch eine erhebliche Anzahl an Verantwortlichen ohne das erforderliche Bewusstsein für den Datenschutz. Die Massenprüfung hatte einen klaren Appellcharakter, welcher von vielen Verantwortlichen auch verstanden wurde, was man an der reichlich genutzten Möglichkeit des Kontakts zur Aufsichtsbehörde feststellen konnte. Die Ergebnisse der Massenprüfung werden von mir dennoch zum Anlass genommen, ähnliche Verfahren in regelmäßigen Abständen zu wiederholen.

Abbildung 2:
Drittanbieterverbindungen nach Häufigkeit, Juni und Oktober 2024 im Vergleich



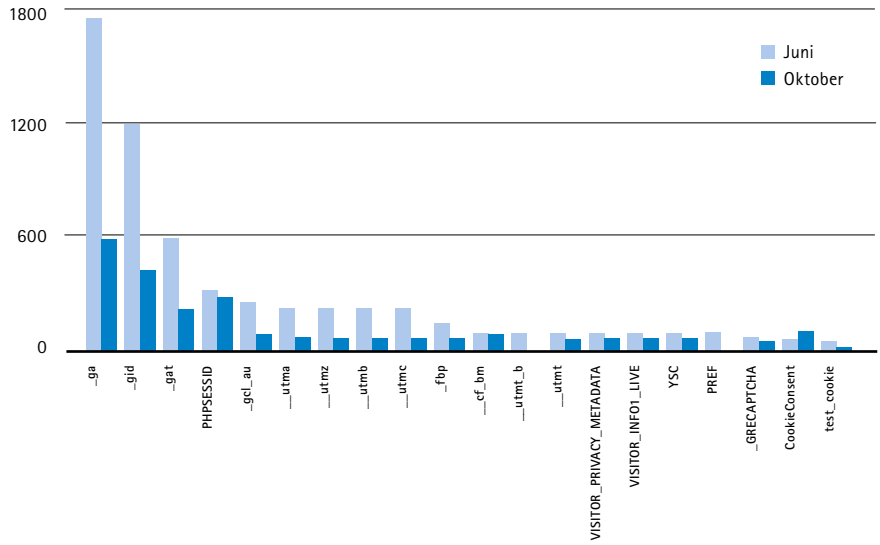


Abbildung 3:
Nutzung von Cookies, Vergleich Juni und Oktober 2024

Was ist zu tun?
Betreiber/innen von Websites sind verantwortlich für die richtigen Rechtsgrundlagen für Verarbeitungen auf der eigenen Website. Insbesondere für den Einsatz eines eigenen Tools für die Verwaltung von Einwilligungen lautet die dringende Empfehlung, neben der rechtlichen Prüfung auch eine technische Prüfung durchzuführen und auch regelmäßig zu überprüfen, ob ein Einwilligungsbanner das tut, was angezeigt wird. Weiterhin sind sowohl die DSGVO (für Verarbeitungen) als auch das TDDDG (für Cookies und ähnliche Techniken) zu beachten.

Verantwortliche, die trotz der Aufforderung meiner Behörde weiterhin rechtswidrig Daten von Nutzerinnen und Nutzern mit Google Analytics verarbeiten, müssen nun mit Sanktionen rechnen. Als Aufsichtsbehörde steht mir hierfür ein umfassender Katalog von Untersuchungs- und Abhilfebefugnissen zur Verfügung, um die Einhaltung datenschutzrechtlicher Bestimmungen durchzusetzen. Erste Verfahren befinden sich in Vorbereitung.

1.6 Mündliche Äußerungen im Beschäftigungsverhältnis

↗ § 26 BDSG

Vielfach erreichen meine Behörde Beschwerden von Beschäftigten über mündliche Äußerungen durch Dienstvorgesetzte oder Beschäftigte der Personalverwaltung im Rahmen von Belegschaftsversammlungen oder Teammeetings, die aus Sicht der betroffenen Beschäftigten in ihr Grundrecht auf informationelle Selbstbestimmung eingreifen. Dies betraf in einem Fall Äußerungen über die fristlose Beendigung eines

Beschäftigungsverhältnisses wegen eines mutmaßlichen Arbeitszeitbetruges oder in einem anderen Vorgang die erwähnte langandauernde Arbeitsunfähigkeit des Beschäftigten, einschließlich einer Mitteilung der ärztlichen Diagnose.

Die Verarbeitung von personenbezogenen Daten für Zwecke des Beschäftigungsverhältnisses richtet sich nach § 26 Bundesdatenschutzgesetz (BDSG) bzw. Art. 6 Abs. 1 Buchst. c Datenschutz-Grundverordnung (DSGVO). Bei den vorgenannten Angaben zur Beendigung des Beschäftigungsverhältnisses sowie des Beendigungsgrunds und auch bei Angaben zur Arbeitsunfähigkeit und zu Ursachen derselben handelt es sich um personenbezogene Beschäftigtendaten im Sinne des Art. 4 Nr. 1 DSGVO, deren Verarbeitung den genannten Datenschutzregelungen entsprechen muss, insbesondere erforderlich sein muss.

Von Verantwortlichen, respektive Dienstvorgesetzten oder auch Beschäftigten der Personalverwaltung wird mitunter jedoch übersehen, dass im Bereich der Datenverarbeitung im Beschäftigungsverhältnis nach § 26 Abs. 1 bis 6 BDSG Datenverarbeitungen erfasst werden, unabhängig davon, ob diese in einem Dateisystem gespeichert sind oder gespeichert werden sollen, vgl. § 26 Abs. 7 BDSG. Durch die Vorschrift des § 26 Abs. 7 BDSG werden so auch mündliche Äußerungen als Datenverarbeitung erfasst und unterliegen daher den Anforderungen des § 26 BDSG.

Im oben genannten Fall einer Kündigung kann es zwar erforderlich sein, die Beendigung des Beschäftigungsverhältnisses intern zu kommunizieren, insbesondere um die internen Abläufe sicherstellen bzw. aufrechterhalten zu können.

Die Information über den konkreten Grund für die Beendigung des Beschäftigungsverhältnisses in einer Belegschaftsversammlung bekannt zu geben wird zumeist jedoch nicht zur Beendigung bzw. Abwicklung des Beschäftigungsverhältnisses erforderlich sein, vgl. § 26 Abs. 1 Satz 1 BDSG.

Auch im Fall der Mitteilung, dass ein/e Beschäftigte/r arbeitsunfähig ist sowie der Angabe der ärztlichen Diagnose, ist, wie im zuvor dargestellten Fall, einer abgestuften datenschutzrechtlichen Prüfung zu unterziehen. Bei der Angabe der Ar-

beitsunfähigkeit sowie ärztlicher Diagnosen handelt es sich um Gesundheitsdaten nach Art. 4 Nummer 15 DSGVO. Die Verarbeitung von Gesundheitsdaten als besonders schützenswerte Daten ist grundsätzlich untersagt, vgl. Art. 9 Abs. 1 DSGVO, soweit nicht ein Ausnahmetatbestand nach Art. 9 Abs. 2 DSGVO besteht. Im Beschäftigungsverhältnis können diese Daten unter den Voraussetzungen des § 26 Abs. 3 BDSG verarbeitet werden. Danach kann eine Verarbeitung zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes erfolgen, soweit dies erforderlich ist und kein Grund zur Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt. Eine Information, dass ein/e Beschäftigte/r arbeitsunfähig ist, kann danach gerechtfertigt sein, nicht jedoch die Angabe der ärztlichen Diagnose bzw. Ursache der Arbeitsunfähigkeit im Rahmen von Belegschaftsversammlungen, Teammeetings und ähnlichen Veranstaltungen. Zu beachten ist in derartigen Fällen, dass zwischen der Datenverarbeitung des Verantwortlichen und der sozialen Kommunikation der Beschäftigten untereinander zu differenzieren ist. Die sozialübliche Kommunikation zwischen den Beschäftigten, beispielsweise Gerede oder „Tratsch" über die Gründe einer Arbeitsunfähigkeit oder Kündigung, unterfallen grundsätzlich nicht den datenschutzrechtlichen Anforderungen – die DSGVO ist nicht anwendbar bei Datenverarbeitung durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten, vgl. Art. 2 Abs. 2 Buchst. c DSGVO.

Diese Ausnahme gilt jedoch nicht für den Verantwortlichen (Arbeitgeber) und für von ihm beauftragte Beschäftigte, wie zum Beispiel die der Personalverwaltung. So handeln die Beschäftigten der Personalverwaltung als sogenannte Erfüllungsgehilfen für den Verantwortlichen, und die entsprechenden Datenverarbeitungen (auch unrechtmäßige) werden grundsätzlich dem Verantwortlichen zugerechnet. Die oben genannten Daten (Kündigungsgrund, Arbeitsunfähigkeit) sind auch Gegenstand der Personalakte (sogenannte Perso-

nalaktendaten). Das Gebot der Gewährleistung der Vertraulichkeit in Bezug auf Personalaktendaten ist eine Verpflichtung des Arbeitgebers, die sowohl innerhalb der Dienststelle bzw. des Betriebes und auch gegenüber außenstehenden Dritten besteht. Die Personalakte ist daher vertraulich zu behandeln, vor unbefugter Einsicht zu schützen und der Zugriff nur für solche Beschäftigten und auf solche Daten zuzulassen, wie dies im Rahmen der Personalverwaltung erforderlich ist. Insbesondere müssen sensible Daten – wie die Angaben über gesundheitliche Verhältnisse – vor allem vor missbräuchlicher Verwendung, wozu auch eine Offenbarung gegenüber unbefugten Beschäftigten oder Dritten gehört, geschützt werden.

Was ist zu tun?
Personalaktendaten sind vertraulich zu behandeln. Daher sind sie auch nicht mündlich zu offenbaren.

2 Grundsätze der Datenverarbeitung

2.1 Rechtmäßigkeits-voraussetzungen der Datenverarbeitung

2.1.1 Mieterhöhungsverlangen auf der Grundlage der Nennung von Vergleichswohnungen

↗ § 558a BGB; Art. 5 Abs. 1 Buchst. c, Art. 6 Abs. 1 Buchst. f, Art. 13, 14, 21 Abs. 1 DSGVO

Kurz vor Jahresende bin ich gehäuft zu Mieterhöhungsverlangen auf der Grundlage der Nennung von Vergleichswohnungen angefragt worden. Die Vergleichswohnungen waren dabei mit Namen der jeweiligen Mieterinnen und Mieter, deren Anschrift, der Wohnungsnummer, der Wohnfläche und der Grundmiete bezeichnet. Die benannten Wohnungen befanden sich teilweise auch in Wohnobjekten anderer Vermieterinnen und Vermieter. An mich gewandt haben sich sowohl selbst betroffene Mieterinnen und Mieter als auch hinweisgebende Personen; Letztere waren dabei regelmäßig Adressaten der Mieterhöhungsschreiben.

Mieterhöhungsverlangen müssen gemäß § 558a Abs. 2 des Bürgerlichen Gesetzbuches (BGB) begründet werden. In § 558a Abs. 2 Nr. 4 BGB wird den Vermietern die Möglichkeit eröffnet, die Begründung anhand von drei Vergleichswohnungen vorzunehmen. Erfolgt die Begründung in dieser Weise, so soll die Mieterin oder der Mieter durch die Benennung einzelner Wohnungen die Möglichkeit haben, sich über die Vergleichswohnungen zu informieren und die behaupte-

te Vergleichbarkeit nachzuprüfen. Die Vergleichswohnungen müssen deshalb so genau bezeichnet werden, dass die Mieterin oder der Mieter sie ohne nennenswerte Schwierigkeiten auffinden kann.

Die Mitteilung der Namen der zu Vergleichszwecken herangezogenen Mieter im Erhöhungsschreiben sowie weiterer Angaben, die im Hinblick auf die Beurteilung der Vergleichbarkeit der Wohnungen erforderlich sind, ist damit grundsätzlich zulässig und ist auch schon Gegenstand höchstrichterlicher Rechtsprechung gewesen. So findet sich beispielsweise im Beschluss des Bundesverfassungsgerichts vom 8. September 1993 (1 BvR 1331/92, juris) die Aussage, dass den Anforderungen an die Begründung eines Erhöhungsverlangens genügt ist, wenn die Mieterin oder der Mieter Informationen über Namen des Wohnungsinhabers, Adresse, Geschoss und Quadratmeterpreis vergleichbarer Wohnungen erhält, die ihr bzw. ihm eine eigene Nachprüfung ermöglichen. Aus datenschutzrechtlicher Sicht kann die Weitergabe der Mieterdaten auf eine Interessenabwägung nach Art. 6 Abs. 1 Buchst. f DSGVO gestützt werden; eine ausdrückliche Zustimmung der Mieterin oder des Mieters muss nicht eingeholt werden.

Gleichwohl empfehle ich wegen des Grundsatzes der Datenminimierung (Art. 5 Abs. 1 Buchst. c DSGVO) regelmäßig, in Mieterhöhungsverlangen auf das Nennen der Namen der Mieterinnen und Mieter der Vergleichswohnungen jedenfalls dann zu verzichten, wenn die Vergleichswohnung auch ohne diese Angabe mit Adresse, Geschoss, Lage und gegebenenfalls Wohnungsnummer hinreichend genau beschrieben werden kann. Darüber hinaus gilt, dass Vermieterinnen oder Vermieter bei derart begründetem Mieterhöhungsverlangen neben ihren und den Belangen der in Bezug auf die Mieterhöhung adressierten Mieterin bzw. des Mieters auch die Interessen der Parteien zu berücksichtigen haben, die die Vergleichswohnungen vermieten oder gemietet haben und die, soweit möglich, ungenannt bleiben wollen. Dem steht nicht entgegen, dass durch Erkundigungen des Mieters oder im Falle eines Rechtsstreits über das Mieterhöhungsverlangen

die Namen der Mieterinnen und Mieter der Vergleichswohnungen möglicherweise ohnehin aufgedeckt werden. Denn in den nicht wenigen Fällen, in denen sich die Mieterin bzw. der Mieter dem Mieterhöhungsverlangen nicht verschließt, bleibt die gewünschte Anonymität der Vermieterinnen, Vermieter oder Mieterinnen, Mieter der Vergleichswohnungen gewahrt (BGH, Rechtsentscheid in Mietsachen vom 20. September 1982 – VIII ARZ 1/82 –, juris, Rn. 16–17).

Grundsätzlich begegnet es gleichfalls keinen datenschutzrechtlichen Bedenken, wenn zur Begründung eines Mieterhöhungsverlangens auch Vergleichswohnungen anderer Vermieterinnen oder Vermieter benannt werden. Generell hinzuweisen ist jedoch auf die je nach Konstellation in Art. 13 bzw. Art. 14 DSGVO verankerten Informationspflichten. Aus den auf dieser Grundlage bereitgestellten Informationen muss für die betroffene Mieterin oder den betroffenen Mieter nachvollziehbar hervorgehen, dass Daten zu seinem Mietverhältnis gegebenenfalls auf der Grundlage einer Interessenabwägung an andere Mieterinnen, Mieter bzw. auch Vermieterinnen, Vermieter zweckgebunden zur Begründung von Mieterhöhungsverlangen weitergegeben werden können. Sodann hat sie bzw. er gegebenenfalls die Möglichkeit, diesbezüglich ihr bzw. sein Widerspruchsrecht nach Art. 21 Abs. 1 DSGVO geltend zu machen.

Was ist zu tun?
Vermieterinnen und Vermieter haben die Möglichkeit, ein Mieterhöhungsverlangen auch mit der Nennung von mindestens drei Vergleichswohnungen zu begründen. Die Vergleichswohnungen müssen dabei so genau bezeichnet werden, dass die Mieterin bzw. der Mieter sie ohne nennenswerte Schwierigkeiten auffinden kann. Die Nennung des Mieternamens ist dabei grundsätzlich zulässig, nichtsdestoweniger wird empfohlen, die Wohnung davon unabhängig eindeutig zu beschreiben, etwa durch eine der Mieterin bzw. dem Mieter bekannte Wohnungsnummer.

2.1.2 Abforderung einer Ausweiskopie bei Untervermietung

↗ § 540 Abs. 1 Satz 1, § 553 Abs. 1 Sätze 1 und 2 BGB; § 20 Abs. 2 Sätze 1, 2 und 4 PAuswG; Art. 5 Abs. 1 Buchst. c DSGVO

Nicht selten betreffen an mich herangetragene Fragestellungen auch den Umgang mit personenbezogenen Daten bei großen Hausverwaltungen. So lag dies auch in dem Fall eines Mieters, der eine andere Person zur Untermiete einziehen lassen wollte. Zwecks Zustimmung hierzu wandte er sich an die zuständige Hausverwaltung. Diese forderte ihn daraufhin zur Vorlage einer ungeschwärzten Kopie des Personalausweises des künftigen Untermieters auf. Auf das

Angebot des Mieters, dass sich der potenzielle Untermieter zur Verifikation seiner Person persönlich bei der Hausverwaltung vorstellt, reagierte diese abschlägig. Deshalb wandte dieser sich hilfesuchend an meine Behörde.

Ausgangspunkt für die von der Hausverwaltung gestellte Forderung war der von dem Mieter geltend gemachte Anspruch auf Untermietung eines Teils seiner Mietwohnung. Denn einer Mietpartei ist es nicht erlaubt, Teile der Mietwohnung ohne Weiteres einer dritten Person zu überlassen, § 540 Abs. 1 Satz 1 Bürgerliches Gesetzbuch (BGB).

Rechtlich gesehen darf eine Mietpartei einzelne oder mehrere Räume ihrer Mietwohnung an eine dritte Person untervermieten. Dem Ansinnen auf Untervermietung hat die vermietende Person grundsätzlich zu entsprechen und der Mietpartei die Erlaubnis hierzu zu erteilen, hat sie doch einen rechtlichen Anspruch auf die Erlaubniserteilung, § 553 Abs. 1 Satz 1 Bürgerliches Gesetzbuch (BGB). Ablehnen kann die vermietende Person die Erlaubnis nur im Ausnahmefall, etwa, wenn in der Person des Dritten ein wichtiger Grund liegt, § 553 Abs. 1 Satz 2 BGB. Dies ist der Fall, wenn ihr die Person der Untermieterin/des Untermieters nicht zuzumuten oder nicht tragbar ist.

Für die Entscheidung über den Mieterantrag benötigt die vermietende Person also ein Mindestmaß an Informationen über die Person, die Untermieter/in werden soll. Nur dann kann sie sich auch ein Bild von dieser machen. Auskünfte über die untermietende Person kann sie nur von der Mietpartei erhalten, die der vermietenden Person die für die Entscheidung notwendigen Informationen zu geben hat. Hierzu gehören der vollständige Name, das Geburtsdatum, der Beruf der potenziellen untermietenden Person oder auch der Grund der Untervermietung. Nicht vorgeschrieben und auch nicht erforderlich ist es jedoch, dass die Mietpartei eine Ausweiskopie der oder des Dritten vorlegt.

Der Umgang mit Personalausweisen ist im Personalausweisgesetz (PAuswG) geregelt. Danach darf nur der Ausweisinhaber selbst oder eine Person, der gegenüber er eine Zustimmung erteilt hat, den Ausweis ablichten, § 20 Abs. 2

Satz 1 PAuswG. Andere Personen als die Ausweisinhabenden dürfen die Kopie nicht an Dritte weitergeben, § 20 Abs. 2 Satz 2 PAuswG. Dritte in diesem Sinne ist jede Person oder Stelle, für die die ausweisinhabende Person keine Zustimmung erteilt hat. Die Weitergabe einer Ausweiskopie an eine dritte Person ist somit auch nicht mit Zustimmung der ausweisinhabenden Person möglich. Dem Interesse der Hausverwaltung wäre somit Genüge getan, wenn sie durch Einsichtnahme in den Personalausweis die Angaben der potenziellen untermietenden Person überprüft und dies für sich dokumentiert. Ich teilte dem Mieter dementsprechend mit, dass ich den von ihm vorgeschlagenen Weg, dass sich der Dritte selbst bei der Hausverwaltung persönlich vorstellt, für die beste und praktischste Alternative halte.

Denn der Hauptzweck des Personalausweises liegt gerade darin, dass dieser als amtliche Urkunde zur Identitätsfeststellung dient. Hierzu reicht im Regelfall eine einfache Sichtkontrolle. Eine Ausweiskopie enthält eine Vielzahl von Informationen, die schlicht für eine Identifizierung nicht erforderlich sind, wie Ausweisnummer, Geburtsort oder Körpergröße. Keinesfalls ist deshalb die Erstellung einer ungeschwärzten Ausweiskopie zulässig. Zwar darf der Ausweis abgelichtet werden, jedoch nur von der ausweisinhabenden Person oder von anderen Personen mit Zustimmung der Ausweisbesitzerin/des Ausweisbesitzers, wobei die Ablichtung eindeutig und dauerhaft als Kopie erkennbar sein muss, § 20 Abs. 2 Satz 1 PAuswG.

Im Übrigen greifen neben den Vorschriften des Personalausweisgesetzes die datenschutzrechtlichen Vorschriften, § 20 Abs. 2 Satz 4 PAuswG. Werden auf der Grundlage der Ausweiskopie darin enthaltene personenbezogene Daten notiert oder in ein Computerprogramm eingegeben und anschließend weiterverarbeitet, ist hierzu die Einwilligung der ausweisinhabenden Person notwendig, Art. 6 Abs. 1 Buchst. a Datenschutz-Grundverordnung. Denn die in § 20 Abs. 2 Satz 1 PAuswG enthaltene Zustimmung bezieht sich nur auf die Anfertigung einer Ausweiskopie. Sie ist keine Einwilligung im datenschutzrechtlichen Sinne in die (eigentliche)

Verarbeitung der Ausweisdaten. Über die Vorschrift des § 20 Abs. 2 Satz 4 PAuswG ist somit klargestellt, dass sich die Verarbeitung einzig nach den datenschutzrechtlichen Vorschriften bemisst.

Ob es in dem an meine Behörde herangetragenen Fall letztlich noch zu einer für alle Seiten zufriedenstellenden Lösung kam und der Dritte als Untermieter einziehen konnte, habe ich nicht erfahren. Gerade in Zeiten der Digitalisierung und des durch den Technikeinsatz bestehenden Missbrauchspotenzials sollte jeder wachsam sein. Dies gilt speziell dann, wenn aus Gründen der Identifikation der ausweisinhabenden Person oder gar einer bzw. eines Dritten die Herausgabe einer (ungeschwärzten) Ausweiskopie verlangt wird.

Was ist zu tun?
Eine vermietende Person darf von der Mietpartei keine Vorlage der Ausweiskopie des künftigen Untermieters bzw. der künftigen Untermieterin verlangen. Es reicht eine einfache Sichtkontrolle, wenn dies von der ausweisinhabenden Person angeboten wird.

2.1.3 Nachweis der Arbeitsunfähigkeit mittels elektronischer Arbeitsunfähigkeitsbescheinigung

↗ § 5 Abs. 1a Satz 2 EFZG

Ein Beschäftigter wandte sich im Berichtszeitraum mit einer Beschwerde an meine Behörde. Er teilte mir mit, dass sein Arbeitgeber im Falle einer Krankschreibung ein schriftliches Attest des behandelnden Arztes verlange, da diese nur noch elektronisch vorläge und von seinem Arbeitgeber abgerufen werden müsste. Daher sollten nunmehr die Beschäftigten den sogenannten Beleg für den Versicherten an den Arbeitgeber übermitteln. Dieser Beleg enthalte jedoch (ärztliche) Diagnosen, die den Arbeitgeber nichts angingen. Er habe daher die Diagnosen geschwärzt. Der Beschwerdeführer fragte meine Behörde, ob dieses Vorgehen des Arbeitgebers mit den Datenschutzregelungen vereinbar sei.

Ich habe dem Beschwerdeführer zunächst mitgeteilt, dass den Arbeitnehmer bei einer Arbeitsunfähigkeit zwei unterschiedliche Verpflichtungen treffen, § 5 Abs. 1 Entgeltfortzahlungsgesetz (EFZG). Zum einen ist der Arbeitnehmer verpflichtet, dem Arbeitgeber die Arbeitsunfähigkeit und deren voraussichtliche Dauer unverzüglich mitzuteilen (sogenannte Mitteilungspflicht nach § 5 Abs. 1 Satz 1 EFZG).

Dauert die Arbeitsunfähigkeit länger als drei Kalendertage, hat der Arbeitnehmer dem Arbeitgeber am darauffolgenden Arbeitstag eine ärztliche Arbeitsunfähigkeitsbescheinigung in Papierform vorzulegen, sofern der Arbeitgeber dies nicht vertraglich oder im Einzelfall durch Weisung bereits zu einem früheren Zeitpunkt verlangen kann (sogenannte Nachweispflicht nach § 5 Abs. 1 Satz 2 EFZG).
Seit der Einführung der elektronischen Arbeitsunfähigkeitsbescheinigung (eAU) ab dem 1. Januar 2023 gilt die Mitteilungspflicht unverändert, anstelle der oben genannten Nachweispflicht besteht jedoch nunmehr eine sogenannte Feststellungspflicht, wonach gesetzlich krankenversicherte Arbeitnehmer/innen ihre Arbeitsunfähigkeit nur durch eine Ärztin bzw. einen Arzt feststellen lassen müssen (§ 5 Abs. 1a Satz 2 EFZG).
Für den/die gesetzlich versicherte/n Arbeitnehmer/in besteht außerdem die Obliegenheit, sich eine lediglich für ihn/sie bestimmte Arbeitsunfähigkeitsbescheinigung in Papierform aushändigen zu lassen (Ausfertigung für den/die Versicherte/n, die auch die ärztliche Diagnose enthält).
Der/Die Arbeitgeber/in erhält von dem/der Arbeitnehmer/in daher keine Arbeitsunfähigkeitsbescheinigung in Papierform mehr, sondern muss die Arbeitsunfähigkeitsdaten bei der Krankenkasse elektronisch abrufen.
Das elektronische Verfahren ab dem 1. Januar 2023 gilt grundsätzlich für alle gesetzlich krankenversicherten Arbeitnehmer/innen und wenn die Feststellung der Arbeitsunfähigkeit durch eine/n an der vertragsärztlichen Versorgung teilnehmende/n Ärztin bzw. Arzt oder Einrichtung erfolgt.
Die Änderungen gelten jedoch nicht:

- für privat krankenversicherte Arbeitnehmer/innen, für gesetzlich krankenversicherte Arbeitnehmer/innen, deren Arbeitsunfähigkeit durch eine/n Ärztin bzw. Arzt festgestellt wurde, die/der nicht an der vertragsärztlichen Versorgung teilnimmt (Privatärztin bzw. -arzt),
- bei Krankschreibung von einer Ärztin bzw. einem Arzt im Ausland,

- für geringfügig Beschäftigte (Minijobber/innen) in Privathaushalten,
- bei Krankschreibung in Rehabilitationseinrichtungen,
- bei Krankschreibung wegen Mutter-Kind-Kur,
- bei „Krankschreibung" wegen Erkrankung des Kindes (für den Bezug von Kinderkrankengeld).

In diesen Fällen bleibt es bei dem bisherigen Prozedere, das heißt, der/die Arbeitnehmer/in ist verpflichtet, dem/der Arbeitgeber/in eine Arbeitsunfähigkeitsbescheinigung in Papierform vorzulegen (Nachweispflicht).
Daneben gilt das elektronische Verfahren nicht, wenn keine abruffähige Fehlzeit vorliegt, etwa beim Beschäftigungsverbot während der Schwangerschaft.
Ich habe dem Beschwerdeführer daher mitgeteilt, dass grundsätzlich keine Verpflichtung besteht, eine Arbeitsunfähigkeitsbescheinigung in Papierform vorzulegen, soweit er gesetzlich krankenversichert sei und keine der zuvor genannten Ausnahmen vorliegen. Weiterhin habe ich darauf hingewiesen, dass bei Vorlage des Beleges für den Versicherten der Beschäftigte in jedem Fall berechtigt sei, die ärztlichen Diagnosen zu schwärzen.

Was ist zu tun?
Für gesetzlich Krankenversicherte besteht keine Verpflichtung zur Vorlage der Arbeitsunfähigkeitsbescheinigung in Papierform. Bei Vorlage eines Versichertenbelegs sind Beschäftigte berechtigt, die ärztlichen Diagnosen zu schwärzen.

2.1.4 (Unrechtmäßige) Mitnahme von (Kunden-)Daten durch ausscheidende Arbeitnehmer/innen

↗ Art. 5 Abs. 1 Buchst. b, Art. 6 Abs. 1 Buchst. f DSGVO; § 3 UWG

Im Berichtszeitraum hatte ich den Hinweis bekommen, dass ein im Pflegebereich tätiges Unternehmen mit Sitz in Sachsen Kundendaten eines konkurrierenden Unternehmens in einem nicht unerheblichen Umfang nutzt, um die Kundinnen und Kunden des konkurrierenden Unternehmens mit dem Ziel anzuschreiben, zu ihrem Unternehmen zu wechseln.
Die Kundendaten erhalten hatte das Unternehmen von einer ehemaligen Mitarbeiterin des konkurrierenden Unternehmens, welche nunmehr bei dem sächsischen Unternehmen tätig gewesen ist. Die angeschriebenen Kundinnen und Kunden

wurden durch die Mitarbeiterin während ihrer Tätigkeit für das konkurrierende Unternehmen – den alten Arbeitgeber – persönlich betreut.

Verlassen Beschäftigte mit intensiverem persönlichen Kundenkontakt ihre/n Arbeitgeber/in, haben sie aufgrund des aufgebauten wechselseitigen Vertrauens regelmäßig die Überlegung, die bisher von ihnen betreuten Kundinnen und Kunden mitzunehmen. Aufgrund der arbeitsvertraglichen Treuepflicht dürfen Beschäftigte selbst aber keine Abwerbungshandlungen vornehmen oder aber Kundendaten aus dem System der/des Arbeitgebers/in mitnehmen.

Das Verhalten der ehemaligen Mitarbeiterin des konkurrierenden Unternehmens hinsichtlich etwaiger vorgenommener Abwerbe- und Mitnahmehandlungen war in Ermangelung eines Wohnsitzes im Freistaat Sachsen und einer damit verbundenen fehlenden örtlichen Zuständigkeit seitens meiner Behörde durch mich datenschutzrechtlich nicht zu bewerten. Durch mich aufzuklären und zu prüfen war aber, ob die Verarbeitung der Kundendaten durch das im Freistaat Sachsen ansässige Pflegeunternehmen rechtlich zulässig gewesen ist.

Das durch mich zu prüfende Unternehmen hatte gegenüber meiner Behörde im Rahmen seiner Anhörung eingeräumt, dass es die Kundendaten in sein Datensystem übernommen und sämtliche Kundinnen und Kunden angeschrieben hatte. Von den angeschriebenen Kundinnen und Kunden entschieden sich rund 38 Prozent für einen Wechsel zu dem sächsischen Unternehmen.

Die datenschutzrechtliche Zulässigkeit der Speicherung und Nutzung der personenbezogenen Daten der Kundinnen und Kunden habe ich aufgrund der Tatsache, dass es sich hier nur um Kontaktdaten gehandelt hat, anhand des Maßstabes des Art 6 Abs. 1 Datenschutz-Grundverordnung (DSGVO) geprüft. Im Ergebnis meiner Bewertung habe ich die Speicherung und Nutzung der Kundendaten für nicht rechtmäßig erachtet, da keiner der hier in Betracht kommenden Erlaubnistatbestände des Art. 6 Abs. 1 DSGVO einschlägig gewesen ist.

Anhaltspunkte, wonach die angeschriebenen Kunden in die Speicherung und Nutzung ihrer Daten zum Zwecke der Kontaktaufnahme gemäß Art. 6 Abs. 1 Buchst. a DSGVO wirksam eingewilligt hatten, bestanden im Ergebnis meiner Ermittlungen nicht.

Die Speicherung und Nutzung der Kontaktdaten konnte auch nicht auf Art. 6 Abs. 1 Buchst. b DSGVO gestützt werden, da die Kontaktaufnahme mit dem Ziel des Abschlusses eines neuen Vertrages nicht von den Kundinnen und Kunden selbst, sondern von dem sächsischen Unternehmen ausgegangen war.

Auch konnte dieses gegenüber meiner Behörde kein eigenes und ein gegenüber den angeschriebenen Kundinnen und Kunden vorrangig zu berücksichtigendes berechtigtes Interesse im Sinne von Art. 6 Abs. 1 Buchst. f DSGVO nachweisen. Anerkannte berechtigte Interessen sind dabei solche, die nach der Rechtsordnung der Europäischen Union oder des anwendbaren Rechts eines Mitgliedstaates verfolgt werden können.

Das von meiner Behörde zu prüfende Unternehmen hatte diesbezüglich geltend gemacht, mit der Speicherung und Verwertung der Kontaktdaten ein eigenes Interesse hinsichtlich der Fortführung der weiteren Betreuung der Kundinnen und Kunden zu verfolgen. Aus meiner Sicht steht dies aber im Widerspruch zur Rechtsordnung.

Das konkurrierende Unternehmen hatte die Daten seiner Kundinnen und Kunden, die durch die ausscheidende Mitarbeiterin betreut wurden, in seinem System zu deren Betreuung gespeichert. Das sächsische Unternehmen hatte die Daten der Kundinnen und Kunden von der Mitarbeiterin erhalten, in sein System übernommen und zur Kontaktaufnahme genutzt.

Da die Kundendaten aber allein für die Betreuung der Kundinnen und Kunden durch das konkurrierende Unternehmen nach dem alten bestehenden Pflegevertrag gedacht waren, stellt die Übernahme und die Nutzung der Daten zur Kontaktaufnahme durch das sächsische Unternehmen eine nicht mit diesem Zweck zu vereinbarende Nutzung und damit einen Verstoß gegen Art. 5 Abs. 1 Buchst. b DSGVO dar.

Unabhängig hiervon bin ich der Auffassung, dass es sich um eine unlautere geschäftliche Handlung im Sinne von § 3 Gesetz gegen den unlauteren Wettbewerb (UWG) handelt, wenn ein/e ehemalige/r Mitarbeiter/in eines Unternehmens Kundendaten ihrer/seines früheren Arbeitgebers/in entwendet und die/der neue Arbeitgeber/in diese nun nutzt, indem sie/er die Kundinnen und Kunden des Konkurrenzunternehmens mit dem Ziel eines Wechsels des Unternehmens anschreibt.
Des Weiteren hat sich für mich im Ergebnis meiner Ermittlungen kein Erfordernis zur Übernahme und Nutzung der Kundendaten durch das sächsische Unternehmen im Sinne von Art. 6 Abs. 1 DSGVO ergeben.
Im Ergebnis waren daher durch das sächsische Unternehmen zumindest die Daten von den Kundinnen und Kunden vollständig zu löschen, mit denen kein neues Vertragsverhältnis begründet werden konnte. Auf meinen Hinweis wurde die vollständige Löschung durch das sächsische Unternehmen umgehend vorgenommen und gegenüber meiner Behörde bestätigt, weshalb ich das aufsichtsrechtliche Verfahren mit einer Verwarnung gemäß Art. 58 Abs. 2 Buchst. b DSGVO abschließen konnte.

Was ist zu beachten?
Auch aus datenschutzrechtlicher Sicht dürfen Kundendaten eines Konkurrenzunternehmens nicht mitgenommen und weiterverarbeitet werden.

2.1.5 Auskunftsverlangen des Jugendamts gegenüber einem Arbeitgeber nach dem Unterhaltsvorschussgesetz (UhVorschG)

↗ UhVorschG

Zur Sicherung des Unterhalts von Kindern alleinerziehender Mütter oder Väter gilt der Unterhaltsvorschuss nach dem Unterhaltsvorschussgesetz (UhVorschG) als eine Leistung der öffentlichen Hand. Er wird gewährt, so ein Kind keinen, nicht regelmäßig oder nicht ausreichend Unterhalt von dem barunterhaltspflichtigen Elternteil erhält.
Zur Durchführung dieser Sozialleistung normiert das UhVorschG bestimmte Auskunfts- und Anzeigepflichten, dabei auch gegenüber dem/der Arbeitgeber eines pflichtigen Elternteils.

Was ist zu beachten?
Die Auskunftspflicht des Arbeitgebers nach § 6 Abs. 2 UhVorschG ist lediglich auf Art und Dauer der Beschäftigung, Arbeitsstätte und Arbeitsverdienst beschränkt.

Hierzu weise ich darauf hin, dass sich die Auskunftspflicht des Arbeitgebers nach § 6 Abs. 2 UhVorschG lediglich auf Art und Dauer der Beschäftigung, Arbeitsstätte und Arbeitsverdienst beschränkt und Nachfragen zum Beispiel zu Krankenversicherungen, Bankverbindungen, Gehaltsbescheinigungen etc. nicht vorgenommen werden dürfen.

2.1.6 Durchgangsverkehr auf einem videoüberwachten Kundenparkplatz

↗ § 83 Abs. 1 Satz 1, Abs. 4 SächsBO; Art. 6 Abs. 1 Buchst. b und f DSGVO

Tätigkeitsbericht Datenschutz 2023:
↗ sdb.de/tb2023

Die Anzahl der Supermärkte und Discounter, die Parkraumbewirtschaftungsunternehmen damit beauftragen, die für ihre Kundinnen und Kunden bereitgestellten Parkplätze zu überwachen, nimmt stetig zu. Aus diesem Grund habe ich mich bereits in meinem Tätigkeitsbericht 2023 (2.2.3, Seite 61 ff.) diesem Thema gewidmet. Die an der Zufahrt zu Kundenparkplätzen angebrachten Videokameras finden dem Beschwerdeaufkommen nach kaum noch Beachtung. Offensichtlich ist hier ein Gewöhnungseffekt eingetreten. Ohnehin liegt diesen keine Videoüberwachung im klassischen Sinn zugrunde. Vielmehr erfolgt eine bloße Kennzeichenerfassung um Dauer- oder Fremdparker ausfindig zu machen, die auch sicherheitsrelevante Feuerwehrzufahrten gefährden oder (vermietete) Stellplatzflächen berechtigter Personen blockieren.
Gleichwohl wurde ich in der Berichtsperiode mit einer interessanten Fallgestaltung konfrontiert, die eine solche Kameratechnik betraf. Was war passiert? Ein Anwohner eines Einkaufszentrums bemerkte, dass zur Bewirtschaftung der Parkplätze eine Videokamera im Zufahrtsbereich installiert wurde. Was den Anwohner zu einer Beschwerde veranlasste, war der Umstand, dass das Grundstück des Einkaufszentrums die einzige Zuwegung zu der dahinterliegenden Straße war. Dementsprechend mussten er und die weiteren anwohnenden Personen die videoüberwachten Zufahrten – auch am hinteren Ausgang des Parkplatzes war eine Kamera angebracht – durchqueren, um zu ihren Grundstücken zu gelangen.

Der besorgte Anwohner befürchtete, dass er bei jedem Durchqueren der Durchgangsstraße mit seinem Kfz ebenso wie beim bloßen Passieren von den dortigen Videokameras erfasst wird. Nachdem dies nicht völlig ausgeschlossen erschien, konfrontierte ich das mit der Parkraumbewirtschaftung beauftragte Unternehmen mit dem Sachverhalt. Dieses stellte mir zunächst die Überfahrsituation näher dar.

Es existiert zwar keine Grunddienstbarkeit, insbesondere ist im Grundbuch kein Wegerecht vermerkt. Vielmehr war nur im Baulastverzeichnis eingetragen, dass zugunsten der dahinterliegenden Grundstücke eine jederzeit ungehinderte Zufahrt zur Verfügung zu stellen ist (§ 83 Abs. 4 Sächsische Bauordnung – SächsBO). Im Gegensatz zu einem im Grundbuch eingetragenen Wegerecht begründet eine Baulast (nur) die öffentlich-rechtliche Verpflichtung eines Grundstückseigentümers gegenüber der Baubehörde, bestimmte Handlungen im Hinblick auf das Grundstück zu tun, zu dulden oder zu unterlassen (§ 83 Abs. 1 Satz 1 SächsBO). Die rein privatrechtlichen Beziehungen zwischen den Nachbareigentümern werden damit nicht geregelt. Die Baulast hat allein die Funktion, die Voraussetzung für die Erteilung einer Baugenehmigung zu schaffen.

Aber zurück zu den von dem Anwohner monierten Videokameras. Im konkreten Fall sind die zur Kennzeichenerfassung eingesetzten Videokameras so ausgerichtet, dass kein öffentlicher Grund erfasst wird. Nur bei einem von den Videokameras erkannten Kfz-Kennzeichen wird ein Standbild mit dem jeweiligen Kennzeichen generiert. Die räumliche Besonderheit besteht darin, dass bei der Kennzeichenerfassung die eigentlichen Parkflächen nicht von der als Durchgangsweg benutzten Straße abgegrenzt werden können.

Das eingesetzte Kennzeichen-Scanner-System wird erst dann aktiviert, wenn ein Fahrzeug in den Erfassungsbereich der Ein- bzw. Ausfahrt einfährt. Aus datenschutzrechtlicher Sicht war letztlich entscheidend, dass die Kennzeichen der durchfahrenden Fahrzeuge nicht dauerhaft gespeichert, sondern nach erfolgter Ausfahrt unverzüglich gelöscht werden. Da auf dem überwachten Gelände ein Aufenthalt bis

zu zwei Stunden kostenfrei gestattet ist, müssen die Kennzeichen der durchfahrenden Fahrzeuge auch nicht in einer Exklusivliste gespeichert werden. Bei bloßer Durchfahrt wird das Kennzeichen nur kurzfristig erfasst und unmittelbar beim Verlassen des Geländes wieder gelöscht. Wie mir das Unternehmen versicherte, ist auch keine nachträgliche Wiederherstellung der Standbilder möglich. Das Gelände passierende Personen werden nicht erfasst.

Das Unternehmen kann sich in Bezug auf den Durchgangsverkehr zwar nicht auf die Erforderlichkeit der Vertragsdurchführung stützen, vgl. Art. 6 Abs. 1 Buchst. b Datenschutz-Grundverordnung (DSGVO). Denn die Anwohner/innen wollen ja gerade nicht die Parkfläche zum Abstellen ihres Fahrzeugs nutzen. Als Rechtsgrund kommt daher die Wahrung der berechtigten Interessen zum Tragen, siehe Art. 6 Abs. 1 Buchst. f DSGVO.

Das berechtigte Verarbeitungsinteresse liegt darin, die ordnungsgemäße Nutzung der privaten Grundstücksfläche – als Parkfläche für die Nutzer des Einkaufszentrums – sicherzustellen. Das Unternehmen konnte mir nachvollziehbar darlegen, dass es alternativ zum Kennzeichenerfassungssystem keine anderen technischen Möglichkeiten gibt und auch der Einsatz von Kontrollpersonen ausscheidet. Obgleich die Durchfahrt durch den Parkplatz die einzige Zugangs- und Zufahrtsmöglichkeit zu der dahinterliegenden Anwohnerstraße darstellt, überwiegen schließlich auch die schutzwürdigen Interessen der betroffenen Personen (Anwohnerinnen und Anwohner, Besucherinnen und Besucher), gerade vor dem Hintergrund der lediglich auf die Dauer der Durchfahrt begrenzten Speicherung der Kfz-Kennzeichen, nicht die berechtigten Interessen des Marktbetreibers.

Dementsprechend konnte ich den Beschwerdeführer beruhigen und seine Befürchtungen zerstreuen. Mit der eingesetzten Technik lässt sich keinerlei Rückschluss auf das Verhalten der durchfahrenden Personen vornehmen, und es werden auch keine Bewegungsprofile erstellt.

Was ist zu beachten?

Beim bloßen Überqueren eines mit Kameratechnik an den Zufahrten zur Kontrolle der Einhaltung der vorgegebenen Parkzeiten überwachten Parkplatzes werden die bei Einfahrt erfassten Kfz-Kennzeichen mit dem Verlassen des Parkplatzes wieder gelöscht. Diese kurzzeitige Speicherung der Kfz-Kennzeichen kann keine das Betreiberinteresse überwiegenden schutzwürdigen Betroffeneninteressen begründen; ein Datenschutzverstoß liegt nicht vor.

2.1.7 Kennzeichnungspflicht von Tür- und Klingelkameras

↗ § 13 SächsDSDG, Art. 4 Nr. 7 DSGVO

Eine Gemeinde bat mich um Hinweise zur datenschutzrechtlichen Zulässigkeit des Betriebes einer sogenannten Klingelkamera, ferner darum, ob Informationspflichten im Sinne des Art. 13 DSGVO bestehen und wie deren Umfang ausfallen sollte. Die Verantwortlichen wollten eine Wechselsprechanlage mit einer Videoklingel am Eingang des Rathauses anbringen, um Besucherinnen und Besuchern auch außerhalb der Sprechzeiten den Zugang zu ermöglichen.
Ich beantwortete die Anfrage folgendermaßen:

> Betrachtet man die Zulässigkeit des Betriebes einer Tür- und Klingelkamera, so liegt eine Videoüberwachung vor, „wenn mit Hilfe optisch-elektronischer Einrichtungen personenbezogene Daten verarbeitet werden. Dies umfasst jegliche Geräte, die zur längerfristigen Beobachtung und somit für einen Überwachungszweck eingesetzt werden. Eine Videoüberwachung kann daher vorliegen, wenn z. B. mit Webcams, Smartphones, Dashcams, Drohnen, Wildkameras sowie Tür- und Klingelkameras gefilmt wird. Auch wenn beim Einsatz dieser Geräte keine ‚Videoüberwachung' im oben definierten Sinne stattfindet und zunächst kein Überwachungszweck verfolgt wird, richtet sich die Zulässigkeit der Datenverarbeitung nach den Vorschriften der Datenschutz-Grundverordnung (DS-GVO)."
> (OH Videoüberwachung durch nichtöffentliche Stellen)

Orientierungshilfe der Datenschutzkonferenz zur Videoüberwachung durch nichtöffentliche Stellen:
↗ sdb.de/tb2107

Gemäß dem Kurzpapier Nr. 15 der Datenschutzkonferenz stellt die Videobeobachtung in Echtzeit einen Sonderfall dar. Die Videoüberwachung in Echtzeit, bei der eine direkte Übertragung der Bilddaten auf einen Monitor ohne Speicherung der erhobenen Daten erfolgt (Verlängertes Auge, Kamera-Monitor-Prinzip) stellt eine ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten dar und ist demzufolge nach der DSGVO zu beurteilen.

Videoüberwachung nach der Datenschutz-Grundverordnung; Kurzpapier Nr. 15 der DSK:
↗ sdb.de/vue13

Digitale Tür- oder Klingelkameras, die den öffentlichen Raum erfassen, können daher nur unter Zuhilfenahme bestimmter technischer Einstellungen und Vorkehrungen eingesetzt werden. Insbesondere ist die Videobeobachtung bzw. -überwachung auf das erforderliche Maß zu beschränken. Die Datenverarbeitung sowie die Auswahl und Gestaltung der Technik sind an dem Grundsatz der Datenminimierung und Speicherbegrenzung gemäß Art. 5 DSGVO auszurichten.
Grundlegende Voraussetzungen des datenschutzkonformen Betriebs einer Klingelkamera oder Videogegensprechanlage sind:

- Die Kamera darf nur anlassbezogen durch das Klingeln an der Tür aktiviert werden können.
- Die Kamera darf nur den unmittelbaren Eingangsbereich (Nahbereich) vor der Tür erfassen.
- Es darf keine Aufzeichnung der Bilder möglich sein.
- Es darf keine Übertragung des Livebildes über das Internet erfolgen.
- Die technische Einstellung hat so zu erfolgen, dass die Bildübertragung automatisch nach wenigen Sekunden wieder deaktiviert wird.
- Insbesondere sind technischen Vorkehrungen zu treffen, dass eine dauerhafte und anlasslose Bildübertragung des öffentlichen Raums ausgeschlossen ist.

Aufgrund der Anwendung des Datenschutzrechts müssen die Verantwortlichen die Informationspflichten aus der DSGVO und § 13 Sächsisches Datenschutzdurchführungsgesetz (Sächs DSDG) auch beim Einsatz einer Tür- und Klingelkamera erfüllen (Verzeichnis von Verarbeitungstätigkeiten, Hinweispflicht). Ich habe dem Verantwortlichen ein Beispiel für ein Hinweisschild für eine Klingelkamera übermittelt. Auf meiner Website habe ich ein Muster für das Hinweisschild zur Videoüberwachung und das entsprechende Informationsblatt veröffentlicht.

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

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

Was ist zu beachten?
Verantwortliche Stellen müssen die Pflichten aus der DSGVO und § 13 SächsDSDG auch beim Einsatz einer Tür- und Klingelkamera erfüllen (Verzeichnis von Verarbeitungstätigkeiten, Hinweispflicht).

2.1.8 Auswertung von Daten aus einer Videoüberwachung

↗ § 13 Abs. 1 2. Alternative SächsDSDG, Art. 6 Abs. 1 Buchst. f DSGVO

Im Berichtszeitraum erreichte mich eine etwas andere Anfrage zur Videoüberwachung durch eine Gemeinde. Dabei ging es weniger um die Zulässigkeit der Überwachung, sondern vielmehr um die Auswertung und auch Weiterleitung der so erlangten Bilddaten sowohl an die Polizei als auch an die eigenen Bediensteten.

Folgender Sachverhalt wurde mir hierzu berichtet:

Auf Aufnahmen einer stattgefundenen Videoüberwachung des Eingangsbereichs eines Dienstgebäudes sah man, wie eine Person (durch Schmierereien) Sachbeschädigung beging. Die Behörde wollte nun über das Intranet die Bilder zur möglichen Erkennung an die eigenen Bediensteten weitergeben. Hintergrund war die Überlegung, dass derartige Sachbeschädigungen häufig auf eine Unzufriedenheit mit dem Handeln/Entscheiden von Behörden im Zusammenhang stehen. Daher ist es zumindest nicht unwahrscheinlich, dass Beschäftigte den/die Täter/in auf den Aufnahmen erkennen.

Diese Vorgehensweise halte ich für vertretbar. Allerdings nicht – wie die anfragende verantwortliche Stelle angenommen hatte – über die Norm des Art. 6 Abs. 1 Buchst. f Datenschutz-Grundverordnung (DSGVO). Öffentliche Stellen können sich bei der Datenverarbeitung in der Regel nicht auf diese Norm stützen. Das Hausrecht öffentlicher Stellen ist vielmehr – zumindest mittelbar – stets mit ihrer Aufgabenerfüllung verbunden. Die mit der Wahrnehmung verbundenen Grundrechtseingriffe sind deswegen im Bereich der Videoüberwachung nach § 13 Abs. 1 2. Alternative Sächsisches Datenschutzdurchführungsgesetz (SächsDSDG) zulässig, soweit die Voraussetzungen gegeben sind.

Dies erstreckt sich auch auf das Interesse der verantwortlichen Stelle an einer eigenen Aufklärung (und nachfolgender Geltendmachung von Schadensersatz) aufgezeichneter Rechtsverstöße und Delikte. Zwar ist die Behörde keine Strafverfolgungsbehörde, weshalb sie auch keine straf-

rechtlichen Ermittlungen vornehmen darf. Ich sah aber keine zwingenden rechtlichen Gründe, die einer Offenlegung der Bilder gegenüber der eigenen Belegschaft entgegenstünden. Vor dem Hintergrund von § 13 Abs. 2 SächsDSDG „Geltendmachung von Rechtsansprüchen" hielte ich es für kaum begründbar, eigene, innerhalb des Verantwortlichen stattfindende Aktivitäten zur Ermittlung von Schadensverursachern zu versagen. Der Weiterverarbeitungszweck dürfte die Befragung von Mitarbeiterinnen und Mitarbeitern des Verantwortlichen umfassen, die dazu dienen soll, die Personen, die Schaden verursacht haben, namentlich benennen (und dann ggf. verklagen) zu können.

Auch diese Form der Weiterverarbeitung unterliegt natürlich dem Grundsatz der Verhältnismäßigkeit, sodass eine unangemessen lange Speicherung grundsätzlich nicht zulässig ist. So wäre zum Beispiel eine temporäre Einstellung der Bilder im Intranet denkbar. Aber grundsätzlich dürften die Bilder bei einem Straftatverdacht ohnehin bis zur Klärung des Sachverhalts und bis zur erfolgreichen Geltendmachung von Schadensersatz aufbewahrt werden (es sind ja Beweismittel sowohl im strafrechtlichen als auch im zivilrechtlichen Verfahren, wobei Letzteres von der betroffenen Behörde selbst als Partei zu führen wäre).

Jedenfalls ist über § 13 Abs. 2 SächsDSDG und die Geltendmachung von Rechtsansprüchen ein gesetzlicher Zweck bestimmt, der eine Weiterverarbeitung von „eigenen" Videoüberwachungsbildern zur Sachverhaltsaufklärung zulässt.

Wichtig ist aber, dass die Beschäftigten darauf hingewiesen werden, dass eine Weiterleitung an Dritte und Verwendung der Bilder für andere Zwecke unzulässig ist.

Was ist zu tun?

Bilder aus einer Videoüberwachung, die Sachbeschädigungen gegen das Dienstgebäude zeigen, können durch die Behörde an die eigenen Bediensteten zur Identifizierung - unter der strickten Auflage, diese nicht weiterzugeben, verschickt werden.

2.1.9 Videoüberwachung an Schulen

↗ § 13 Abs. 1 SächsDSDG, § 30 Abs. 1 SächsPBG

Da sich sicherheitsrelevante, auch schwerwiegende Vorfälle an und im Umfeld von sächsischen Schulen in der letzten Zeit häuften, wurde im Berichtszeitraum Videoüberwachung

an Schulen durch mehrere Anfragen an meine Behörde thematisiert.
Ausgangspunkt war auch ein Schreiben des Landesamts für Schule und Bildung (LaSuB), das einen bereits im Jahre 2017 veröffentlichten „Rahmenplan für sächsische Schulen zur Bewältigung von Bedrohungs- und Amoksituationen" des Landespräventionsrats Sachsen zitiert. In diesem Rahmenplan wird Videoüberwachung befürwortet:

> „Die Sicherheit, insbesondere in den Eingangsbereichen, lässt sich durch Installation von Videoüberwachungseinrichtungen verbessern. Dadurch kann der kontrollierte Zutritt zum Schulgebäude verbessert und eine abschreckende Wirkung auf unbefugte Personen erzielt werden. Im Hinblick auf eine spätere Identifizierung von Straftätern sind Geräte zur automatischen Bildaufzeichnung und Bildspeicherung erforderlich. Diese sind in einem gesicherten Bereich aufzustellen. Aus datenschutzrechtlichen Gründen ist eine öffentliche Bekanntgabe der Maßnahme, beispielsweise auf Hinweistafeln bzw. durch schriftliche oder mündliche Unterrichtung des berechtigten Personenkreises, erforderlich."

Ich musste den anfragenden Gemeinden indes mitteilen, dass ich diese Ansicht nicht teilen kann, zumal der Plan vor Inkrafttreten der DSGVO erstellt wurde und damit in jedem Fall einer grundsätzlichen Überarbeitung bedarf. Zudem kann eine pauschale Annahme, Videoüberwachung sei zulässig, aus meiner Sicht ganz klar nicht den gesetzlichen Erfordernissen genügen.
Die aus meiner Sicht relevantesten und interessantesten Fragen möchte ich an dieser Stelle wiedergeben.

1. Wer ist verantwortlich für die Videoüberwachung - Schulträger (Gemeinde) oder die Schule selbst?
   Hier kommt es darauf an, wer auf die Videodaten Zugriff hat, also diese erhebt. Regelmäßig ist dies der Schulträger, da er auch für das Schulgebäude und die entsprechende Ausstattung verantwortlich ist.

2. Kann die Gemeinde als Verantwortliche auf dem Gelände der Schule auch als Polizeibehörde im Rahmen der Ermächtigungsgrundlage des § 30 Abs. 1 Sächsisches Polizeibehördengesetz (SächsPBG) videoüberwachen? Dies ist grundsätzlich nicht möglich. Tatbestandsvoraussetzungen dieser Ermächtigungsgrundlage erfordern Tatsachen, die die Annahme rechtfertigen, dass dort künftig erhebliche Gefahren für die öffentliche Sicherheit entstehen. Die Schwelle ist somit sehr hoch. Dies gilt für Zeiten sowohl während als auch außerhalb des Schulbetriebes. Diese Rechtsgrundlage spielt in diesem Zusammenhang deswegen praktisch keine Rolle.
3. Kann eine Videoüberwachung im Eingangsbereich einer Schule während des Schulbetriebs nach § 13 Abs. 1 Sächsisches Datenschutzdurchführungsgesetz (SächsDSDG) zulässig sein? Nach dieser Norm ist die Erhebung personenbezogener Daten mithilfe von optisch-elektronischen Einrichtungen (Videoüberwachung), deren Speicherung und sonstige Verarbeitung nur dann zulässig, soweit dies jeweils zur Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe oder in Ausübung des Hausrechts erforderlich ist und keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen betroffener Personen überwiegen.
   Die Ermächtigungsgrundlage des § 13 Abs. 1 SächsDSDG kann an dieser Stelle auch nur in der Tatbestandsvariante der Ausübung des Hausrechts einschlägig sein. Dass eine Schule nur unter Zuhilfenahme von Videoüberwachung ihren Bildungsauftrag ausüben kann (Erforderlichkeit zur Aufgabenerfüllung), ist nämlich kaum vorstellbar.

Um überhaupt eine Videoüberwachung begründen zu können, müssen schwerwiegende Anhaltspunkte zu ihrer Erforderlichkeit dargelegt werden, so wiederkehrende strafbewährte Vorfälle, denen man nur mit der Überwachung begegnen kann. Die Videoüberwachung des Eingangsbereichs ist zum Beispiel auch nicht stets geeignet, da Personen bei offener

Videoüberwachung sich höchstwahrscheinlich anderweitig unbefugt Zugang zum Schulgelände verschaffen würden.

Es sollte vor allem bedacht werden, dass während der Schulzeiten (verstärkte) persönliche Aufsicht zum einen das mildere Mittel darstellt. Zum anderen dürfte sie auch wegen der deutlich kürzeren Reaktionszeiten effektiver sein. Als ein weniger invasives Mittel kann auch eine sogenannte Videoklingel in Betracht gezogen werden.

In letzter Zeit werden standardmäßig im Zuge von Sanierungsmaßnahmen der Schulen im Eingangsbereich Videoklingeln eingebaut. Die Nutzung erachte ich als zulässig – aber nur dann, wenn die Videoübertragung nicht permanent läuft, sondern nur beim Klingeln, und nach einer bestimmten Zeit wieder ausgeht.

Videoüberwachung an Schulen erachte ich – wenn überhaupt die Hürde der Erforderlichkeit und Geeignetheit erfüllt wird – nach alledem nur außerhalb des Schulbetriebs als statthaft und zulässig. Und auch nur dann, wenn das Schulgelände nicht nach dem Unterricht noch anderweitig genutzt wird, etwa durch Sportvereine. Der öffentliche Raum darf dabei nicht videografiert werden. Auch wenn ich das wachsende Sicherheitsbedürfnis durchaus nachvollziehen kann, ist doch zu bedenken, dass Videoüberwachung einen erheblichen Eingriff in das grundrechtlich garantierte informationelle Selbstbestimmungsrecht darstellt (Art. 1 Abs. 1, Art. 2 Abs. 1 Grundgesetz) und sehr hohen gesetzlichen Anforderungen und Hürden unterliegt.

Zu weiteren Ausführungen betreffend Videoüberwachung verweise ich auf die Broschüre „Achtung Kamera! Hinweise zur Videoüberwachung für Bürgerinnen und Bürger, Wirtschaft und Behörden" (Download: sdb.de/achkam) und die „Orientierungshilfe für die Videoüberwachung durch sächsische Kommunen nach § 13 SächsDSDG und § 30 SächsPBG" (Download: sdb.de/vue16).

Was ist zu tun?
Schulen dürfen während der Schulzeiten grundsätzlich das Schulgelände und auch den Eingangsbereich nicht videoüberwachen.

2.1.10 Weitergabe von Beschwerden an Beschwerdegegner

↗ § 3 Abs. 2 SächsDSDG

Mich erreichten Petitionen im schulischen Bereich dahingehend, dass das Landesamt für Schule und Bildung (LaSuB) hinsichtlich dort eingereichter Beschwerden die jeweiligen Schulen über Beschwerdeführerinnen und Beschwerdeführer sowie den Beschwerdegegenstand informierte. Die Petentinnen und Petenten gingen jedoch davon aus, dass keine entsprechenden Rückmeldungen an die Schule, über die sich beschwert wurde, erfolgten.

Das zur Stellungnahme aufgeforderte LaSuB teilte mir zunächst mit, dass es sich dabei um die gemäß § 3 Abs. 2 SächsDSDG datenschutzrechtlich zulässige Wahrnehmung von Aufsichtsbefugnissen handelte. Zwar seien entgegenstehende Interessen der Beschwerdeführer immer zu berücksichtigen und in Abwägung zu bringen mit dem Interesse an Aufklärung von Versäumnissen durch Handelnde an Schulen. Für eine sachgerechte Bearbeitung sei es jedoch in der Regel erforderlich, die Schulleitungen über die Beschwerdeführerinnen und Beschwerdeführer sowie den Beschwerdegegenstand zu informieren.

Diese Auffassung konnte ich jedoch nicht teilen. In der Regel wird man vielmehr die Gefahr einer Diskriminierung der Beschwerdeführenden nicht ausschließen können und sollte somit die Beschwerdeführenden nach entgegenstehenden Interessen bzw. einer Einwilligung anfragen. Ich forderte das LaSuB daher erneut zur Stellungnahme auf.

Dieses teilte hierauf mit, dass – sofern eine Gefahr von Diskriminierung der Beschwerdeführenden gesehen wird – die Schulleitungen nicht über die Beschwerdeführenden und den Beschwerdegegenstand informiert werden. Zutreffend wies es darauf hin, dass es sich hierbei um eine am Einzelfall ausgerichtete Ermessensentscheidung handelt. Es räumte jedoch ein, dass in den gegenständlichen Petitionen das Ermessen leider nur unzureichend ausgeübt wurde und bedauerte dies. Zugleich nahm es die mit mir geführte Kommu-

Was ist zu tun?
Generell sollten Aufsichtsbehörden bei Beschwerden davon absehen, diese den Beschwerdegegnern zur Stellungnahme zu übermitteln, sofern der Beschwerde nicht ausdrücklich zu entnehmen ist, dass hiergegen keine Bedenken bestehen.

nikation zum Anlass, alle Organisationseinheiten des LaSuB über die vorstehend ausgeführten Grundsätze zur Übermittlung personenbezogener Daten in Kenntnis zu setzen. Ich halte dies für ausreichend und habe die Petentinnen und Petenten entsprechend informiert.

2.1.11 Schulsozialarbeiter im Jugendhilfegesetz

↗ §§ 13, 62 SGB VIII; § 21 LJHG

Mich erreichen zunehmend Anfragen von Schulleitungen bzw. Beschwerden von Eltern wegen der Verarbeitung personenbezogener Daten durch Schulsozialarbeiterinnen und Schulsozialarbeiter. Diese sind regelmäßig Mitarbeitende von externen Stellen. In Abstimmung mit dem Landesamt für Schule und Bildung (LaSuB) vertrete ich dazu folgende Auffassung:
Schulsozialarbeit ist keine originäre Aufgabe der Schule, sondern gemäß § 13a Achtes Buch Sozialgesetzbuch (SGB VIII) eine Aufgabe der Jugendhilfe. Schulsozialarbeit im Freistaat Sachsen ist ein eigenständiges Handlungsfeld der Kinder- und Jugendhilfe am Lern- und Lebensort Schule. Die Träger der Jugendhilfe kooperieren zwar zur Erfüllung ihrer Aufgaben mit der Schule, die Verantwortung für die Datenverarbeitung im Rahmen des Aufgabenfelds der Schulsozialarbeit liegt jedoch bei dem Träger der Jugendhilfe.
Die Schule darf dabei grundsätzlich nicht von sich aus Schulsozialarbeiterinnen und Schulsozialarbeiter mit personenbezogenen Daten von Schülerinnen und Schülern oder Eltern versehen. Das Sächsische Schulgesetz sieht eine solche Datenübermittlung nicht vor. Sie kann auch nicht auf den schulischen Erziehungs- und Bildungsauftrag gestützt werden. Denn dessen Erfüllung obliegt der Schule zwar im Zusammenwirken mit den Eltern, aber nicht in einem weitreichenden Zusammenwirken mit Dritten, deren Tätigkeit von der Schule nicht bestimmt wird und auch kein verpflichtendes, sondern für die Schülerinnen und Schüler freiwilliges Angebot ist. Schulsozialarbeiterinnen und Schulsozialarbei-

ter dürfen daher ohne Einwilligung der Betroffenen keinen Zugriff auf Schülerdaten erhalten.
Aufgrund von § 61 Abs. 3 SGB VIII weise ich darauf hin, dass die Vorschriften des SGB nicht direkt auf Träger der freien Jugendhilfe Anwendung finden.
Die Aufgaben der Schulsozialarbeit sind nach § 13a SGB VIII nach Landesrecht zu regeln. Hier hat nun das „Dritte Gesetz zur Änderung des Landesjugendhilfegesetzes vom 13. Juni 2024" zu einem neuen Abschnitt 5 „Schulsozialarbeit" geführt. Der entsprechende § 21 enthält jedoch keinerlei Regelungen über die Verarbeitung personenbezogener Daten. Eine ausdrückliche Regelung enthält hingegen beispielsweise der mit Gesetz vom 15. Mai 2024 geänderte § 31 Abs. 4 des Niedersächsischen Schulgesetzes oder § 5 Abs. 2 Nr. 5 des Saarländischen Schulwesen-Datenschutzgesetzes vom 10. Juli 2024. Angesichts einer weiterhin fehlenden Regelung in Sachsen wird in § 21 Landesjugendhilfegesetz im Wesentlichen die dargestellte bisherige Praxis festgeschrieben.

Was ist zu tun?
Schulen mit externen Sozialarbeitern sollten darauf achten, dass eine Datenübermittlung an diese in den meisten Fällen nur mit Einwilligung der Schülerinnen und Schüler bzw. deren Personensorgeberechtigten zulässig ist.

Gern hätte ich im Gesetzgebungsverfahren auf diese Regelungsmöglichkeit hingewiesen. Das für den Gesetzesentwurf (LT-Drs. 7/15755) zuständige Sächsische Staatsministerium für Soziales und Gesellschaftlichen Zusammenhalt hat jedoch eine entsprechende Anregung des Landesjugendhilfeausschusses (siehe Seite 47 des Gesetzentwurfs) nicht aufgegriffen und von meiner Beteiligung abgesehen.

2.1.12 Versammlungsaufruf durch Hochschule

↗ SächsHSG

Bereits mein Amtsvorgänger hatte sich mit Aufrufen sächsischer Hochschulen zur Teilnahme an Versammlungen beschäftigt.

18. Tätigkeitsbericht:
↗ sdb.de/tb2111

Im 18. Tätigkeitsbericht zitierte er im Beitrag 5.1.4 (Seite 43 ff.) über die „Weitergehende Nutzung von Beschäftigten- und Studentendaten" die einschlägige höchstgerichtliche Rechtsprechung:

> „Soweit ein Amtsinhaber am politischen Meinungskampf zwischen den politischen Parteien teilnimmt, muss zur Wahrung der Chancengleichheit dieser Parteien sichergestellt sein, dass ein Rückgriff auf die mit dem Amt verbundenen Mittel und Möglichkeiten unterbleibt. Nimmt der Amtsinhaber für sein Handeln die Autorität des Amtes oder die damit verbundenen Ressourcen in spezifischer Weise in Anspruch, ist es im Verhältnis zu den politischen Parteien dem Neutralitätsgebot unterworfen."

Im Berichtszeitraum erhielt ich nun eine Beschwerde wegen einer Rundmail des Studentenrats einer sächsischen Hochschule, in der unter Verwendung des E-Mail-Verteilers dieser Hochschule zu einer Demonstration aufgerufen wurde. Der Studentenrat ist als Organ der Studentenschaft eine Teilkörperschaft der Hochschule und untersteht deren Rechtsaufsicht.

Der Kanzler der zur Stellungnahme aufgeforderten Hochschule hatte mir dazu mitgeteilt, dass er davon ausgeht, dass der Aufruf zu einer „Großdemo für Demokratie" von den Aufgaben des Studentenrats nach § 25 Abs. 3 Nr. 7 Sächsisches Hochschulgesetz (SächsHSG) umfasst ist („Förderung der politischen Bildung, des staatsbürgerlichen Verantwortungsbewusstseins und des zivilgesellschaftlichen Engagements der Studentinnen und Studenten auf der Grundlage der Bürger- und Menschenrechte sowie der freiheitlichen demokratischen Grundordnung").

Ich wies ihn darauf hin, dass im Inhalt der Rundmail jedoch auf eine Seite im Internet verlinkt wurde, auf der es heißt: „Jetzt wollen wir dafür sorgen, dass die [...] an den Wahlurnen verliert." Wegen dieser Verlinkung wurde schließlich nach Rücksprache mit dem Studentenrat entschieden, dass Rundmails, die der Studentenrat versenden möchte, bis auf Weiteres genehmigt werden müssen. Weiterhin hat die Geschäftsführung des Studentenrats eine Selbstverpflichtung zu den Inhalten von E-Mails verfasst, die über den Verteiler versendet werden, um im Sinne des Neutralitätsgebots und

Was ist zu tun?
Generell sollten Hochschulen bei der Versendung von Rundmails darauf achten, dass das Neutralitätsgebot beachtet wird.

zur Erfüllung der Aufgaben der Studentenschaft gemäß § 25 Abs. 3 Nr. 7 SächsHSG relevante Aussagen immer mittels Begründung und Quellenverweisen zu belegen und sie so von Wahlwerbung abzugrenzen.
Ich halte dies für ausreichend und habe den Petenten entsprechend informiert.

2.1.13 Auskunftserteilung aus dem Liegenschaftskataster zum Ausbau des Glasfasernetzes und digitale Daseinsvorsorge

↗ Art. 6 Abs. 1 Buchst. e DSGVO, § 11 Abs. 2 Satz 4 SächsVermKatG

Im Berichtszeitraum wandte sich ein Petent an mich und monierte, dass ein Landkreis seine personenbezogenen Daten (Name und Anschrift) verwendet habe, um im Namen eines Netzanbieters Werbung für den Glasfaseranschluss zu betreiben. Der Landkreis versandte hierzu unaufgefordert entsprechende Schreiben an anliegende Haushalte, da diese an der entsprechend verlegten bzw. geplanten Trasse liegen. Hintergrund ist der vom Bund geförderte Ausbau des Glasfasernetzes, gerade im ländlichen Raum. Der Petent war indes der Ansicht, dass die Verwendung seiner Daten hierfür nicht zulässig sei, und bat mich um datenschutzrechtliche Überprüfung der erfolgten Datenverarbeitung und Weiterleitung.
In den fraglichen Schreiben wird den Anliegern im Zuge des Trassenausbaus die Verlegung eines (aufgrund der staatlichen Förderung) vergünstigten Anschlusses angeboten und in diesem Zug die sogenannte Eigentümer-Gestattung erbeten. Dies ist aber nicht möglich ohne Namen und Anschrift der Eigentümer.
Nach Beschwerdeeingang forderte ich den betreffenden Landkreis zur Stellungnahme auf. Dieser teilte mir mit, dass der Glasfaserausbau auf Grundlage der Richtlinie „Förderung zur Unterstützung des Breitbandausbaus in der Bundesrepublik Deutschland" vom 22. Oktober 2015 nach einem durchgeführten Vergabeverfahren durch ein Privatunternehmen erfolgt. Weiterhin wurde mitgeteilt, dass zur effektiven und

zielgerichteten Durchführung dem Unternehmen ein Muster-Anschreiben an die Anlieger zur Verfügung gestellt wurde und die entsprechenden Daten aus dem Liegenschaftskataster gezogen und weitergegeben worden sind.

Nach daraufhin erfolgter umfassender Prüfung der Sach- und Rechtslage konnte ich im Ergebnis einen datenschutzrechtlichen Verstoß nicht erkennen. Ich kam zu dem Schluss, dass vorliegend für die Datenweitergabe an das Unternehmen die Rechtsgrundlage in den Normen Art. 6 Abs. 1 Buchst. e Datenschutz-Grundverordnung in Verbindung mit § 11 Abs. 2 Satz 4 Sächsisches Vermessungs- und Katastergesetz (SächsVermKatG) zu finden ist.

Nach dieser Norm dürfen Informationen aus den Eigentümerdaten des amtlichen Vermessungswesens juristischen und natürlichen Personen nur bereitgestellt werden, wenn ein berechtigtes Interesse besteht und offenkundig schutzwürdige Interessen Betroffener nicht entgegenstehen.

Bei meiner Prüfung konnte ich dem Landkreis ein berechtigtes Interesse an der Verarbeitung und Übermittlung der personenbezogenen Daten der Grundstückseigentümer attestieren: Dies folgt aus der Tatsache, dass Gebietskörperschaften, vorliegend der Landkreis, für die in ihrem Zuständigkeitsgebiet lebenden Bürgerinnen und Bürger die sogenannte kommunale Daseinsvorsorge tragen. Dazu zählt auch der Breitbandausbau als Teil der sogenannten digitalen Daseinsvorsorge, dies umso mehr im ländlichen Raum. Im digitalen Zeitalter ist eine leistungsstarke und sichere Internetverbindung für viele Bürgerinnen und Bürger privat wie auch beruflich (man denke nur an Homeoffice und mobiles Arbeiten) unabdingbar.

Dies wurde auch bereits 2012 durch den Bundestag so gesehen: „Internet als Teil der staatlichen Daseinsvorsorge", siehe hierzu die Ausarbeitung Deutscher Bundestag – Wissenschaftliche Dienste, Az.: WD 10 – 3000/115-11, abrufbar unter: sdb.de/tb2401.

Daraus lässt sich ableiten, dass den Landkreis und andere Gebietskörperschaften nicht nur das Recht, sondern gar die Pflicht der kommunalen Aufgabe trifft, im Rahmen der be-

stehenden Angebote und Förderungen die eigenen Einwohnerinnen und Einwohner mit leistungsfähigem Internet zu versorgen.

Ich konnte somit das berechtigte Interesse für die Datenweitergabe gemäß § 11 Abs. 2 Satz 4 SächsVermKatG bejahen und teilte dem Landkreis und dem Petenten mit, dass ich in diesem Fall die Datenverarbeitung als zulässig erachte. Hier muss insbesondere das allgemeine Interesse der Bevölkerung an leistungsstarker Internetverbindung bei zunehmender Digitalisierung des öffentlichen und auch privaten Lebens berücksichtigt werden. Ein entgegenstehendes offenkundiges schutzwürdiges Interesse des Betroffenen im vorliegenden Fall war mir nicht ersichtlich.

Diese Linie führt die bereits bestehende Auslegung des berechtigten Interesses an Eigentümerdaten aus dem Liegenschaftskataster fort. In meinem Tätigkeitsbericht 2023 (2.2.28, Seite 111 ff.) berichtete ich über einen mir angetragenen Fall, bei dem das Vermessungsamt aus dem Liegenschaftskataster gemäß gleicher Befugnisnorm Eigentümerdaten an Windkraftunternehmen weitergegeben hat. Auch dies begründet das berechtigte Interesse und ist zulässig. Unbedingte Voraussetzung ist nur, dass das infrage stehende Flurstück sich in einem sogenannten Eignungs- und Vorranggebiet für Windenergie befindet. (Für die Aufstellung der Windräder müssen Kauf- oder Pachtverträge mit den Flächeneigentümerinnen und -eigentümern geschlossen werden. Um deren Daten erst in Erfahrung zu bringen, sind ebenfalls Auskünfte aus dem Liegenschaftskataster notwendig.) Diese Linie wird auch vom Sächsischen Oberverwaltungsgericht getragen.

Für Interessierte ist im oben genannten Beitrag der Sachverhalt und die rechtliche Einordnung eingehend beschrieben.

Tätigkeitsbericht Datenschutz 2023:
↗ sdb.de/tb2023

Was ist zu beachten?
Internet und Bandbreiteausbau zählen zur kommunalen und staatlichen Daseinsvorsorge. Deswegen dürfen Eigentümerdaten aus dem Liegenschaftskataster (nicht dem Grundbuch!) an Netzbetreiber zu Zwecken des Ausbaus von Breitband und Glasfaser übermittelt werden.

2.1.14 Persönliches Aufsuchen von Dienstaufsichtsbeschwerdeführern an ihrer Wohnanschrift ist nicht erforderlich

↗ § 3 SächsDSDG, Art. 5 DSGVO

Eine Petentin schrieb mich an und beschwerte sich darüber, dass ein Polizeibeamter (der Leiter des örtlichen Polizeireviers) zwei Mal innerhalb einer Woche ihre Wohnanschrift aufgesucht habe. Zuvor hatte sie sich bei der obersten Aufsichtsbehörde, dem Sächsischen Staatsministerium des Innern, über einen aus ihrer Sicht unangemessenen Umgang von Polizeibeamten mit ihr bei einem Vorkommnis im Straßenverkehr beschwert. Ihre Beschwerde hatte sie lediglich per E-Mail übersandt, weitere Kontaktdaten wollte sie bewusst nicht offenlegen. Die Petentin zeigte sich verwundert darüber, dass die Polizei Kenntnis von ihrer privaten Wohnanschrift hatte. An beiden Terminen, an denen der Revierleiter ihre Privatwohnung aufsuchte, war sie nicht anwesend; allerdings hätten ihr Sohn und ihr Ehemann ihr berichtet, dass ein Polizist da gewesen sei, der sie habe sprechen wollen.

Im Zuge der Sachverhaltsaufklärung stellte sich heraus, dass das Polizeirevier um eine Zuarbeit zur Bearbeitung der Beschwerde der Petentin gebeten worden war. Dem Revierleiter sei es nicht gelungen, die Beamten, über die sich die Petentin beschwert hatte, zu identifizieren. Aufgrund einer früheren Beschwerde der Petentin sei im Revier ihre Wohnanschrift bekannt gewesen. Der Revierleiter entschied sich, ein persönliches Gespräch mit der Petentin zu führen und sie dazu an ihrer Wohnanschrift aufzusuchen, was allerdings misslang. Auf Nachfrage teilte die Polizei mit, dass die frühere Beschwerde, aus der die Wohnanschrift der Petentin entnommen worden sei, schon einige Jahre zurücklag und unter Verstoß gegen die Aufbewahrungsbestimmungen im Polizeirevier noch vorgelegen habe. Die Unterlagen aus dem früheren Vorgang seien vernichtet und die Bediensteten sensibilisiert worden.

Ich habe der zuständigen Polizeidirektion mitgeteilt, dass sehr fraglich sei, ob das persönliche Aufsuchen von Beschwerdeführerinnen oder Beschwerdeführern für die Bearbeitung

einer Dienstaufsichtsbeschwerde geeignet und erforderlich ist. Das persönliche Aufsuchen durch (uniformierte) Polizeibeamte kann durchaus negative, datenschutzrechtlich relevante Auswirkungen auf das Persönlichkeitsrecht der Betroffenen haben (vgl. OLG Stuttgart, Beschluss vom 26. August 2002 – 1 Ss 230/2002 –, Rn. 11, 15 juris, auch wenn der Entscheidung eine andere polizeiliche Maßnahme zugrunde lag). Dies gilt insbesondere, wenn dadurch Dritte – wie im vorliegenden Fall Familienmitglieder der Petentin – Kenntnis von einem Vorgang erhalten, die sie zuvor möglicherweise nicht hatten. Ebenso wenig können Spekulationen im räumlichen Umfeld der Wohnanschrift über den Grund des polizeilichen Erscheinens ausgeschlossen werden.

Die Polizeidirektion habe ich gebeten, in künftigen Fällen sehr sorgfältig zu prüfen, ob ein Aufsuchen von Beschwerdeführerinnen und Beschwerdeführern für die Vorgangsbearbeitung tatsächlich erforderlich ist (vgl. § 53 Abs. 2 Sächsisches Polizeivollzugsdienstgesetz in Verbindung mit § 3 Sächsisches Datenschutzdurchführungsgesetz); im Regelfall wird die Kontaktaufnahme über den Weg, den Beschwerdeführer/innen zur Einlegung ihrer Beschwerde gewählt haben (hier die E-Mail), ausreichend sein.

Die bestimmungswidrige Aufbewahrung von abgeschlossenen Vorgängen stellte einen Verstoß gegen datenschutzrechtliche Vorschriften dar. Allerdings habe ich angesichts der von der Polizei unverzüglich ergriffenen Maßnahmen von weiteren aufsichtsbehördlichen Schritten abgesehen.

Was ist zu tun?
Das persönliche Aufsuchen von Beschwerdeführerinnen und Beschwerdeführern an deren Wohnanschrift durch (uniformierte) Polizeibedienstete wird zur Bearbeitung einer Dienstaufsichtsbeschwerde grundsätzlich nicht erforderlich sein. Die bestimmungswidrige Aufbewahrung von Unterlagen verstößt gegen datenschutzrechtliche Vorschriften (Art. 5 DSGVO). Die Polizei ist gehalten, ihre Maßnahmen vor Durchführung sorgfältig zu prüfen und Aufbewahrungsbestimmungen einzuhalten.

2.1.15 Fingerabdruckpflicht bei Beantragung von Personalausweisen laut Verordnung (EU) 2019/1157 – Nachtrag zum Tätigkeitsbericht 2023

↗ Verordnung (EU) 2019/1157; Gesetz zur Stärkung der Sicherheit im Pass-, Ausweis- und ausländerrechtlichen Dokumentenwesen

In meinem Tätigkeitsbericht 2023 (2.2.29, Seite 114) habe ich über die Verordnung (EU) 2019/1157 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 20. Juni 2019 zur Er-

Tätigkeitsbericht Datenschutz 2023:
↗ sdb.de/tb2023

höhung 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 – und deren nationalrechtliche Umsetzung berichtet.

Aufgrund dieser Verordnung müssen seit dem 2. August 2021 bei der Beantragung von Personalausweisen EU-weit zwingend Fingerabdrücke abgegeben werden.

Alle EU-Verordnungen sind in den EU-Mitgliedstaaten unmittelbar geltendes Recht, sie sind unmittelbar anwendbar. In der Bundesrepublik Deutschland wurden die einschlägigen Gesetze, zum Beispiel das Passgesetz, durch das „Gesetz zur Stärkung der Sicherheit im Pass-, Ausweis- und ausländerrechtlichen Dokumentenwesen" (verkündet im Bundesgesetzblatt [BGBl]. I 2020, Nr. 60 vom 11.12.2020, Seite 2744) angepasst.

In dem vorgenannten Bericht habe ich auch über ein entsprechendes Verfahren vor dem Europäischen Gerichtshof (EuGH) berichtet – Rechtssache EuGH C-61/22. Vorgelegt wurde die Rechtsfrage, da Zweifel an der Rechtmäßigkeit dieser Verordnung bestanden haben. Zum Zeitpunkt des Redaktionsschlusses des Tätigkeitsberichts 2023 war eine Entscheidung noch nicht verkündet worden.

Dieser rechtliche Schwebezustand führte unter anderem auch dazu, dass das Verwaltungsgericht Hamburg (VG Hamburg – 20 E 377/23) in einem einstweiligen Verfahren einen Anordnungsbeschluss erlassen hatte, der bestimmte, dass Hamburger Bürgerinnen und Bürger einstweilen nicht zur Abgabe von Fingerabdrücken gezwungen werden konnten. Ich musste indes anfragenden sächsischen Bürgerinnen und Bürgern erläutern, dass ein Urteil des Hamburgischen Verwaltungsgerichts keine Rechtswirkungen für andere Bundesländer entfalten kann.

Nunmehr hat der EuGH über die Rechtssache entschieden und die Verordnung als rechtmäßig bestätigt – EuGH, Urteil vom 21.03.2024 - C-61/22. Der Grundrechtseingriff – Grundrechte auf Achtung des Privatlebens (Art. 7 Grundrechte-Charta) und Schutz der personenbezogenen Daten (Art. 8

Grundrechte-Charta) – wurde vom EuGH zwar erkannt, dieser aber als gerechtfertigt angesehen.
Aufgrund eines formalen Fehlers bei der Gesetzgebung (der EU-Gesetzgeber hatte eine falsche Rechtsgrundlage zitiert) ist laut EuGH die Verordnung zwar formal ungültig, bleibt aber befristet weiter wirksam. Dies deswegen, da eine sofortige Ungültigkeit der Verordnung für eine erhebliche Zahl von Unionsbürgerinnen und -bürger schwerwiegende negativen Folgen für ihre Sicherheit haben könnte. Für den Erlass einer neuen Verordnung hat der EuGH dem EU-Gesetzgeber Zeit bis Ende 2026 gegeben.
Die Verordnung wird damit gerechtfertigt, Kriminalität und Terrorismus sowie die Herstellung gefälschter Personalausweise und Identitätsdiebstahl zu bekämpfen. Weiterhin soll sie Überprüfungen erleichtern. Außerdem ermögliche eine zuverlässige Identifizierung den EU-Bürgerinnen und -Bürgern, ihr Recht auf Freizügigkeit in der EU leichter auszuüben. Allein ein Foto als Identifizierungsmittel wäre weniger wirksam, so der EuGH.
Die vorgesehenen Schutzmechanismen – u. a. dürfen Daten nicht in anderen Datenbanken weiterverwendet werden; datenerhebende Behörden dürften die Daten nur zeitlich begrenzt (höchstens 90 Tage) für die Erstellung des Ausweises speichern – sieht der EuGH als ausreichend an.
Für den Reisepass wurde im Übrigen bereits 2013 vom EuGH die Speicherung von Fingerabdrücken als rechtmäßig anerkannt.

Was ist zu beachten?
Der EuGH hat die Pflicht zur EU-weiten Abgabe von Fingerabdrücken bei der Beantragung von Personaldokumenten bestätigt.

2.1.16 Einsatzfahrten der Feuerwehr

↗ Art. 4 Nr. 7 DSGVO

Im Berichtszeitraum wurde ich informiert, dass im Internet zahlreiche Videos aus dem Straßenverkehr von Einsatzfahrten einer sächsischen Feuerwehr veröffentlicht wurden. Es stellte sich heraus, dass es sich um eine ganze Serie von Videos von Einsatzfahrten, Einsatzübungen und echten Einsätzen auf einem Youtube-Kanal handelte.

Im Internet waren beispielweise Videos veröffentlicht, die Fehlverhalten von Verkehrsteilnehmern zeigen sollten. Die Videoaufnahmen enthielten sowohl personenbezogene Daten von Angehörigen der Ortswehr der Gemeinde als auch Daten von Dritten (Personen im öffentlichen Verkehrsraum). Dabei wurde das gesamte Umfeld aufgenommen, ohne dass eine Verpixelung von Personen oder Kennzeichen der Fahrzeuge erfolgte. Zusätzlich wurden auch die Gespräche der Einsatzleitung aufgezeichnet. Auch diese konnten im Internet abgehört werden.

Die Videoüberwachung greift als Datenverarbeitung signifikant in das allgemeine Persönlichkeitsrecht in seiner Ausprägung als „Recht auf informationelle Selbstbestimmung" (Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 Grundgesetz, Art. 33 Verfassung des Freistaates Sachsen) ein. Dieses Recht umfasst die Befugnis des Einzelnen, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden, und daher grundsätzlich selbst über die Preisgabe und Verwendung persönlicher Daten zu bestimmen.

Meine Datenschutzprüfung lief wie folgt ab:

Leider gab es auf diesem Youtube-Kanal kein Impressum, so dass es zunächst unklar war, wem diese Veröffentlichung zuzuordnen war. Die nähere Auswertung eines im Beschwerdesachverhalt konkret benannten Videos ergab, dass die Videos vermutlich durch einen Angehörigen der Feuerwehr oder zumindest mit dessen Erlaubnis entstanden. Die Videokamera war direkt im Führerhaus eines Feuerwehreinsatzfahrzeugs betrieben worden und filmte nach vorn Richtung Fahrzeugführer und Einsatzleiter sowie natürlich auf die Fahrbahn. Auch die Gespräche der Fahrzeugführer und Einsatzleiter konnten mitgehört werden.

Aufgrund der fehlenden Angaben zum verantwortlichen Betreiber des Youtube-Kanals war mir eine Klärung meiner Zuständigkeit sowie ferner ein weiteres Vorgehen in der Sache nicht möglich. Vor diesem Hintergrund musste ich mich zunächst an die Gemeinde der betroffenen Ortsfeuerwehr wenden.

Der sächsischen Gemeinde waren die veröffentlichten Videos im Detail nicht bekannt, jedoch wurden die Einsatzfahrten mit Unterstützung der örtlichen Feuerwehr selbst gefilmt. Diese Videos sollten auf die ungenügende Sorgfaltspflicht der Verkehrsteilnehmer bei der Bildung von Rettungsgassen auf Autobahnen aufmerksam machen.

Die Gemeinde teilte mir mit, dass die Ortswehr eine Dashcam in ihrem Fahrzeug angebracht hatte, welche jedoch dem Inhaber des Youtube-Kanals gehört. Die Ortswehr wollte die Aufnahmen ursprünglich für interne Zwecke nutzen (zum Beispiel für Aus- und Weiterbildungsziele). Sie erlaubte jedoch dem Besitzer der Kamera die Veröffentlichung der Aufnahmen im Internet und gab daher die Videoaufnahmen weiter. Ich musste feststellten, dass – vermutlich seit Inbetriebnahme der Videoanlage – Bildaufnahmen von Einsatzfahrten der Ortswehr gefertigt und gespeichert wurden, ohne vorherige datenschutzrechtliche Prüfung.

Die Gemeinde ist somit gemäß Art. 4 Nr. 7 Datenschutz-Grundverordnung datenschutzrechtlich Verantwortliche für die Videoaufnahmen. Vor diesem Hintergrund ist durch den Verantwortlichen zu prüfen, ob die mithilfe der Dashcam erfolgte Verarbeitung personenbezogener Daten (Videoaufzeichnung einschließlich Veröffentlichung) den rechtlichen Vorschriften entspricht. In den Videoaufnahmen waren sowohl personenbezogene Daten von Angehörigen der Ortswehr (Beschäftigtendatenschutz) als auch Daten von Dritten (Personen im öffentlichen Verkehrsraum) enthalten. Es war nicht ersichtlich, auf welche Rechtsgrundlage die Datenverarbeitung dabei jeweils konkret gestützt werden konnte. Insbesondere für die Weitergabe der Videoaufnahmen an Dritte (hier: an den Besitzer der Videokamera zum Zweck der Veröffentlichung im Internet) konnte ich derzeit keine Verarbeitungsbefugnis erkennen. Diese war daher datenschutzrechtlich nicht zulässig.

Ich habe die Gemeinde aufgefordert, die aktuelle Verfahrensweise unverzüglich einzustellen und sicherzustellen, dass die Übermittlung der Bildaufzeichnungen der Videokameras an Dritte – ohne vorherige datenschutzrechtliche

Was ist zu tun?
Durch den datenschutzrechtlich Verantwortlichen ist vorab zu prüfen, ob die mithilfe einer Dashcam erfolgte Verarbeitung personenbezogener Daten (Videoaufzeichnung einschließlich Veröffentlichung) den rechtlichen Vorschriften entspricht.

Prüfung – unterbleibt. Ferner waren unberechtigt erstellte und veröffentlichte Bildaufnahmen zu löschen.
Abschließend wurde mir durch den Verantwortlichen mitgeteilt, dass der Betreiber des Youtube-Kanals anfänglich nicht bereit war, die Videos der Feuerwehr aus seinem Youtube-Kanal zu löschen. Er ist der Aufforderung jedoch zwischenzeitlich nachgekommen.

2.1.17 Reichweite des Informations- und Akteneinsichtsrechts von Gemeinde- und Stadträten

↗ § 28 Abs. 5 und 6 SächsGemO

Ein Dauerbrenner im kommunalen Datenschutz ist die Frage nach dem Umgang mit personenbezogenen Daten durch Gemeinderätinnen und -räte im Rahmen ihrer Ratsarbeit. Vorliegend wurde durch eine Datenschutzbeauftragte einer Gemeinde folgende Frage thematisiert:
Wie weit reicht das Informations- und Akteneinsichtsrecht von Stadträten gemäß § 28 Abs. 5 und 6 Sächsische Gemeindeordnung (SächsGemO) in sachlicher bzw. inhaltlicher Hinsicht?
§ 28 Abs. 5 SächsGemO räumt dem Gemeinderat ausdrücklich ein umfassendes Informations- und Akteneinsichtsrecht bezüglich aller gemeindlichen Angelegenheiten ein. Ausgenommen hiervon sind nach § 28 Abs. 7 SächsGemO die nach § 53 Abs. 3 Satz 3 SächsGemO geheim zu haltenden Angelegenheiten. So ist aber zumindest aus dem Gesetzeswortlaut nicht offensichtlich, ob der Anspruch auf Einsicht sich auch auf Personal- und Lohnakten, Akten der Kämmerei (Haushalt) und Geschäfte der laufenden Verwaltung (insbesondere Rechnungen) erstreckt.
Um eine einheitliche Rechtsauffassung zu wahren und bei den Gemeinden nicht noch weitere Unsicherheiten zu generieren, wandte ich mich mit dieser Frage an das Sächsische Staatsministerium des Inneren (SMI). Dies hatte schon letztes Jahr als Hilfestellung an Gemeinden ein Hinweisblatt über die Reichweite des Informations- und Akteneinsichtsrechts

nach § 28 Abs. 5 SächsGemO per Rundschreiben versendet. Deswegen war eine bilaterale Abstimmung angezeigt.

Basierend auf der Abstimmung mit dem SMI habe ich der Datenschutzbeauftragten mitgeteilt, dass auch Personal-, Besoldungs- und Steuerakten grundsätzlich vom Recht auf Gewährung von Akteneinsicht umfasst sind. Das Recht ist auch nicht an die Organzuständigkeit der Gemeinde gebunden, sondern umfasst auch die Angelegenheiten, die die/der Bürgermeister/in in eigener Zuständigkeit erledigt, insbesondere also die Geschäfte der laufenden Verwaltung sowie Weisungsaufgaben. Keine Gemeindeangelegenheiten sind demnach hingegen dienstrechtliche Angelegenheiten der Bürgermeisterin/des Bürgermeisters, wie etwa deren/dessen Verpflichtung, eine Erklärung über ihre/seine Nebentätigkeit abzugeben. Dem Gemeinderat kommt keine dienstrechtliche Kontrollfunktion gegenüber dem/der Bürgermeister/in zu.

Das Akteneinsichtsrecht bezieht sich auch nur auf die bei der Verwaltung der Gemeinde vorhandenen Unterlagen, nicht auf solche, die erst beschafft werden müssen, zum Beispiel bei einem Zweckverband. In einer anderen Angelegenheit wollte ein Bürgermeister wissen, ob auch seine ausgetauschten E-Mails mit Bediensteten bezüglich eines Betriebsausfluges unter den Aktenbegriff nach § 28 Abs. 5 SächsGemO fallen. Dies habe ich eindeutig verneint. Dieser erstreckt sich ausdrücklich nur auf Verwaltungsvorgänge, nur diese sind vom Informations- und Akteneinsichtsrecht der Gemeinderäte umfasst.

Stets genau zu prüfen ist auch, ob nicht schutzwürdige Belange Betroffener oder Dritter dem Recht auf Auskunftserteilung und Akteneinsicht entgegenstehen. Derartige Belange können sich aus den Grundrechten, datenschutzrechtlichen Bestimmungen oder der Gemeindeordnung selbst ergeben. Bestehen solche Belange, hat die Bürgermeisterin/der Bürgermeister nach pflichtgemäßem Ermessen zu entscheiden, ob die begehrte Auskunft erteilt bzw. Akteneinsicht gewährt wird oder nicht. Dabei ist die hohe Bedeutung des Informationsanspruchs des Gemeinderats als wichtiges Kontrollinstrument im demokratisch organisierten Gemeinwesen den

schutzwürdigen Belangen Betroffener oder Dritter gegenüberzustellen und zu prüfen, ob und ggf. wie deren Interessen bei Auskunftserteilung oder Gewährung von Akteneinsicht hinreichend geschützt werden können.

Es wäre aber zu kurz gedacht zu unterstellen, dass in keinem Fall Auskünfte zu erteilen sind, wenn in irgendeiner Form Rechte Dritter/Betroffener tangiert werden. Gemeinderatsmitglieder sind schließlich nach § 19 Abs. 2 Satz 1 SächsGemO zur Verschwiegenheit verpflichtet. Unzulässig wäre es deswegen, pauschal zu unterstellen, dass einzelne Gemeinderatsmitglieder die ihnen mitgeteilten Informationen unter Verstoß gegen diese Pflicht an Dritte weitergeben. Auf der anderen Seite kann man auch nicht einen Automatismus annehmen, in dem Sinne, dass jedem Begehren auf Auskunft oder Akteneinsicht schon deshalb zu entsprechen ist, weil die Gemeinderäte zur Verschwiegenheit verpflichtet sind.

Zu prüfen wäre deswegen stets sorgfältig und einzelfallbezogen, ob es Anzeichen für eine Verletzung der Verschwiegenheitspflicht gibt (vgl. OVG Nordrhein-Westphalen, Beschluss vom 22.05.2013 – 15 B 556/13 – juris Rn. 11). In diesem Fall wäre das Akteneinsichtsgesuch abzulehnen, die Entscheidung aber hinreichend zu begründen. Um sicherzustellen, dass Informationen nur in dem Maße bekannt werden, wie dies für die Ausübung des Informationsrechts erforderlich ist, kann zudem die Behandlung in nichtöffentlichen Sitzungen nach § 37 Abs. 1 Satz 1 SächsGemO erfolgen.

Stehen dem Informations- und Akteneinsichtsrecht schutzwürdige Belange Betroffener oder Dritter entgegen, ist zudem zu prüfen, ob eine Schwärzung bzw. Anonymisierung der Informationen infrage kommt. Erst wenn auch dies trotz sorgfältiger Prüfung verneint wird, kann eine gänzliche Ablehnung des Antrages erfolgen.

Was ist zu tun?

Gemäß § 28 Abs. 5 und 6 SächsGemO haben Mitglieder von Gemeinderäten ein umfassendes Informations- und Akteneinsichtsrecht bezüglich aller gemeindlichen Angelegenheiten. Das Recht auf Gewährung von Akteneinsicht umfasst grundsätzlich auch Personal-, Besoldungs- und Steuerakten. Dem Recht nach § 28 Abs. 5 SächsGemO können in Ausnahmefällen schutzwürdige Belange Betroffener oder Dritter entgegenstehen. Daraufhin ist zu prüfen, ob ein Schutz der betroffenen Belange durch Anonymisierung der Informationen möglich ist.

2.1.18 Verpflichtungsgesetz und das kommunale Mandat

↗ § 11 Abs. 1 Nr. 2 und Nr. 4 StGB, § 31 Abs. 3 Satz 1 SächsLKrO, § 35 Abs. 3 Satz 1 SächsGemO, Verpflichtungsgesetz

Das Gesetz über die förmliche Verpflichtung nichtbeamteter Personen vom 2. März 1974 (Verpflichtungsgesetz) besagt, dass Personen auf die gewissenhafte Erfüllung ihrer Obliegenheiten zu verpflichten sind, wenn sie, ohne Amtsträger/in (§ 11 Abs. 1 Nr. 2 Strafgesetzbuch [StGB]) zu sein, bei einer Behörde oder sonstigen Stelle, die Aufgaben der öffentlichen Verwaltung wahrnimmt, beschäftigt oder für sie tätig sind.
Bereits in den Vorjahren habe ich in meinen Tätigkeitsberichten zu Fragen des Verpflichtungsgesetzes berichtet – so Tätigkeitsbericht 2022, (4.2.2, Seite 140 f., abrufbar unter sdb.de/tb2022), Tätigkeitsbericht 2023 (4.3.1, Seite 174 f., abrufbar unter sdb.de/tb2023). Diese betrafen Fragen von Auftragsverarbeitung für öffentliche Stellen.
In diesem Berichtszeitraum wandte sich nun die behördliche Datenschutzbeauftragte einer Kommune an mich mit der interessanten Frage, ob auch Gemeinderätinnen und -räte (gilt entsprechend auch für Kreisrätinnen und -räte) nach dem Verpflichtungsgesetz verpflichtet werden müssen.
Mitglieder des Gemeinderats (entsprechend des Kreistags für Landkreise) sind ehrenamtlich tätig und üben ein ihnen durch Wahl übertragenes Mandat zur Vertretung der Einwohnerinnen und Einwohner aus. Sie sind regelmäßig deswegen gerade nicht als Amtsträger/in im Sinne von § 11 Abs. 1 Nr. 2 StGB anzusehen. Auch sind sie nicht bei der Gemeinde/beim Landkreis „beschäftigt oder für sie tätig" (§ 11 Abs. 1 Nr. 4 StGB).
Das durch Wahl erlangte Mandat „beißt" sich auch mit einem gemeindlichen Beschäftigungs- oder Auftragsverhältnis. Das Mandat ist nämlich frei auszuüben (§ 35 Abs. 3 Satz 1 Sächsische Gemeindeordnung bzw. § 31 Abs. 3 Satz 1 Sächsische Landkreisordnung), entsprechende mit einem Beschäftigungsverhältnis verbundene Weisungsrechte der Gemeinde wären damit nicht zu vereinen. Der Gesetzgeber hat schließ-

lich nicht umsonst die Entscheidung getroffen, das Mandat nicht als Amt auszugestalten. Dies wäre ausgehöhlt, würde man Mandatsträger/innen nach Verpflichtungsgesetz verpflichten.

Was ist zu tun?
Mitglieder des Gemeinderats und des Kreistags sind nicht nach Verpflichtungsgesetz zu verpflichten.

Folglich habe ich der Datenschutzbeauftragten mitgeteilt, dass Mandatsträger/innen nicht nach Verpflichtungsgesetz zu verpflichten sind bzw. auch nicht verpflichtet werden dürfen.

2.2 Einwilligungsfragen

2.2.1 Veröffentlichung von Abbildungen von Kindern in Social Media und Einwilligung von Elternsorgeberechtigten

↗ Art. 2 Abs. 2 Buchst. c DSGVO; Art. 6 Abs. 1 Buchst. a DSGVO

Stets erreichen meine Behörde auch Beschwerden in Bezug auf Abbildungen in Social Media, auch soweit sie Kinder betreffen.

In einem Fall wandte sich beispielsweise ein Vater hilfesuchend an meine Dienststelle und teilte mit, dass er und seine Partnerin ein gemeinsames Kind hätten. Die Kindesmutter würde Abbildungen der Tochter über mehrere internationale soziale Netzwerke verbreiten und weltweit frei zugänglich machen. Er habe die Kindesmutter gebeten, die Veröffentlichungen zu unterlassen, was allerdings ignoriert werde. Auch habe ihm der Anwalt der Mutter mitgeteilt, dass diese die Bilder der Tochter ohne sein Einverständnis veröffentlichen dürfe.

Bei Social-Media-Veröffentlichungen ist zunächst zu fragen, ob eine sogenannte Haushaltsausnahme gemäß Art. 2 Abs. 2 Buchst. c Datenschutz-Grundverordnung (DSGVO) vorliegt. Nach der Vorschrift ist auf rein persönliche oder familiäre Tätigkeiten die Datenschutz-Grundverordnung nicht anwendbar. Nach herrschender Meinung gilt diese Ausnahme allerdings nicht, wenn in sozialen Medien die Internetinhalte für jedermann frei zugänglich sind. Bei bestehender Zu-

gangsbeschränkung würde allerdings die Haushaltsausnahme greifen und die Datenschutz-Grundverordnung sachlich nicht zur Anwendung kommen. In diesen Fällen könnte dann auch kein Datenschutzverstoß vorliegen bzw. wäre eine weitere Befassung meiner Behörde nicht möglich.

Im vorliegenden Fall war im Ergebnis vom freien Zugang zu den Abbildungen auszugehen und daher die Zulässigkeit der personenbezogenen Datenverarbeitung bzw. Veröffentlichung nach dem Erlaubniskatalog des Art. 6 DSGVO zu prüfen, in dem die Befugnisgründe für personenbezogene Datenverarbeitung normiert sind.

Abzuheben war auf eine wirksame Einwilligung. Bei der Verbreitung von Abbildungen von Personen hat regelmäßig eine Einwilligung der betroffenen Person vorzuliegen, Art. 6 Abs. 1 Buchst. a DSGVO. Bei minderjährigen Kindern, die nicht, auch nicht teilweise, geschäftsfähig sind, ist auf die sorgeberechtigte Person abzustellen. Insoweit war bei der Frage der Zulässigkeit der Veröffentlichung der Bilder im Beispielfall entscheidend, ob eine gemeinsame Elternsorgeberechtigung vorgelegen hat oder ob die Mutter allein sorgeberechtigt gewesen ist. Im letzteren Fall entscheidet die Mutter allein. Deren Einwilligung wäre ausreichend gewesen. Grenzen wären nur dann erreicht, wenn das Kindeswohl verletzt wäre, was dann wiederum gerichtlich beim Familiengericht festgestellt werden müsste. Nähere Angaben, welcher Art die Bildaufnahmen gewesen sind, waren seitens des Beschwerdeführers auch nicht mitgeteilt worden.

Bei einem gemeinsamen Sorgerecht wiederum wäre die Ausgestaltung des Sorgerechts zu untersuchen und damit, ob für die Veröffentlichung der Kinderbilder die Einwilligung beider Sorgeberechtigter notwendig ist.

Derartige zivilrechtliche Vorfragen, die in der Praxis auch häufig noch streitig sind, ist meine Behörde nicht gesetzlich berufen zu entscheiden. Auch kann meine Behörde insoweit keinen weitergehenden Rechtsrat erteilen. Dem Beschwerdeführer gegenüber habe ich Entsprechendes umfänglich und aufklärend vermittelt, womit der Vorgang abgeschlossen werden konnte.

Was ist zu beachten?

Im Falle von Social-Media-Veröffentlichungen ist bei frei zugänglichen Abbildungen von Kindern zunächst die Einwilligung der Elternsorgeberechtigten erforderlich. Im Falle eines gemeinsamen Sorgerechts oder streitigen Verhältnissen sollten die interessierten Eltern zivilrechtlichen Rat suchen, den die Datenschutzaufsichtsbehörde bei zivilrechtlichen Vorfragen nicht zu leisten berufen ist.

2.2.2 Informationen beim Online-Ticketverkauf

↗ § 7 UWG, Art. 6 DSGVO

Durch Beschwerdeführende, die den Verkaufsprozess eines Online-Ticketverkäufers bei personengebundenen Tickets abgebrochen hatten, ist mir folgende Formulierung auf der Internetpräsenz des Händlers mitgeteilt worden:

> „Wir gehen davon aus, dass durch Sie registrierte weitere Teilnehmer die entsprechende Erlaubnis zur Verarbeitung der personenbezogenen Daten erteilt haben. Sie haben dafür Sorge zu tragen, dass der entsprechende Nachweis auf Verlangen vorgelegt werden kann. Weiterhin behält sich [der Verantwortliche] vor, die weiteren Teilnehmer über diese und ähnliche eigene Veranstaltungen zu informieren."

Demnach sollten bei Sammelbestellungen der personengebundenen Tickets durch die Kunden, die für weitere Personen mitbestellen wollten, eine Erlaubniserteilung zur personenbezogenen Datenverarbeitung und eine Befugnis, auch die weiteren Ticketinhaber/innen – für die mitbestellt worden ist – mit Werbung oder Mitteilungen zu beschicken, vorausgesetzt werden.
Die chronologisch nachfolgende Checkbox wies sodann bei dem Bestellprozedere folgenden Text auf:

> „Ich bestätige, dass ich mit der o. g. Verarbeitung einverstanden bin. Weiter bestätige ich, dass ggf. weitere, durch mich registrierte Teilnehmer zur o. g. Verarbeitung informiert wurden und ihr Einverständnis gegeben haben."

Ohne dass diese Checkbox angekreuzt worden ist, konnte der Bestellvorgang nicht fortgesetzt werden.
Aus Sicht der Aufsichtsbehörde begegneten die Texte jeweils datenschutzrechtlichen Bedenken. Im Hinblick auf die Verarbeitung der personenbezogenen Daten bei personengebundenen Tickets ist zunächst sicherlich von einer wirksamen Vertretung bzw. zumindest einer Anscheinsvollmacht

auszugehen und dass der Verantwortliche die Informationen aus vertraglichen Gründen zu verarbeiten befugt ist, Art. 6 Abs. 1 Buchst. b Datenschutz-Grundverordnung (DSGVO).
Hingegen ist es grundsätzlich als unzulässig zu betrachten, wenn der Verantwortliche in diesen und vergleichbaren Fällen seine Befugnis voraussetzt, den Personen, für die mitbestellt wurde, Werbung und Mitteilungen zusenden zu dürfen, auch nicht aus berechtigtem Interesse heraus, vgl. Art. 6 Abs. 1 Buchst. f DSGVO.
Auch die beabsichtigte Werbeansprache (mittels E-Mail-Newsletter) insoweit an die Fortsetzung des Bestellvorgangs zu koppeln, war nach meiner Auffassung unzulässig. In Betracht für ein Feld kam daher allenfalls die Bestätigung der Kenntnisnahme der diesbezüglich bereitgestellten Informationen.
Der Verantwortliche hatte mir zugesichert, die diesbezüglichen Kundeninformationen zeitnah zu überarbeiten. Mir stellte sich im Zusammenhang mit Stellvertretungshandlungen zudem die Frage, ob das Bestandskundenprivileg voraussetzungslos auf diejenigen Personen ausgeweitet werden kann, die nicht unmittelbar am Bestellvorgang beteiligt gewesen sind. So geht der Verantwortliche davon aus, dass auch diese Personen nach Vertragsabschluss zu Bestandskunden geworden sind, vgl. § 7 Abs. 3 Gesetz gegen den unlauteren Wettbewerb (UWG). Auch diese Auffassung konnte ich aufgrund der Interessenlage nicht teilen.
Wie sich am Fallbeispiel im Event- und Ticketverkauf gezeigt hat, sollte sprachlich klar kommuniziert und vermieden werden, unterschiedliche, nicht miteinander zusammenhängende Willensbekundungen innerhalb einer Checkbox abzufordern.

Was ist zu tun?
Grundsätzlich ist Verantwortlichen im Bereich E-Commerce zu raten, in der Sprache verständlich und gewählt zu kommunizieren. Auch sind Bestätigungsfelder zur Kenntnisnahme auf der einen und Einwilligungen, Einverständnisse und Zustimmungen auf der anderen Seite präzise zu trennen und zu unterscheiden.

2.2.3 Keine „Blankoeinwilligungen" für behördliche Datenerhebungen bei anderen Behörden

↗ § 30 AO, §§ 8, 37 StAG, § 24 VwVfG, § 71 SGB X

Das Sächsische Staatsministerium des Innern (SMI) hörte mich im Berichtszeitraum zu einer Neufassung der Verwaltungsvorschrift „Staatsangehörigkeitsverfahren" an, die

aufgrund der Änderung gesetzlicher Vorschriften notwendig geworden war. Die Verwaltungsvorschrift bestimmt im Wesentlichen die praktische Ausgestaltung des Einbürgerungsverfahrens. Einbürgerungsverfahren werden in der Regel mit der Antragstellung ausländischer Personen eingeleitet, die die deutsche Staatsangehörigkeit erwerben möchten. Das Gesetz legt Voraussetzungen fest, die für eine Einbürgerung erfüllt sein müssen (vgl. § 8 Staatsangehörigkeitsgesetz [StAG]). Einerseits liegt es im Interesse der Antragsteller, die für die Bearbeitung des Antrags und zum Nachweis des Vorliegens der gesetzlichen Einbürgerungsvoraussetzungen notwendigen Unterlagen vorzulegen und insofern am Verfahren aktiv mitzuwirken, zugleich gilt aber im Verwaltungsverfahren der Einbürgerung der Untersuchungsgrundsatz nach § 24 Verwaltungsverfahrensgesetz (VwVfG), der ein Tätigwerden der Behörde selbst erfordert, wenn es um verfahrensrelevante Informationen geht, über die die Antragsteller nicht selbst verfügen (können) oder die aufgrund spezialgesetzlicher Vorschriften von der Einbürgerungsbehörde bei Dritten einzuholen sind (zum Beispiel zu eventuellen Erkenntnissen der Verfassungsschutzbehörden, § 37 StAG).

Die Neufassung der Verwaltungsvorschrift umfasste, ebenso wie die zuvor geltende Verwaltungsvorschrift, in den Anlagen Informationsblätter, Formulare und Muster von Einwilligungserklärungen. Eine Einwilligungserklärung, die von Antragstellenden unterzeichnet werden sollte, betraf die Erhebung von Informationen bei Sozialleistungsträgern, insbesondere zu der Frage, ob die Antragstellenden die Inanspruchnahme von Sozialleistungen zu vertreten haben. Eine andere Einwilligungserklärung bezog sich auf die Erhebung von Daten des Antragstellenden oder seines Ehegatten durch die Einbürgerungsbehörde beim Finanzamt, wobei sich Antragstellende und gegebenenfalls Ehegatten damit einverstanden erklären sollten, dass die Einbürgerungsbehörde zum Zweck der Durchführung des Einbürgerungsverfahrens „Auskunft zu den erforderlichen Daten" bei einem in der Erklärung konkret zu bezeichnenden Finanzamt einholt.

Hinsichtlich der Einwilligungserklärung für Datenerhebungen bei Sozialleistungsträgern machte ich das Staatsministerium darauf aufmerksam, dass gesetzliche Datenverarbeitungsvorschriften existieren, die der Einbürgerungsbehörde die Erlangung der notwendigen Informationen auch ohne Einwilligung der Betroffenen ermöglichen. Ein Nebeneinander von gesetzlichen Übermittlungsvorschriften und Übermittlungen auf Einwilligungsbasis, die ein und denselben Bereich erfassen, sollte möglichst vermieden werden, um die Transparenz eines gesetzmäßigen Verfahrens zu gewährleisten und betroffene Personen nicht zu Erklärungen zu drängen, die nicht notwendig sind. Die Frage, ob Antragstellende die Inanspruchnahme von Leistungen zu vertreten haben, kann auf Grundlage der §§ 31, 32 Satz 1 StAG und § 71 Abs. 2 Satz 1 Nr. 5 Zehntes Buch Sozialgesetzbuch (SGB X) auch ohne Einwilligung der betroffenen Person geklärt werden. Das SMI reagierte auf diesen Hinweis mit der Entfernung dieser Einwilligungserklärung aus den Anlagen der Verwaltungsvorschrift.

Gegen die Verwendung der Einwilligungserklärung zur Datenerhebung beim Finanzamt äußerte ich schwere Bedenken. Die behördliche Einholung von Auskünften beim Finanzamt wirft mit Blick auf das Steuergeheimnis nach § 30 Abgabenordnung (AO) Schwierigkeiten auf. Den Antragstellenden obliegt die Nachweispflicht steuerrelevanter Informationen etwa im Hinblick auf die Vorlage von Einkommenssteuerbescheiden; darüber werden sie auch informiert. Es war schon nicht erkennbar, inwiefern darüber hinaus die Einbürgerungsbehörde überhaupt personenbezogene Daten bei Finanzämtern erheben muss. Die Formulierung der Einwilligung ließ im Übrigen weder erkennen, welche Daten die Einbürgerungsbehörde beim Finanzamt erheben möchte, noch Raum für eine konkrete Bezeichnung zu erhebender Angaben, die ggf. im Einzelfall vorzunehmen wäre. Antragstellenden und Einwilligenden erschließt sich nicht, was genau „erforderliche Daten" sind. Würde eine solche Erklärung zu Beginn eines Verfahrens unterzeichnet, wüsste auch die Einbürgerungsbehörde selbst noch nicht, ob und gegebenenfalls welche

Angaben sie überhaupt vom Finanzamt benötigen würde; es läge eine völlig unbestimmte Blankoeinwilligung vor. In einem gesetzlich streng geschützten Bereich wie dem des Steuergeheimnisses sind Einwilligungen in Datenverarbeitungen aber so präzise zu formulieren, dass den betroffenen Personen ohne Weiteres klar ist, in welche Verarbeitung welcher Daten sie einwilligen.

Im Laufe eines konstruktiven Austauschs mit dem Ministerium verdeutlichte ich meine Position mit dem Hinweis darauf, dass die Verwendung der Einwilligungserklärung ohne Änderung rechtswidrig wäre. Denn sie umginge die gesetzgeberische Wertung, nach der das Steuergeheimnis gemäß § 30 AO auch gegenüber staatlichen Stellen und Behörden gilt. Der Gesetzgeber bestimmt in § 30 Abs. 4 AO, unter welchen Umständen und für welche (behördlichen) Zwecke das Steuergeheimnis durchbrochen werden darf. Die Verwendung steuerlicher Angaben für Einbürgerungsverfahren wird dabei nicht erfasst; eine gesetzliche Grundlage für die Übermittlung steuerlicher Informationen durch die Finanzbehörden an Einbürgerungsbehörden für Zwecke des Einbürgerungsverfahrens existiert nicht. Diese Wertung darf nicht durch die Verwendung einer Einwilligungserklärung betroffener Personen umgangen werden, deren freiwillige Abgabe gegenüber der für die beantragte Einbürgerung zuständigen Behörde schon äußerst fraglich ist (vgl. Erwägungsgrund 43 der DSGVO). Allenfalls eine Zustimmung der betroffenen Person in die Offenbarung oder Verwertung konkreter Angaben oder einzelner, konkret zu bezeichnender Unterlagen der Finanzbehörde wäre zulässig (vgl. § 30 Abs. 4 Nr. 3 AO). Es obliegt den Antragstellern, Nachweise zu Angaben über ihre Verhältnisse vorzulegen (so etwa einen Einkommensteuerbescheid). Kommen sie dieser Obliegenheit nicht nach, müssen sie mit einem Stillstand des Verfahrens rechnen. Die Einbürgerungsbehörde wiederum darf nur die Informationen über die betroffenen Personen erheben und verarbeiten, die für eine Entscheidung über den Antrag zwingend notwendig sind. Die wirtschaftlichen Verhältnisse der Antragstellenden sind im Hinblick auf § 8 Abs. 1 Nr. 4 StAG relevant. Dem Ein-

kommenssteuerbescheid, der vom Antragstellenden vorgelegt wird, kommt dabei entscheidende Bedeutung zu. Andere steuerliche Verhältnisse sind für die Einbürgerungsbehörde in aller Regel ohne Relevanz; dass Einbürgerungsverfahren, wie oben erwähnt, nicht in § 30 Abs. 4 AO erwähnt werden, spricht für sich. Sollte die Staatsangehörigkeitsbehörde im Einzelfall doch einmal eine bestimmte Information oder Unterlage der Finanzbehörde zu der oder dem Antragstellenden für das Einbürgerungsverfahren unbedingt benötigen, kann sie der oder dem Antragstellenden die Vorlage auferlegen oder seine Zustimmung zur Offenbarung durch das Finanzamt einholen (§ 30 Abs. 4 Nr. 3 AO, siehe oben). In diesen Fällen aber wird und muss die Behörde in der Lage sein, die erforderlichen – aus ihrer Sicht verfahrensrelevanten – Angaben bzw. Unterlagen genau zu bezeichnen.

Im Ergebnis einer intensiven Diskussion nahm das Staatsministerium meine Hinweise auf und änderte den Vordruck der Einwilligungserklärung dergestalt, dass nun unter einem auszufüllenden Freifeld der Hinweis „konkrete Bezeichnung der zu erhebenden Angaben/Unterlagen" erscheint.

Durch diese Ausgestaltung des Formulars wird gewährleistet, dass die Einbürgerungsbehörde die Erforderlichkeit der Erhebung der im Einzelfall tatsächlich erforderlichen Informationen geprüft und bejaht hat und – noch wichtiger – dass die betroffene Person voll informiert und auf die genau bezeichneten Daten bezogen entscheiden kann, ob sie ihre Einwilligung in die Erhebung beim Finanzamt erteilt. Damit sehe ich die Anforderungen von § 30 Abs. 4 Nr. 3 AO als erfüllt und die Beachtung des gesetzgeberischen Willens in Bezug auf den hohen Schutz des Steuergeheimnisses als sichergestellt an.

Dies gilt selbstverständlich nur, wenn das Freitextfeld „konkrete Bezeichnung der zu erhebenden Angaben/Unterlagen" bereits zum Zeitpunkt der Unterschrift der betroffenen Person ausgefüllt ist und die konkret zu erhebenden Angaben/Unterlagen präzise benennt. Die Vorlage des Formulars zur Unterschrift durch die oder den Antragstellenden ohne diese von der Einbürgerungsbehörde vorzunehmenden Angaben

Was ist zu tun?
Formulare für Einwilligungserklärungen zu behördlichen Datenerhebungen sind nur dann zu verwenden, wenn die bezweckten Datenerhebungen nicht gesetzlich geregelt sind. Die betroffene Person muss vor Erklärung ihrer Zustimmung durch präzise Angaben darüber informiert werden, welche konkreten Angaben/Unterlagen für welche Zwecke bei welcher Stelle erhoben werden sollen.

verböte sich. Dankenswerterweise nahm das Staatsministerium in seinem Informationsschreiben an die Staatsangehörigkeitsbehörden über die Änderung des Formulars zur Einwilligung in die Datenerhebung beim Finanzamt auch diese Klarstellung auf.

2.2.4 Zur Erforderlichkeit der Einwilligungserklärung zu Datenerhebungen beim Finanzamt zwecks Überprüfung der Vermögensverhältnisse

↗ § 30 AO

Ein Petent berichtete, er sei im Rahmen der Überprüfung der Angemessenheit einer bereits bewilligten Ratenzahlung einer Geldstrafe von der Staatsanwaltschaft schriftlich aufgefordert worden, einen „Fragebogen zwecks Überprüfung der Vermögensverhältnisse" vollständig auszufüllen und mit den entsprechenden Belegen fristgerecht der zuständigen Staatsanwaltschaft vorzulegen. Andernfalls gelte die Bewilligung der Ratenzahlung als widerrufen.
Am Ende des Fragebogens fand sich ohne weitere Erläuterung folgender Passus:

> „Erklärung:
> Ich bin damit einverstanden, dass vom Finanzamt Auskünfte eingeholt werden und erteile dem Finanzamt die Genehmigung, Auskünfte über mein Einkommen, meine Umsätze und andere mich betreffende Steuerfragen zu erteilen.
> Ich versichere, dass meine Angaben der Wahrheit entsprechen."

Anschließend sollte der Betroffene unterzeichnen.
Diese Einwilligungserklärung entspricht nicht den datenschutzrechtlichen Vorgaben. Wie bereits im Beitrag 2.3.3 erläutert, gilt das Steuergeheimnis gemäß § 30 Abgabenordnung (AO) auch gegenüber staatlichen Stellen und Behörden. Die Verwendung steuerlicher Angaben für die staatsanwaltschaftliche Überprüfung der Vermögensverhältnisse

von Betroffenen ist gesetzlich gemäß § 30 Abs. 4 AO nicht als Ausnahme zur Durchbrechung des Steuergeheimnisses vorgesehen. Ebenso wenig existiert eine andere Rechtsgrundlage, die die Finanzämter zur direkten Datenübermittlung an die abfragende Staatsanwaltschaft befugt. Auch sehe ich eine solche Einholung von Auskünften beim Finanzamt zu den wirtschaftlichen Verhältnissen der Betroffenen nicht als erforderlich an. Die Betroffenen, das heißt die Antragsteller, sind ausdrücklich verpflichtet, an der Prüfung der Angemessenheit der Ratenzahlung durch persönliche Erteilung von Auskünften und Vorlage entsprechender Belege selbst mitzuwirken. Eine zusätzliche „Absicherung" durch das Finanzamt erscheint daher weder erforderlich noch gesetzlich zulässig.

Auch wenn der Gesetzgeber in § 30 Abs. 4 Nr. 3 AO bestimmt, dass eine Durchbrechung des Steuergeheimnisses zulässig ist, soweit die betroffene Person zustimmt, darf die Voraussetzung der Erforderlichkeit einer Datenabfrage bei den Finanzämtern nicht umgangen werden. Zudem habe ich starke Zweifel, ob die zitierte „Erklärung" im Fragebogen von den Betroffenen noch als freiwillige Einwilligung zu verstehen ist. Aufgrund der Formulierung, der mangelnden Hinweise (zum Beispiel „ggf. einzeln oder insgesamt streichen") sowie der Verbindung zur Erklärung zur Wahrheitspflicht (bezüglich aller getätigten Angaben in dem Fragebogen) könnte bei dem Betroffenen der Eindruck entstehen, die Einwilligung in die Erklärung in ihrer Gesamtheit sei verpflichtend, um den ausdrücklich angedrohten Widerruf der Ratenzahlungsbewilligung zu vermeiden.

Meine datenschutzrechtlichen Bedenken teilte ich der Staatsanwaltschaft mit und bat um entsprechende Stellungnahme. Aufgrund der grundsätzlichen Bedeutung für den gesamten Geschäftsbereich der sächsischen Staatsanwaltschaften befasste sich folgend die Generalstaatsanwaltschaft Dresden mit der datenschutzrechtlichen Prüfung und erklärte, dass sie meine Zweifel an der Rechtmäßigkeit der Einwilligungserklärung teile und zeigte sich äußerst lösungsorientiert und engagiert hinsichtlich der datenschutzkonformen Änderung des Formblattes. Bei dem Fragebogen

zur Überprüfung der Vermögensverhältnisse handelt es sich um ein länderübergreifend abgestimmtes Formblatt, das den sächsischen Staatsanwaltschaften durch den Text-Süd-Verbund zur Verfügung gestellt wurde. Dem Text-Süd-Verbund gehören neben Sachsen der Freistaat Bayern (als federführendes Bundesland), Thüringen, Baden-Württemberg und das Saarland an. In dem Verbund werden einheitlich fachlich-inhaltliche Vorgaben für Formulare ausgearbeitet, die dann in der Textverarbeitung der Staatsanwaltschaften der beteiligten Bundesländer genutzt werden. Die Änderung des Formblattes wurde im Länderverbund priorisiert sowie außerhalb regulärer Sitzungen im Umlaufverfahren beschlossen und konnte so nicht nur für den Freistaat Sachsen, sondern auch für die im Länderverbund beteiligten Bundesländer Freistaat Bayern, Freistaat Thüringen, Baden-Württemberg und das Saarland umgesetzt werden.

Was ist zu tun?
Formulare für Einwilligungserklärungen zu behördlichen Datenerhebungen sind nur dann zu verwenden, wenn die bezweckten Datenerhebungen nicht gesetzlich geregelt sind und für die Aufgabenerfüllung der abfragenden Behörde erforderlich sind.

2.3 Sensible Daten, besondere Kategorien personenbezogener Daten

2.3.1 Anlasslose Vorortkontrolle des Gesundheitsamts eines Landkreises nach § 20 Abs. 12 Infektionsschutzgesetz

↗ § 20 Abs. 12 IfSG

Mit einer Beschwerde rügte ein Petent, dass das Gesundheitsamt des Landkreises eine Kontrolle sämtlicher Nachweise des ausreichenden Impfschutzes gegen Masern in der Kindertagesstätte, die sein Kind besucht, durchgeführt hat. Dabei hatte das Gesundheitsamt Notizen mit Daten seines Kindes sowie des Attests angefertigt. Er bat um Prüfung, ob eine anlasslose Kontrolle der Kita durch das Gesundheitsamt des Landkreises zulässig sei.
Der Petent zitierte dazu den Kommentar von Kießling, Infektionsschutzgesetz, 3. Auflage 2022, Rn. 61 zu § 20 Infektionsschutzgesetz (IfSG):

„1. Befugnisse des Gesundheitsamtes [...]
[...] Die Benachrichtigung der Einrichtungsleitung (oder der nach Abs. 9 S. 3 Nr. 2 anderweitig bestimmten Stelle) geht der Aufforderung durch das Gesundheitsamt also immer voraus, da das Gesundheitsamt erst aufgrund der Benachrichtigungsverpflichtung der Einrichtungsleitung die personenbezogenen Daten der anschließend behördlich ermessensgeleitet aufzufordernden Personen erlangt. [...]"

Meine Prüfung führte zu folgendem Ergebnis: In der Bundestagsdrucksache 19/13452, Seite 30, wird zu § 20 IfSG Abs. 12, hingegen ausgeführt:

„Die Gesundheitsämter können von Personen, die nach Absatz 8 Satz 1 einen nach den Empfehlungen der STIKO ausreichenden Impfschutz gegen Masern oder eine durch eine Masernerkrankung erlangte Immunität gegen Masern aufweisen müssen, einen Nachweis nach Absatz 9 Satz 1 anfordern, allerdings erst zu dem Zeitpunkt, zu dem eine Nachweispflicht besteht. Dabei macht es keinen Unterschied, ob es sich um stichprobenartige Kontrollen in solchen Einrichtungen handelt oder um Personen, über die das Gesundheitsamt nach Absatz 9 Satz 6, Absatz 10 Satz 2 oder Absatz 11 Satz 2 benachrichtigt wurde. Eine doppelte Kontrolle wird jedoch regelmäßig nicht in Betracht kommen."

Das Sächsische Staatsministerium für Soziales und Gesellschaftlichen Zusammenhalt wurde um Stellungnahme zur Vorgehensweise des Gesundheitsamts gebeten. Dieses teilt die Ansicht, die in der Bundestagsdrucksache 19/13452 vertreten wird. Es ist der Auffassung, dass eine anlasslose Prüfung der Dokumentation der Impfnachweise zum Masernschutz in der Einrichtung durch das zuständige Gesundheitsamt des Landkreises/der Kreisfreien Stadt zulässig ist. Aus datenschutzrechtlicher Sicht ist die Vorgehensweise des Gesundheitsamts des Landkreises/der Kreisfreien Stadt daher aus meiner Sicht nicht rechtswidrig.

Was ist zu tun?
Das Gesundheitsamt des Landkreises/der Kreisfreien Stadt darf ohne konkreten Anlass die Notizen zu den Nachweisen des ausreichenden Impfschutzes gegen Masern in der Einrichtung/Kita prüfen.

3 Betroffenenrechte

3.1 Spezifische Pflichten des Verantwortlichen

3.1.1 Mitteilungspflichten nach Art. 19 DSGVO

↗ Art. 19 DSGVO

In Ergänzung der Rechte einer betroffenen Person auf Berichtigung nach Art. 16 Datenschutz-Grundverordnung (DSGVO), auf Löschung nach Art. 17 Abs. 1 DSGVO und auf Einschränkung der Verarbeitung ihrer personenbezogenen Daten nach Art. 18 DSGVO normiert Art. 19 Satz 1 DSGVO eine Pflicht für den Verantwortlichen, allen Empfängern der personenbezogenen Daten mitzuteilen, dass bezüglich der Daten eine Berichtigung, eine Löschung oder eine Einschränkung der Verarbeitung erfolgt ist. Der Verantwortliche unterrichtet die betroffene Person über diese Empfänger, wenn die betroffene Person das verlangt (vgl. Art. 19 Satz 2 DSGVO).

Eine Mitteilungspflicht nach Art. 19 Satz 1 an die Empfänger besteht allerdings dann nicht, wenn die Mitteilung mit einem unverhältnismäßigen Aufwand für den Verantwortlichen verbunden oder ihm diese unmöglich ist, vgl. Art. 19 Satz 1 2. Halbsatz DSGVO.

Zweck des Art. 19 DSGVO ist es, den betroffenen Personen eine beschleunigte und vereinfachte Rechtsdurchsetzung zu ermöglichen. Sie sollen wegen ihrer Betroffenenrechte nach Art. 16 ff. DSGVO nicht an jeden Datenempfänger einzeln herantreten und hierfür gegebenenfalls zunächst ein Auskunftsrecht nach Art. 15 DSGVO geltend machen müssen.

Verstöße gegen Art. 19 DSGVO können für einen Verantwortlichen Schadensersatzansprüche der jeweils betroffenen Person gemäß Art. 82 DSGVO zur Folge haben. Zudem kann die Aufsichtsbehörde gemäß Art. 83 Abs. 5 DSGVO ein Bußgeld verhängen. Betroffene Personen haben daneben die Möglichkeit, eine Beschwerde bei der zuständigen Aufsichtsbehörde gemäß Art. 77 DSGVO zu erheben.

Eine solche Beschwerde habe ich im vergangenen Jahr erhalten. Der Beschwerdeführer hatte vor einiger Zeit an einem Seminar teilgenommen. Der Veranstalter des Seminars, mit Sitz im Freistaat Sachsen, hatte die Kontaktdaten aller Seminarteilnehmer an das Unternehmen weitergegeben, welches mit der Durchführung des Seminars beauftragt worden war. Nach dem Seminar hatte der Beschwerdeführer bei dem Veranstalter die Löschung seiner Kontaktdaten beantragt. Der Veranstalter hatte dem Antrag entsprochen; die Löschung wurde gegenüber dem Beschwerdeführer bestätigt.

In diesem Jahr erhielt der Beschwerdeführer, für ihn vollkommen überraschend, von dem seminardurchführenden Unternehmen, welches keine Niederlassung im Freistaat Sachsen hat, Nachfragen zur Wirksamkeit der Fortbildung und zu den gemachten Erfahrungen im Nachgang zu dem Seminar.

Aus diesem Grund erhob der Beschwerdeführer neben der Beschwerde bei meiner Behörde auch eine Beschwerde nach Art. 77 DSGVO bei der Aufsichtsbehörde, die für das seminardurchführende Unternehmen zuständig ist.

Im Rahmen des in meiner Behörde geführten Aufsichtsverfahren bestätigte der Veranstalter das Bestehen seiner Mitteilungspflicht nach Art. 19 Satz 1 DSGVO über die erfolgte Löschung der personenbezogenen Daten des Beschwerdeführers gegenüber dem Unternehmen, welches er mit der Durchführung des Seminars beauftragt hatte. Die Einhaltung der Mitteilungspflicht konnte der Veranstalter jedoch gegenüber meiner Behörde nicht nachweisen. Eine Nachfrage seitens meiner Behörde bei der zuständigen Aufsichtsbehörde für das vom Veranstalter beauftragte Unternehmen ergab, dass dort ebenfalls keine Erkenntnisse zu einer erfolgten Information durch den Veranstalter vorlagen.

Was ist zu tun?
Erfolgt die Weitergabe von personenbezogenen Daten durch einen Verantwortlichen an einen Dritten, so bedarf bei bestehender Mitteilungspflicht die Benachrichtigung an den Dritten über eine vorgenommene Berichtigung, Löschung oder Einschränkung der Verarbeitung der weitergegebenen personenbezogenen Daten einer Nachweisführung.

Im Ergebnis meiner Prüfung habe ich deshalb gegenüber dem Veranstalter einen datenschutzrechtlichen Verstoß gegen Art. 19 Satz 1 DSGVO festgestellt. Zugleich habe ich ihn aufgefordert, seine Prozesse zu überprüfen und so zu optimieren, dass ihm künftig in vergleichbaren Fällen eine Nachweisführung zur Erfüllung seiner Mitteilungspflicht nach Art. 19 Satz 1 DSGVO problemlos möglich ist.

3.2 Auskunftsrecht

3.2.1 Auskunftsersuchen zu polizeilich gespeicherten Daten sind durch jede Polizeidienststelle entgegenzunehmen

↗ § 13 SächsDSUG, § 92 SächsPVDG, Art. 15 DSGVO

Ein Petent war persönlich in einem sächsischen Polizeirevier erschienen und bat um kurzfristige Auskunft über die zu seiner Person gespeicherten Daten. Dabei berief er sich auf Art. 15 Datenschutz-Grundverordnung (DSGVO). Dem vom Petenten angesprochenen Beamten sei eine Abfrage der polizeilichen Speicherungen zum Petenten nicht gerechtfertigt erschienen. Dem Petenten sei auch mitgeteilt worden, dass die DSGVO keine Anwendung auf die Polizei finde und es keine rechtliche Grundlage gebe, seine Anfrage zu bearbeiten.
Bereits mit meiner ersten Bitte um Stellungnahme habe ich die zuständige Polizeidirektion auf die Rechtslage hingewiesen. Zutreffend ist, dass die DSGVO keine Anwendung findet, soweit zuständige Behörden personenbezogene Daten für Zwecke der Strafverfolgung oder zur straftatenverhütenden Gefahrenabwehr verarbeiten. Hierzu zählen auch die polizeiliche Bearbeitung von Strafanzeigen und insoweit die Daten der Anzeigeerstattenden ebenso wie die Daten eventuell beschuldigter Personen. Dass die DSGVO in diesem Bereich keine Anwendung findet, ergibt sich ausdrücklich aus der DSGVO selbst: Art. 2 Abs. 2 Buchst. d DSGVO. Damit ist auch der Anwendungsbereich von Art. 15 DSGVO nicht eröffnet.

Richtig ist aber auch, dass bei der Verarbeitung personenbezogener Daten im Bereich der Strafverfolgung und straftatenverhütenden Gefahrenabwehr andere spezielle und allgemeine datenschutzrechtliche Vorschriften zur Anwendung kommen (vgl. § 92 Abs. 2 Sächsisches Polizeivollzugsdienstgesetz [SächsPVDG] in Verbindung mit § 13 Sächsisches Datenschutz-Umsetzungsgesetz [SächsDSUG]).

Falsch ist, dass es keine Rechtsgrundlage für die Polizei gäbe, Auskunftsanträge entgegenzunehmen und zu bearbeiten. Das Gegenteil ist der Fall: Auskunftsanträge sind entgegenzunehmen und zu bearbeiten. Auf der Website der Polizei Sachsen findet sich dazu ein entsprechender Hinweis: „Jede betroffene Person kann Auskunft über ihre von der sächsischen Polizei verarbeiteten personenbezogenen Daten verlangen. Dem Betroffenen ist auf Antrag gemäß § 92 Abs. 2 SächsPVDG in Verbindung mit § 13 SächsDSUG Auskunft zu erteilen, ob und welche personenbezogene Daten zu seiner Person verarbeitet werden. Anträge sind durch alle sächsischen Polizeidienststellen entgegenzunehmen." (siehe sdb.de/tb2402).

An die Polizei gerichtete Auskunftsanträge werden bei der Sächsischen Polizei zentral durch das Landeskriminalamt Sachsen bearbeitet, da nicht jede Dienststelle Zugriff auf den gesamten Inhalt aller polizeilichen Dateien hat und insoweit eine vollständige Auskunft erteilen könnte. Erhält eine andere Dienststelle einen Antrag, leitet sie diesen zur Bearbeitung und Auskunftserteilung an das LKA Sachsen weiter. Dort findet die Prüfung des Antrags und eventuell bestehender Auskunftsbeschränkungen statt (vgl. § 13 Abs. 2 SächsDSUG).

Eine „Falschbezeichnung" von an die Polizei gerichteten Auskunftsanträgen betroffener Personen, die sich auf Art. 15 DSGVO berufen, ist unbeachtlich. Eine genaue Kenntnis der einschlägigen Rechtsvorschriften kann von betroffenen Personen nicht erwartet oder verlangt werden. Da auch Auskunftsanträge ohne Angabe von Rechtsgrundlagen zu bearbeiten wären, darf auch der irrtümliche Bezug auf Art. 15 DSGVO dem Antragsteller nicht zum Nachteil gereichen und zur Verweigerung der Entgegennahme und Bearbeitung führen.

Was ist zu tun?
Anträge auf Auskunft können voraussetzungslos an alle Polizeidienststellen gerichtet werden, die zur Entgegennahme und Bearbeitung bzw. gegebenenfalls Weiterleitung verpflichtet sind. Eine unzutreffende rechtliche Bezeichnung der Vorschriften zum Auskunftsanspruch ist unschädlich.

Die Polizeidirektion schloss sich meiner Sichtweise an und teilte mit, dass die pauschale Ablehnung eines Auskunftsanspruchs in der Polizeidirektion nicht üblich sei. Der Sachverhalt sei kritisch ausgewertet, die Beamtinnen und Beamten auf die gängige Verfahrensweise hingewiesen worden.

3.2.2 Handlungsleitfaden für Kommunen und Verwaltungen zur Auskunftserteilung nach Artikel 15 DSGVO erschienen

↗ Art. 12, 15 DSGVO

Gemäß Art. 15 der Datenschutz-Grundverordnung (DSGVO) haben Betroffene (Personen, deren personenbezogene Daten verarbeitet wurden bzw. werden) das Recht, von einem Verantwortlichen Auskunft über ihre gespeicherten Daten zu verlangen.

Handlungsleitfaden für Kommunen und Verwaltungen zur Auskunftserteilung nach Art. 15 DSGVO:
↗ sdb.de/tb2403

Hierzu hat der Europäische Gerichtshof (EuGH) jüngst in mehreren wegweisenden Urteilen den Anspruch konkretisiert und einige bisher unbeantwortete Fragen und unklare Rechtslagen ausgeräumt. Dies hat mich veranlasst, einen möglichst praxisrelevanten Handlungsleitfaden zu dieser Thematik zu veröffentlichen. Dieser richtet sich an sächsische öffentliche Stellen, die Verantwortliche im Anwendungsbereich der DSGVO sind und Auskunft nach Art. 15 DSGVO erteilen müssen. Zu dem Urteil des EuGH vom 26. Oktober 2023 zur Rechtssache C-307/22 verweise ich im Übrigen auch auf meinen Tätigkeitsbericht 2023 (9.5., Seite 277 ff.).

Tätigkeitsbericht Datenschutz 2023:
↗ sdb.de/tb2023

Das nun veröffentlichte Papier basiert auf der derzeit geltenden Rechts- und Gesetzeslage einschließlich EuGH- und nationaler Rechtsprechung. Es berücksichtigt auch die entsprechend veröffentlichte Leitlinie 01/2022 (Guidelines 01/2022 on data subject rights – Right of access) des Europäischen Datenschutzausschusses (EDSA).

Sowohl formale Voraussetzungen der Auskunft – Eingangsbestätigung, Fragen der Form und Frist, Zuständigkeiten, zeitlicher Umfang – werden in dem Dokument erörtert als auch das sehr relevante Thema der Identitätsfeststellung und Berechtigung der Antragstellerin/des Antragstellers. Inhalt-

lich geht es sodann um Fragen zu Gegenstand und Umfang des Anspruchs, Prüfung einer Ausnahme oder Einschränkung oder Betroffenheit von Rechten Dritter und den hieraus erwachsenden Rechtsfolgen. Auch etwaige einfachgesetzliche Einschränkungen spielen eine Rolle. Abschließend informiert der Leitfaden über Rechtschutzmöglichkeiten bei fehlender oder unvollständiger Auskunft.

Besonderes Augenmerk wurde in dem Handlungsleitfaden auf die sogenannte zweistufige Vorgehensweise gelegt, bei der der Verantwortliche in legitimer Weise zunächst bei der/dem Betroffenen um Konkretisierung ihres/seines Auskunftsanspruches bitten kann. Dies ist eine zulässige Möglichkeit zu versuchen, das Auskunftsverlangen zu begrenzen. Gelingt dies nicht, ist der Verantwortliche aber dennoch zur vollständigen Beauskunftung verpflichtet. Es gilt deswegen: Die Bürgerin bzw. der Bürger kann – muss aber nicht – ihr/sein Anliegen präzisieren.

Eine Reihe verantwortlicher Stellen, meist sind dies kleinere Gemeinden, sehen sich indes oft personell wie auch organisatorisch nicht in der Lage, umfassende Auskunftsersuchen – die sogenannte Globalauskunft – in der gesetzlich vorgegebenen Frist (1 Monat, die auf 3 Monate verlängert werden kann, Art. 12 Abs. 3 Sätze 1 und 2 DSGVO) zu beantworten. Die derzeitige Rechtslage gestaltet sich indes derart, dass Verwaltungsaufwand keinen Beschränkungs- oder gar Ablehnungsgrund einer Auskunftserteilung darstellen kann. Gesetzlich ist dies derzeit nur in bestimmten Rechtsgebieten (Sozialverwaltung, Finanzbehörden, nichtöffentliche Stellen) vorgesehen, zu der die allgemeine Verwaltung – wie die oben benannten Gemeinden – gerade nicht zählt. Auch hierüber informiert der Handlungsleitfaden umfassend.

Was ist zu beachten?
Verantwortliche Stellen haben Betroffenen auf Antrag über die verarbeiteten personenbezogenen Daten Auskunft zu erteilen. Der entsprechende Aufwand ist für den Bereich der allgemeinen Verwaltung kein Ausschlusstatbestand.

4 Pflichten Verantwortlicher und Auftragsverarbeiter

4.1 Verantwortung für die Verarbeitung, Technikgestaltung

4.1.1 Anlasslose Prüfung eines Onlinehändlers im Bereich Consumer-Elektronik

↗ § 25 TTDSG bzw. neu § 25 TDDDG; Art. 5 Abs. 1 Buchst. a in Verbindung mit Art. 6 Abs. 1 DSGVO; Art. 5 Abs. 1 Buchst. e, Art. 5 Abs. 2, Art. 7, Art. 25 DSGVO

Mit meinem IT-Labor (siehe 6.2.10) habe ich bei einem sächsischen Onlinehändler bei einer anlasslosen Prüfung mehrere Verstöße gegen die Datenschutz-Grundverordnung (DSGVO) und das Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) festgestellt. Das Unternehmen handelt mit Consumer-Elektronik und beschäftigt mehrere hundert Mitarbeiterinnen und Mitarbeiter. Konkret simulierte das IT-Labor im Frühjahr 2024 einen Interessenten, der sich auf der Website und in der App des Shops im jeweiligen Einwilligungsbanner ausdrücklich „nicht einverstanden" mit der Verarbeitung personenbezogener Daten sowie der Speicherung von Informationen auf dem Endgerät und dem Zugriff auf Informationen auf dem Endgerät erklärte und sich anschließend sechs Minuten lang nur über die Angebote des Anbieters informierte.
In der Analyse stellte das IT-Labor fest, dass bereits vor der Ablehnung Verbindungen zu externen Diensten von Dritten hergestellt und einwilligungspflichtige Verarbeitungen durchgeführt wurden, obwohl der Nutzer diese Dienste nicht wünschte.

Trotz des nachfolgenden Anklickens „nicht einverstanden" im Consentbanner wurden einwilligungspflichtige personenbezogene Daten des Nutzers durch mehr als 30 Verbindungen zu Diensten von Dritten verarbeitet. Mehr als 20 einwilligungspflichtige Cookies führten trotz Ablehnung zu einer weiteren Verarbeitung personenbezogener Daten ohne Rechtsgrundlage. Das IT-Labor detektierte einwilligungspflichtige Local-Storage-Einträge.

Der Nutzerwunsch war und ist hinsichtlich der Speicherung von Informationen in der Endeinrichtung des Endnutzers oder des Zugriffs auf Informationen maßgeblich, § 25 Abs. 2 Nr. 2 Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG). Wird der Nutzerwunsch nicht berücksichtigt, hat dies auch Auswirkungen auf die Rechtmäßigkeit der nachfolgenden Verarbeitung von personenbezogenen Daten.

Ich informierte das Unternehmen über die festgestellten Verstöße, stellte eine Untersagungsanordnung in Aussicht (Entwurf wurde beigefügt) und gab die Gelegenheit zur Stellungnahme zu meinen obigen Feststellungen binnen Monatsfrist. Das Unternehmen nahm Akteneinsicht, kündigte eine Neugestaltung der App und der Website an und bat um einen Gesprächstermin zur Abklärung von technischen Fragen. Der Termin wurde eingehalten und die angekündigte Umgestaltung innerhalb der vereinbarten Frist durchgeführt.

Insgesamt habe ich dadurch im Jahr 2024 sehr viele Verstöße des Unternehmens festgestellt und mit meinen Analysen verglichen. Sie betrafen den § 25 TDDDG sowie Art. 5 Abs. 1 Buchst. a in Verbindung mit Art. 6 Abs. 1 DSGVO, Art. 5 Abs. 1 Buchst. e DSGVO, Art. 5 Abs. 2 DSGVO, Art. 7 DSGVO und Art. 25 DSGVO.

Das Verwaltungsverfahren ist noch nicht abgeschlossen, da ich nach einer Nachschau auf der Website weitere Fragen gestellt und Hinweise erteilt habe. Ich habe erkennbare Bemühungen des Unternehmens zur Umsetzung des Datenschutzes festgestellt.

Was ist zu tun?

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

4.1.2 Gastzugang im Onlinehandel

↗ § 7 UWG, Art. 21 DSGVO

Im Hinblick auf die Ansprache von ausgewählten Personen verfolgt die Werbewirtschaft ein legitimes Interesse (Direktmarketing). In der Umkehrung besteht allerdings die ebenso berechtigte Erwartung der Kundin oder des Kunden, von unerwünschter und insbesondere von störender Werbung verschont zu werden.

Direktmarketing per E-Mail ist in Deutschland aufgrund § 7 Gesetz gegen den unlauteren Wettbewerb (UWG) in einer Weise ausgestaltet, die es dem Werbetreibenden ermöglicht, sich seinen Bestandskunden gegenüber auf kostengünstige Art in Erinnerung zu halten bzw. Umsätze zu generieren. Interessebezogen sollte diese Möglichkeit Bestand behalten, hat doch der/die einzelne Kunde/Kundin auch die Möglichkeit, einen Werbewiderspruch durchzuführen, Art. 21 Abs. 2, 3 Datenschutz-Grundverordnung (DSGVO).

Gleichwohl irritiert es derzeit schon viele Einmal-Kundinnen und -Kunden, wenn sie zum Teil Monate nach dem Geschäft einen Werbe-Newsletter erhalten und dann feststellen müssen, dass dies auf unabsehbare Zeit fortgesetzt wird. Der erwähnte einmalig geltend zu machende Werbewiderspruch nach Art. 21 Abs. 2 DSGVO soll dem gesetzlich vorgreifen. Seriöse Werbetreibende bieten einen entsprechenden (funktionierenden) Abmeldelink an, wodurch – wenn er angeklickt wird – sichergestellt ist, dass weitere Werbeansprachen zuverlässig unterbleiben – von bereits beauftragten Nachläufern einmal abgesehen.

Nicht funktionierende Abmeldelinks sind hingegen nicht selten der Anlass für Beschwerden bei der Aufsichtsbehörde und werfen überdies kein gutes Licht auf die IT-Organisation beim Verantwortlichen. Freilich, und darauf sei immer wieder hingewiesen, ist die/der Betroffene nicht darauf beschränkt, den Abmeldelink zu nutzen; auch die Einreichung des Widerspruchs auf anderen Wegen (ausgenommen No-Reply-Adressen) hat der Werbetreibende und Verantwortliche in seinen Workflow zu integrieren.

Hinweise der DSK – Datenschutzkonformer Onlinehandel mittels Gastzugang:
↗ sdb.de/tb2404

Der jüngste Beschluss der Datenschutzkonferenz befasst sich mit der Thematik.

Unbeschadet der Frage, ob ein Gastzugang aus Gründen der Vertragsfreiheit tatsächlich verlangt werden kann bzw. welche Ausnahmen davon gelten sollen, vgl. LG Hamburg, 22.02.2024, Az. 327 O 250/22), ist bereits in der aufsichtsrechtlichen Praxis weitgehend durchgesetzt, dass Kundinnen und Kunden, die den Gastzugang bewusst gewählt haben, sich nicht als Bestandskunden im Sinne von § 7 Abs. 4 UWG identifizieren und daher auch keine auf dieser Grundlage versandte E-Mail-Werbeansprache erwarten. Postalische Werbung ist hiervon im Übrigen nicht berührt.

Auf datenschutzrechtliche Entwicklungen und sich verändernde Kundengewohnheiten sollte das E-Business bereits aus wirtschaftlichem Eigeninteresse heraus eingehen, und zwar unabhängig von der Rechtsfrage, ob die Kundin oder der Kunde auch unter Nutzung des optionalen Gastzugangs zum Bestandskunden nach dem UWG geworden ist.

Auch wenn mit der bewussten Wahl des Gastzugangs kein Werbewiderspruch gegen Werbeansprachen auf Basis des Bestandskundenprivilegs anzunehmen sein wird, dürfte doch empirisch unstreitig sein, dass die bzw. der typische Gastzugangskunde/-kundin nicht als Newsletter-Empfänger/in registriert sein möchte, weil er/sie insgesamt nur einen einmaligen Vertragsabschluss ins Auge gefasst hat.

In diesen Fallgestaltungen nicht auf dem Bestandskundenprivileg zu bestehen, sollte schon die geschäftliche Vernunft gebieten. Wenn zufriedene Gastzugangskundinnen und -kunden ein erneutes Geschäft abzuschließen gedenken, wird sich ohnedies die Frage stellen, ob sie nicht ein bequemeres Kundenkonto eröffnen. Hingegen wird schon eine als ungehörig empfundene Werbeansprache durch einen E-Mail-Newsletter sich indessen als dauerhaft kontraproduktiv erweisen können. Nichts spricht insoweit dagegen, der/dem Gastzugangskundin/-kunden eine vom Verantwortlichen frei gestaltbare Einwilligung zu allerlei Arten von Werbepost anzubieten.

In einer im Berichtszeitraum bearbeiteten Eingabe traten sogar mehrere vom Gastzugangskunden unerwartete Fragen

Was ist zu tun?
E-Commerce-Anbieterinnen und -Anbietern ist zu raten, das Bestandskundenprivileg bei Kundinnen und Kunden mit Gastzugang nicht auszuüben und gegebenenfalls alternativ explizite Einwilligungslösungen für E-Mail-Werbung anzubieten. Dies wird auch der Idealvorstellung von dem/der mündigen Vertragspartner/in am ehesten gerecht. Denn nur jene Gastkundinnen bzw. Gastkunden, die sich in ihrer bewussten Entscheidung respektiert fühlen, werden zufrieden sein.

auf. Nicht nur wurde der Kunde wie bei Neuregistrierungen üblich per E-Mail „willkommen" geheißen. Auch wurden ihm künftige „Vorschläge" per Newsletter angekündigt. Des Weiteren wurde ihm trotz des gewählten Gastzugangs ein Link auf die Gastzugangsdaten offeriert. Der Beschwerdeführer fragte sich als Kunde, worin der datenschutzrechtlich erhebliche Unterschied zwischen dem Gastzugang und dem Kundenkonto bestände.
Die Prüfung beim Verantwortlichen ergab, dass man sich wohl der Einfachheit halber etlicher Bausteine aus dem Kundenkonto bedient hatte, ohne diese entsprechend anzupassen. Der Verantwortliche konnte schließlich davon überzeugt werden, einen leistungsfähigen Gastzugang zu implementieren, um Kundinnen und Kunden künftig nicht mehr zu verärgern.

4.1.3 Effektive und einfache Rechtsdurchsetzung gegen Autoportal

↗ § 25 TTDSG bzw. neu § 25 TDDDG; Art. 5 Abs. 1 Buchst. a in Verbindung mit Art. 6 Abs. 1 DSGVO; Art. 5 Abs. 2, Art. 7, Art. 25 DSGVO

Durch die Beschwerde eines Petenten wurde ich auf ein sächsisches Unternehmen aufmerksam, dass online mit Autos handelt. Konkret ging es in der Beschwerde um 18 Trackingeinbettungen ohne Rechtsgrundlage bei dem Betrieb der Internetplattform.
Ich stellte in einer Analyse mit dem Website Evidence Collector (Analysewerkzeug des Europäischen Datenschutzbeauftragten) fest, dass, bereits unmittelbar nachdem das Autoportal ohne Einwilligung von mir im Internet aufgerufen wurde, mehrere externe Dienste von Dritten gestartet wurden, obwohl der/die Nutzer/in diese Dienste nicht wünschte. Der Nutzerwunsch war und ist hinsichtlich der Speicherung von Informationen in der Endeinrichtung des Nutzers bzw. der Nutzerin oder des Zugriffs auf Informationen maßgeblich, § 25 Abs. 2 Nr. 2 Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG). Wird der Nutzerwunsch nicht berücksichtigt, hat dies auch Auswirkungen auf die Rechtmäßigkeit der nachfolgenden Verarbeitung von personenbezogenen Daten.

Ich informierte das Unternehmen über die Beschwerde und die erfolgte Prüfung hinsichtlich der Trackingeinbettungen im März 2023. Unter einer Fristsetzung von einem Monat forderte ich das Unternehmen schriftlich zur Bereitstellung einer vollständigen Liste über die auf dem Portal eingebundenen Ressourcen auf. Ich empfahl, eine Tabelle zu erstellen, die die Cookies/Local-Storage-Objekte und Datenverarbeitungen einschließlich der Datenübermittlungen an Dritte umfasst. Weiterhin erwartete ich eine Rechtsgrundlagenbenennung, unterschieden nach Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG, neu seit 14.05.2024: TDDDG) und Datenschutz-Grundverordnung (DSGVO). Soweit die Verarbeitung auf eine Erforderlichkeit nach § 25 Abs. 2 Nr. 2 TTDSG bzw. auf ein berechtigtes Interesse nach Art. 6 Abs. 1 Buchst. f DSGVO gestützt werden sollte, forderte ich eine Beschreibung des Zwecks und der Funktionsweise sowie die Benennung der konkreten Nutzerdaten.

Das Unternehmen antwortete zwar innerhalb der Frist, tat sich aber mit der Vollständigkeit der Informationen sehr schwer. Ich bat daher um die Ergänzung der Informationen und setzte hierfür eine erneute Frist. Gleichzeitig kündigte ich eine mögliche Untersagung der Website an, da zum Beispiel die Rechenschaftspflicht für die Einhaltung von Art. 5 Abs. 1 DSGVO, insbesondere für die Rechtmäßigkeit nach Art. 5 Abs. 1 Buchst. a DSGVO, durch das Unternehmen nicht erfüllt werden konnte, geschweige denn eine rechtmäßige Verarbeitung vorlag (weiterer Verstoß gegen Art. 5 Abs. 1 Buchst. a DSGVO in Verbindung mit Art. 6 Abs. 1 DSGVO).

Die Informationen wurden nun vom Unternehmen zur Verfügung gestellt. Da ich wesentliche Änderungen an der Website feststellte, forderte ich das Unternehmen zusätzlich dazu auf, Informationen zum Stand vor der Überarbeitung der Website mir gegenüber mitzuteilen. Hintergrund dieser Forderung war meine Bewertung der bisherigen Verarbeitung aus der Ausgangsübersicht vor den Überarbeitungen. Dieser Aufforderung kam das Unternehmen schließlich nach. Die Verstöße wurden abgestellt.

Was ist zu tun?
Es ist selbstverständlich, dass bei einem Geschäftsmodell die rechtlichen Rahmenbedingungen sondiert und von Anfang an der Datenschutz bei der Entwicklung neuer Internetdienste beachtet wird. Die Rechtsdurchsetzung kann aufgrund der bestehenden Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO für Unternehmen effektiv und einfach durch die Sächsische Datenschutz- und Transparenzbeauftragte erfolgen. Der Europäische Gerichtshof (EuGH) hat mehrfach entschieden, dass die Rechenschaftspflicht aus Art. 5 Abs. 2 DSGVO zu einer Beweislast des Verantwortlichen für die Einhaltung der Grundsätze des Art. 5 Abs. 1 DSGVO führt (EuGH, Urteil vom 04.05.2023, C-60/22, Rn. 53).

Insgesamt habe ich dadurch im Zeitraum November 2022 bis Oktober 2023 sehr viele Verstöße des Unternehmens festgestellt und mit meinen Analysen verglichen. Sie betrafen den § 25 TTDSG sowie Art. 5 Abs. 1 Buchst. a) in Verbindung mit Art. 6 Abs. 1 DSGVO, Art. 5 Abs. 2 DSGVO, Art. 7 DSGVO und Art. 25 DSGVO.
Das verwaltungsrechtliche Verfahren endete im August 2024 mit einer Verwarnung gemäß Art. 58 Abs. 2 Buchst. b DSGVO gegenüber dem Unternehmen, da ich den Eindruck hatte, dass die Verwarnung zur Prävention von Verstößen und zur proaktiven Anpassung der Verarbeitungsvorgänge bei dem Unternehmen führt. Von der Einleitung eines Bußgeldverfahrens wurde durch das hierfür zuständige Referat abgesehen.
Durch eine Verwarnung wird keine konkrete, unmittelbare Rechtspflicht ausgelöst. Mit einer Verwarnung wird implizit ausgedrückt, dass sich der Adressat künftig datenschutzkonform verhalten soll (VG Mainz, Urteil vom 24.05.2020, Az. 1 K 647/19.MZ, Rn. 16).

4.1.4 Unvollständige Schwärzung

↗ Art. 32 DSGVO

Ich wurde durch einen Petenten darauf hingewiesen, dass in der im Dokumentationssystem EDAS des Sächsischen Landtags veröffentlichten Antwort auf eine Kleine Anfrage zum Thema „Veränderung von Arbeitsaufgaben und Stellenplan in der Staatskanzlei" (LT-Drs.-Nr. 7/10737) die Mitarbeiterdaten der Beschäftigten der Sächsischen Staatskanzlei datenschutzwidrig veröffentlicht wurden.
Zwar erschienen diese Daten auf den ersten Blick schwarz, konnten jedoch durch Kopieren und Einfügen in beispielsweise ein Word-Dokument sichtbar gemacht werden. Zudem wurden diese bei einer EDAS-Suche als Ergebnis angezeigt. Der von mir angeschriebene Sächsische Landtag entfernte das gegenständliche Dokument unverzüglich.
Da das Dokument durch die Sächsische Staatskanzlei in EDAS eingestellt wurde, forderte ich diese zur Stellungnahme auf. Diese bestätigte zunächst, dass die Schwärzung im gegen-

ständlichen Dokument nicht nachhaltig erfolgte. Dazu wäre es zusätzlich erforderlich gewesen, bei den geschwärzten Passagen die dahinterliegenden Inhalte zu entfernen. Um dies künftig zu verhindern, seien den Beschäftigten (nochmals) Hinweise zum ordnungsgemäßen Schwärzen von personenbezogenen Daten gegeben worden. Auf meine Nachfrage wurden mir die Hinweise übersandt und zudem mitgeteilt, dass eine Prüfung aller in dieser Legislaturperiode durch die Sächsische Staatskanzlei verfassten Antworten zu parlamentarischen Anfragen und Vorgängen keine weiteren nicht nachhaltigen Schwärzungen ergeben habe.

Ich halte dies für ausreichend. Erwähnenswert halte ich, dass dieser Vorgang auch in der lokalen Presse thematisiert wurde, wenn auch nicht nur wegen des Datenschutzaspekts (beispielsweise in der Freien Presse vom 7. August 2024: „Datenpanne: Benutzt Kretschmer offizielle Regierungstermine für den Wahlkampf?").

Da diese fehlerhafte Schwärzung nicht der erste Vorfall im Berichtszeitraum war, habe ich die Petition zum Anlass genommen, eine Anleitung zum datenschutzgerechten Schwärzen auf meiner Homepage zur Verfügung zu stellen: sdb.de/tb2405

Was ist zu tun?
Jeder Verantwortliche sollte bei zu schwärzenden Dokumenten prüfen, ob eine entsprechende Unkenntlichmachung tatsächlich stattgefunden hat oder der Text lediglich entsprechend markiert wurde, und die Beschäftigten entsprechend sensibilisieren.

4.1.5 Verwendung mehrerer privater E-Mail-Adressen im offenen Adressfeld

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

Eine Wohnungsverwaltung hatte im Auftrag des Vermieters – wie wohl häufig vorkommend – das Protokoll der Mieterversammlung mit einer E-Mail gleichzeitig an mehrere E-Mail-Adressen der jeweiligen Mieter/innen mit offenem Verteiler versandt. Damit wurden allen Mieterinnen und Mietern die E-Mail-Adressen der anderen die Mitteilung empfangenden Personen offenbart. Dabei handelt es sich unproblematisch um eine Datenverarbeitung nach Art. 4 Nr. 2 Datenschutz-Grundverordnung (DSGVO). Die E-Mail-Adresse ist auch ein personenbezogenes Datum nach Art. 4 Nr. 1 DSGVO, bereits, soweit sie einem Individuum als Pseudonym zuordenbar ist,

erst recht, wenn in der E-Mail-Adresse der erkennbare Name (auch Namensbestandteile) angegeben ist.
Für eine rechtmäßige Datenverarbeitung benötigt der Verantwortliche gemäß der Datenschutz-Grundverordnung einen Rechtfertigungsgrund. Diese Gründe sind in Artikel 6 DSGVO abschließend angegeben.
Im vorliegenden Fall ist die Versendung des Protokolls im laufenden E-Mail-Verteiler – mit der Angabe der E-Mail-Adressen anderer Mieter/innen – gemäß Art. 6 Abs. 1 Buchst. b DSGVO zur Vertragserfüllung schlicht nicht erforderlich. Im seltenen abweichenden Falle eingeholter Einwilligungen bei sämtlichen betroffenen Personen und einem geeigneten Zweck der Transparenz des E-Mail-Verteilers sämtlicher Empfänger/innen kann gegebenenfalls anders verfahren werden.
Regelmäßig möchte verständlicherweise nicht jede Mieterin oder jeder Mieter, dass ihre bzw. seine private E-Mail-Adresse anderen bekannt wird, zumal es zwischen zahlreichen Mietparteien nach allgemeiner Lebenserfahrung regelmäßig vielfältige Konfliktlagen gibt. Dies kann – nicht nur – bei sehr großen Häusern mit dutzenden gegebenenfalls hunderten weiteren Mieterinnen und Mietern zu erheblichen Belästigungen durch unerwünschte E-Mails führen. Daher ist die einzelne private E-Mail-Adressatin bzw. der einzelne private E-Mail-Adressat erkennbar schutzbedürftig, was der Verantwortliche hätte voraussehen müssen. Insoweit war ein Datenschutzverstoß seitens der Wohnungsverwaltung zu bejahen.
Grundsätzlich sind die Beschäftigten von Haus- bzw. Wohnungsverwaltungen entsprechend zu schulen bzw. dahingehend zu sensibilisieren, damit derartige Datenschutzverstöße vermieden werden.

Was ist zu tun?
Wohnungsverwaltungen bzw. Vermieter/innen haben Informationen an alle Mieter/innen nicht im offenen E-Mail-Verteiler zu versenden, es sei denn, die Mieter/innen hätten zugestimmt. Gleiches gilt für ähnliche Fallgestaltungen in anderen Konstellationen, bei denen private E-Mail-Adressen verwendet werden sollen. Anders kann dies allerdings zum Beispiel bei beruflichen E-Mail-Adressen in Unternehmen, Behörden und Verbänden zu beurteilen sein.

4.1.6 Essen sicher online bestellen

↗ Art. 32 DSGVO

Die Beschwerde eines Online-Essenbestellers richtete sich gegen den Lieferdienst seiner Wahl, der das Passwort des Kundenkontos im Klartext speicherte und nicht auf seine Aufforderung reagierte, dies zu unterlassen.

Ich schrieb das Unternehmen an und bat um eine Stellungnahme im Rahmen der Zusammenarbeit mit der Aufsichtsbehörde, Art. 31 DSGVO. Vorsorglich gab ich dem Unternehmen den Hinweis, dass die Authentifizierung mittels Nutzername und Passwort bei Diensten eine Maßnahme nach Art. 32 DSGVO ist, Art. 58 Abs. 1 Buchst. d DSGVO. Um die Vertraulichkeit, Integrität und Verfügbarkeit der Daten dauerhaft zu gewährleisten, ist eine sichere Authentifizierung des Nutzers notwendig. Unzureichend sicher gespeicherte Passwörter stellen einen Verstoß gegen Art. 32 DSGVO dar.
Das Unternehmen optimierte den Registrierungsprozess zeitnah, das heißt, Klartextpasswörter werden nicht mehr gespeichert. Nachdem ich mich von der Umsetzung persönlich überzeugt habe, wurde der Beschwerdeführer über die Abstellung des Verstoßes informiert und der Vorgang von mir geschlossen.

Was ist zu tun?
Kundenorientiertes Verhalten durch Zuhören kann den Kundinnen und Kunden den Weg zur Aufsichtsbehörde und dem Unternehmen den Kontakt mit der Aufsichtsbehörde ersparen. Authentifizierungsdaten müssen bei der Speicherung und Verarbeitung ausreichend geschützt werden. Sie dürfen nicht im Klartext, sondern müssen immer verschlüsselt gespeichert und/oder übertragen werden.

4.2 Auftragsverarbeitung

4.2.1 „Elektronische" Übergabe und Versendung von Schreiben des Jugendamts des Landratsamts/der Kreisfreien Stadt durch einen Postdienstleister

↗ § 65 SGB VIII, § 80 SGB X

Der Datenschutzbeauftragte eines Landratsamts bat mich um Prüfung, ob die „elektronische" Übergabe und Versendung von Schreiben des Jugendamts durch einen Postdienstleister zulässig sei oder ob § 65 Abs. 1 Achtes Buch Sozialgesetzbuch (SGB VIII) dem entgegenstehe, da es sich bei den Daten um Sozialdaten handele, die dem Jugendamt anvertraut worden seien. Ich habe hierzu wie folgt Stellung genommen:

1. Für den Bereich des Sozialrechts trifft § 80 SGB X eine ergänzende Regelung, unter welchen Voraussetzungen die Auftragsverarbeitung von Sozialdaten erfolgen darf. Auch der Auftragsverarbeiter ist im Bereich des Sozialrechts kein „Dritter" nach Art. 4 Nr. 10 DSGVO.

2. Die Erteilung eines Auftrags nach Art. 28 DSGVO zur Verarbeitung von Sozialdaten ist zulässig, wenn die Voraussetzungen des § 80 SGB X vorliegen.
   Die Verarbeitung ist der Rechts- oder Fachaufsichtsbehörde des Jugendamts entsprechend den Anforderungen nach § 80 Abs. 1 SGB X rechtzeitig schriftlich oder elektronisch anzuzeigen. In Bezug auf den Ort der Verarbeitung ist § 80 Abs. 2 SGB X zu beachten. Zulässig ist die Auftragsverarbeitung nur, wenn § 80 Abs. 3 Nr. 1 oder Nr. 2 SGB X vorliegt. Danach ist die Erteilung eines Auftrags zur Verarbeitung von Sozialdaten durch nichtöffentliche Stellen nur zulässig, wenn beim Verantwortlichen sonst Störungen im Betriebsablauf auftreten können oder die übertragenen Arbeiten beim Auftragsverarbeiter erheblich kostengünstiger besorgt werden können.
3. Bei Schreiben des Jugendamts ist zu beachten, ob es sich dabei tatsächlich im Einzelfall um anvertraute Daten nach § 65 SGB VIII handelt, die dem dort normierten besonderen Weitergabeverbot unterliegen.
   Bei Daten im Sinne dieser Vorschrift handelt es sich um Daten, die tatsächlich (besonders und ganz persönlich, vor allem auch ausdrücklich) nicht dem Träger der öffentlichen Jugendhilfe, sondern einer einzelnen Fachkraft des Jugendamts „anvertraut" worden sind. Diese dürfen nicht weitergegeben werden, auch nicht im internen Dienstverkehr der Behörde (vgl. § 65 Abs. SGB VIII). Solche Daten sind aufgrund des § 65 SGB VIII nicht in der üblichen Weise behördenverfügbar – mit der Folge, dass diese Angaben (Daten) in der allgemeinen Sachakte des Jugendamts nichts zu suchen haben (siehe VG München, Beschluss vom 08.12.2011 - M 18 K9 11.5827 – juris Rn. 8; 9. Tätigkeitsbericht für den öffentlichen Bereich (2001), 10.2.9, Seite 146 f.).
   Daraus folgt, dass die Anforderungen an den Tatbestand des „Anvertrauens" bzw. „Anvertraut-Seins" über das allgemeine sich bereits aus der Natur der Sache im Bereich des SGB VIII oftmals gesteigerte Vertrauensverhältnis

zwischen dem/der Behördenmitarbeiter/in und dem/der zu Beratenden deutlich hinausgehen. Deshalb kann nicht jede Mitteilung der Klientin/des Klienten an die Fachkraft der Behörde im Bereich des SGB VIII als anvertraut bezeichnet werden. Vielmehr wird in der Fachliteratur zu Recht gefordert, dass sich der Betroffene gegenüber der Fachkraft der Behörde speziell in der Erwartung offenbart hat, dass diese die Informationen ausschließlich für sich behält im Sinne eines „das sage ich nur Ihnen und Sie dürfen es keinem weitersagen" und die Fachkraft ausdrücklich oder konkludent zu verstehen gibt, dass sie diese Verschwiegenheit zusichert.
Die Übersendung von Schreiben, die anvertraute Daten betreffen, scheidet folglich gemäß § 65 SGB XIII nur dann aus, wenn diese derartig „anvertraut" wurden. Damit scheidet folgerichtig auch nur dann eine Verarbeitung dieser Daten durch einen Auftragsverarbeiter aus. Eine andere Rechtslage ergibt sich, wenn die betreffende Fachkraft des Jugendamts nach entsprechender Prüfung die anvertrauten Daten auf der Grundlage einer der in § 65 Abs.1 SGB VIII genannten Übermittlungsbefugnisse und damit rechtmäßig weitergeben oder übermitteln darf, zum Beispiel wegen des Verdachts der Kindeswohlgefährdung nach § 8a Abs. 2 SGB VIII. Dann ist auch die elektronische Übermittlung an den Auftragsverarbeiter zum Zwecke der Versendung zulässig.

4. In Bezug auf die Einschaltung des Dienstleisters im Wege der Auftragsverarbeitung durch eine Behörde ist beim Abschluss des Auftragsverarbeitungsvertrags darauf zu achten, ob für die Wahrnehmung der Aufgabe eine Verpflichtung nach dem Verpflichtungsgesetz erforderlich ist (siehe Tätigkeitsbericht Datenschutz 2022, 4.2.2, Seite 140 f.). Das Landratsamt kann sich bei der Verpflichtung der Stelle bedienen, bei der die zu verpflichtende Person beschäftigt ist (siehe Tätigkeitsbericht Datenschutz 2023, 4.3.1, Seite 174 f.).

Tätigkeitsbericht Datenschutz 2022:
↗ sdb.de/tb2022

Was ist zu tun?
Das Landratsamt/Die Kreisfreie Stadt darf auch Schreiben des Jugendamts „elektronisch" an einen Postdienstleister übergeben und durch diesen versenden lassen, wenn es sich im Einzelfall nicht um anvertraute Daten nach § 65 SGB VIII handelt.

4.2.2 Auftragsverarbeitungsvertrag nach Art. 28 DSGVO bei Auskunftsanfragen externer Transplantationsbeauftragter im Organspende-Register

↗ Art. 28 DSGVO

Der Datenschutzbeauftragte eines Universitätsklinikums im Freistaat Sachsen bat mich um Stellungnahme zu folgender Frage:

Ist die Verwendung von Auftragsverarbeitungsverträgen erforderlich, wenn ein Krankenhaus, das für Organentnahmen zugelassen ist (Entnahmekrankenhaus), über externe Transplantationsbeauftragte Auskunft haben will, ob mit irreversiblen Hirnfunktionsausfall betroffene Menschen im Organspende-Register des Bundesinstituts für Arzneimittel und Medizinprodukte registriert sind?

Die Auskunft ist erforderlich, da noch nicht alle Entnahmekrankenhäuser die technischen und organisatorischen Voraussetzungen geschaffen haben, um selbst Einblick in das Organspende-Register nehmen zu können.

Meine Prüfung kam zu folgendem Ergebnis:

Art. 1 Abs. 1 Datenschutz-Grundverordnung (DSGVO) legt fest, dass diese Verordnung Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten enthält. Erwägungsgrund 27 DSGVO lautet wörtlich: „Diese Verordnung gilt nicht für die personenbezogenen Daten Verstorbener. Die Mitgliedstaaten können Vorschriften für die Verarbeitung der personenbezogenen Daten Verstorbener vorsehen."

Überdies ist die DSGVO nur für personenbezogene Daten von „natürlichen Personen" anwendbar (vgl. Art. 4 Nr. 1 DSGVO).

Ein Auftragsverarbeitungsvertrag im Sinne von Art. 28 DSGVO setzt eine Verarbeitung personenbezogener Daten voraus.

Zwar sind die im Organspende-Register vorhandenen Daten personenbezogen. Die DSGVO schließt aber die Anwendung der DSGVO hinsichtlich der personenbezogenen Daten eines Verstorbenen aus (siehe Erwägungsgrund 27 der DSGVO; BGH-Urteil vom 12.07.2018, III ZR 183/17, Rn. 67).

Eine natürliche Person wird als rechtsfähige Person im Sinne von § 1 Bürgerliches Gesetzbuch (BGB) verstanden. Dies liegt ab Vollendung der Geburt der Person vor.
Nach § 1922 Abs. 1 BGB geht mit dem Tode einer Person deren Vermögen auf eine oder mehrere andere Personen über. Daraus wird abgeleitet, dass die Rechtsfähigkeit der Person im Todeszeitpunkt endet mit der Folge, dass eine natürliche Person in Sinne des BGB im Todeszeitpunkt nicht mehr existiert.
Menschen mit irreversiblem Hirnfunktionsausfall gelten nach zurzeit vertretener medizinischer Meinung als tot. Bei Hirntod tritt der Tod einer Person ein (vgl. Müller-Christmann, in: BeckOK, 70. Edition, § 1922, Rn. 5).
Die DSGVO ist demnach hier nicht einschlägig. Es bedarf deshalb nach dem Tod des Patienten keines Auftragsverarbeitungsvertrags nach Art. 28 DSGVO zum Zwecke der Einsichtnahme in das Organspende-Register, da die DSGVO nur einen Schutz personenbezogener Daten von natürlichen Personen entfaltet, was im vorliegenden Fall zu verneinen ist.

Was ist zu tun?
Stellt eine externe Transplantationsexpertin oder ein externer Transplantationsexperte für ein Krankenhaus beim Organspende-Register einen Auskunftsantrag, ist es nicht erforderlich, dass das Klinikum deshalb mit der Transplantationsexpertin/dem Transplantationsexperten einen Auftragsverarbeitungsvertrag abschließt.

4.3 Sicherheit der Verarbeitung

4.3.1 Teile von Passwörtern dürfen nicht separat gespeichert werden

↗ Art. 32 DSGVO

Mich erreichte im letzten Jahr eine Petition zu der Authentifizierungsmethode eines Verantwortlichen in Sachsen. Im vorliegenden Fall benutzte der Kundendienst des Verantwortlichen ein Verfahren zur Verifikation der Identität eines Kunden über Kommunikationskanäle außerhalb des eigenen Systems (zum Beispiel Telefon oder E-Mail). Dafür fragte der Kundendienst den Kunden nach einem Teil des Passworts, welches für den Login bei dem Verantwortlichen genutzt wird. Der Petent vermutete einen Verstoß gegen die Sicherheit seiner Daten und wandte sich damit an mich.

Tätigkeitsbericht Datenschutz 2022:
↗ sdb.de/tb2022

Ich sehe in der Umsetzung tatsächlich einen Verstoß gegen Art. 32 Datenschutz-Grundverordnung (DSGVO). Wie ich bereits im Tätigkeitsbericht 2022 (4.3, Seite 141 ff.) geschrieben habe, dürfen Passwörter nicht im Klartext gespeichert werden. Art. 32 der DSGVO schreibt vor, dass unter Berücksichtigung des Stands der Technik und anderer Faktoren geeignete Maßnahmen getroffen werden, um personenbezogene Daten zu schützen. Ich sehe diese Bedingungen im Falle der gängigen Praxis, Passwörter durch Hash-Verfahren zu verschlüsseln, als erfüllt an. Unverschlüsselt gespeicherte Passwörter ermöglichen im Fall eines Datenlecks nicht nur den Zugang zu den Nutzerkonten, sondern sie legen auch Passwörter offen, welche von Kundinnen und Kunden häufig bei anderen Diensten genutzt werden. Tatsächlich kann ein beträchtlicher Anteil der Angriffe auf Nutzerkonten auf solche Datenlecks zurückgeführt werden.

Damit der Kundendienst einen Teil des Passworts selbst überprüfen kann, ohne dabei auf das unverschlüsselte Passwort zugreifen zu können, muss dieser Teil separat verfügbar sein. Hierbei ist es jedoch unerheblich, ob der separat verfügbare Teil durch Hash- oder andere Verfahren geschützt wird, da ein derartiger Schutz erst ab einer gewissen Mindestlänge funktioniert, welche auch Teil der Anforderungen an das Passwort ist. Unterhalb dieser Länge kann ein Angreifer mit einem hinreichend starken Computer alle möglichen Kombinationen durchprobieren und in kurzer Zeit den separaten Teil des Passworts offenlegen. Sobald ein Teil des Passworts im Klartext bekannt ist, sinkt jedoch die Sicherheit des verschlüsselten Passworts drastisch, da nun nur noch die übrigen Stellen erraten werden müssen. Um die Sicherheit des Passworts zu erhalten, müssten somit die Mindestanforderungen entsprechend angepasst werden. Sinnvoller wäre es jedoch, für niederschwellige Authentifizierungen einen anderen Mechanismus zu verwenden, wie beispielsweise eine PIN oder TAN.

Was ist zu tun?
Das separate Speichern von Teilen eines Passworts beeinträchtigt die Sicherheit des Passworts in der Regel auf unzulässige Weise. Stattdessen sollten Verantwortliche andere Mechanismen nutzen um die Identität einer Kontaktperson zu überprüfen.

4.4 Meldung von Datenschutzverletzungen

4.4.1 Allgemeine Hinweise zur Meldepflicht von Datenpannen

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

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

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

Tätigkeitsbericht Datenschutz 2023:
↗ sdb.de/tb2023

Sozialbehörden haben im Fall einer Meldepflicht nach Art. 33 DSGVO auch § 83a Zehntes Buch Sozialgesetzbuch (SGB X) zu erfüllen (siehe Tätigkeitsbericht 2023, 4.4.2, Seite 176 ff.).

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

Verstöße sowohl gegen Schutzmaßnahmen gemäß Art. 32 DSGVO als auch gegen formelle Anforderungen der Meldung bzw. Benachrichtigung gemäß Art. 33, 34 DSGVO können Gegenstand eines bußgeldrechtlichen Verfahrens gemäß Art. 83 Abs. 4 Buchst. a DSGVO werden. Daher empfehle ich

sowohl zum Schutz der Interessen der Betroffenen als auch der eigenen wirtschaftlichen Interessen der Verantwortlichen, die oben dargelegten Vorkehrungen zu prüfen und stets auf aktuellem Stand zu halten.

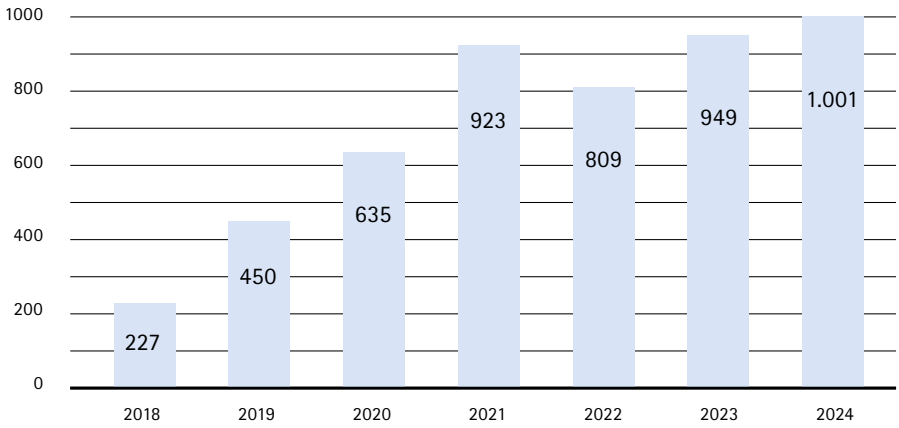
4.4.2 Wieder neuer Höchstwert bei Meldungen nach Artikel 33 DSGVO

↗ Art. 33 DSGVO

Nach Artikel 33 Datenschutz-Grundverordnung 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 2024 sind bei mir 1.001 solcher Meldungen eingegangen. Im Vergleich zum vorjährigen Berichtszeitraum 2023 mit 949 Meldungen entspricht dies einem leichten Anstieg um gut 5 Prozent und stellt zu den vorherigen Berichtszeiträumen erneut einen neuen Höchstwert der jährlichen Meldungen von Datenschutzverletzungen dar.

Abbildung 4:
Meldungen von Datenschutzverletzungen nach Art. 33 DSGVO



Die folgenden Fallgruppen sind im Berichtszeitraum besonders häufig gemeldet worden:

Fehlversendung

Die Fehlversendung von Unterlagen mit personenbezogenen Daten zählt weiterhin zu den häufigsten Ursachen für Datenschutzverletzungen. Häufig entstehen diese durch eine fehlerhafte Zuordnung von Dokumenten, Probleme bei der maschinellen Kuvertierung, ungenaue Adressdaten oder Verwechslungen von Namen. Obwohl das Risiko für betroffene Personen in der Regel als gering eingeschätzt werden kann – da die Datenschutzverletzung üblicherweise vom unbeabsichtigten Empfänger gemeldet wird – sind dennoch sofortige datenschutzrechtliche Maßnahmen erforderlich. Dazu zählen unter anderem die Löschung der übermittelten Daten, die Rücksendung der Dokumente, die Beseitigung der Fehlerursache sowie die korrekte Neuzustellung der Unterlagen. All diese Schritte hat der Verantwortliche zu veranlassen.

Offener E-Mail-Verteiler

Ein weiterer häufiger Grund für Datenschutzverletzungen, der mir regelmäßig gemeldet wird, ist die Nutzung eines offenen E-Mail-Verteilers. Dabei werden E-Mail-Adressen nicht im Blindkopie-Feld (Bcc), sondern im Kopie-Feld (Cc) angegeben. Dieser Fehler stellt eine typische Fallgruppe dar, die meldepflichtig ist, sofern die Empfänger/innen nicht ausdrücklich zugestimmt haben, dass ihre E-Mail-Adresse öffentlich weitergegeben wird. In solchen Fällen fehlt es an einer rechtlichen Grundlage für die Verarbeitung der personenbezogenen Daten. Die Nutzung eines offenen E-Mail-Verteilers beruht meist auf einem Versehen des Absenders. Aus diesem Grund ist es besonders wichtig, wiederholte Sensibilisierungsmaßnahmen zu ergreifen. Diese dienen nicht nur dazu, ähnliche Fehler zu verhindern, sondern fördern auch das allgemeine Bewusstsein für einen verantwortungsvollen Umgang mit personenbezogenen Daten in der E-Mail-Kommunikation.

Verlust auf dem Postweg

Neben der Fehlversendung gehört auch der Verlust von Unterlagen mit personenbezogenen Daten auf dem Postweg zu den häufig gemeldeten Vorfällen. Der zentrale Unterschied zur Fehlversendung liegt darin, dass beim Verlust der Verbleib der Unterlagen unklar bleibt. Dies führt dazu, dass das Risiko für die betroffenen Personen in der Regel höher eingestuft wird als bei einer Fehlversendung. Im Falle einer Fehlversendung kann der falsche Empfänger den Vorfall melden, wodurch eine abschließende Risikobewertung und eine rasche Klärung möglich sind. Beim Verlust hingegen besteht die Unsicherheit über den Verbleib der Dokumente, was das Risiko einer unbefugten Nutzung oder eines unberechtigten Zugriffs erhöht. Diese Ungewissheit erfordert besondere Aufmerksamkeit und proaktive Maßnahmen seitens des Verantwortlichen, um die möglichen Risiken für die betroffenen Personen zu minimieren. Eine sorgfältige Überwachung und ein effektives Reaktionsmanagement sind daher bei Verlusten von Unterlagen auf dem Postweg essenziell.

Einbruch und Diebstahl

Datenschutzverletzungen infolge von Diebstählen und Einbrüchen gehören auch im aktuellen Berichtszeitraum zu den häufig gemeldeten Vorfällen. Auffällig ist dabei, dass die kriminellen Handlungen nicht unbedingt darauf abzielen, personenbezogene Daten direkt zu erlangen. Vielmehr richten sich die Aktivitäten auf die Entwendung von Gegenständen, die personenbezogene Daten enthalten, wie beispielsweise Digitalkameras oder Laptops, und weniger auf die personenbezogenen Daten selbst. Dennoch darf das Risiko für die Betroffenen nicht unterschätzt werden, da nicht ausgeschlossen werden kann, dass die Täter später auf die gespeicherten Daten zugreifen, um daraus finanzielle Vorteile zu ziehen. Um das Risiko in solchen Fällen zu minimieren, ist es besonders wichtig, den Anreiz für Diebstähle zu verringern. Dies lässt sich durch die ordnungsgemäße Sicherung technischer Geräte erreichen – etwa indem diese nicht unbeaufsichtigt gelassen werden. Zudem tragen die Verschlüsselung der ge-

speicherten Daten, regelmäßige Backups und ein sicherer Passwortschutz maßgeblich dazu bei, die Auswirkungen solcher Vorfälle zu begrenzen.

Cyberkriminalität

Meldungen im Zusammenhang mit Cyberkriminalität bleiben auch im aktuellen Berichtszeitraum eine zentrale Kategorie von Datenschutzverletzungen. Diese umfassen alle Handlungen und Straftaten, die mithilfe von Informations- und Kommunikationstechnologien ausgeführt werden. Eine besondere Herausforderung liegt darin, dass diese Aktivitäten von nahezu jedem Ort der Welt aus durchgeführt werden können und die Täter ihre Spuren häufig effektiv verschleiern. Typische Beispiele für Cyberkriminalität sind Spam- und Phishing-Mails, die Verschlüsselung von Systemen durch Ransomware, der Einsatz von Schadsoftware (Malware) sowie das Ausnutzen von Sicherheitslücken. Solche Angriffe sind besonders problematisch, da sie nicht nur technisch vielfältig und zunehmend raffiniert sind, sondern auch global stattfinden und die Identifizierung der Täter/innen erheblich erschweren. Daher ist es essenziell, Sicherheitsmaßnahmen kontinuierlich zu optimieren und potenzielle Bedrohungen aktiv zu überwachen. Durch diese Vorsorge können schnelle und gezielte Gegenmaßnahmen ergriffen werden, um die Auswirkungen von Cyberangriffen so gering wie möglich zu halten.
Zur Vermeidung von Meldefällen ist hinsichtlich der technisch-organisatorischen Maßnahmen stets besonderes Augenmerk auf die Informations-/Datensicherheit zu legen. Insoweit verweise ich auch auf meine Hinweise zu vorbeugenden Maßnahmen unter 4.4.4.

Kompromittiertes E-Mail-Konto

Datenschutzverletzungen, die durch kompromittierte E-Mail-Konten entstehen, stellen ein ernstes Risiko dar und haben als Meldungen im Berichtszeitraum signifikant zugenommen. Bei derartigen Vorfällen gelangen unbefugte Dritte durch Hacking, Phishing oder unsichere Passwörter in den Besitz von

Zugangsdaten und nutzen das Konto, um personenbezogene Daten auszuspähen, betrügerische Nachrichten zu versenden oder weiteren Schaden anzurichten. Hinsichtlich der betroffenen Personen im Sinne des Art. 33 DSGVO sind sämtliche Personen einzubeziehen, deren personenbezogene Daten in dem E-Mail-Konto verarbeitet werden.
Anzeichen einer Kompromittierung können unter anderem folgende sein:

- Ungewöhnliche Aktivitäten: E-Mails im „Gesendet"-Ordner, die nicht vom Kontoinhaber verschickt wurden
- Fehlende oder gelöschte Nachrichten: Der Angreifer löscht Nachrichten, um Spuren zu verwischen.
- Benachrichtigungen über verdächtige Anmeldungen: Hinweise auf Zugriffe von unbekannten Geräten oder Standorten.
- Beschwerden von Kontakten: Freunde oder Kollegen melden verdächtige Nachrichten, die scheinbar von ihrer Adresse stammen.
- Abgewiesene Login-Versuche: Der Zugriff auf das Konto ist gesperrt, weil der Angreifer die Zugangsdaten geändert hat.

Um das Risiko einer Kompromittierung zu minimieren, sollten proaktiv Sicherheitsvorkehrungen getroffen werden:

- Starke Passwörter: Verwenden Sie komplexe Passwörter mit einer Kombination aus Buchstaben, Zahlen und Sonderzeichen. Vermeiden Sie leicht zu erratende Informationen wie Geburtsdaten.
- Zwei-Faktor-Authentifizierung (2FA): Aktivieren Sie 2FA, um eine zusätzliche Sicherheitsebene zu schaffen. Selbst wenn die Zugangsdaten kompromittiert sind, bleibt der Zugriff ohne den zweiten Faktor verwehrt.
- Regelmäßige Passwortänderungen: Ändern Sie Passwörter in regelmäßigen Abständen und verwenden Sie keine Wiederholungen oder ähnliche Varianten.
- Vorsicht bei Phishing-Mails: Seien Sie skeptisch gegenüber unaufgefordert erhaltenen E-Mails,

insbesondere solchen mit Links oder Anhängen. Prüfen Sie die Absenderadresse sorgfältig.
- Sicherheitsupdates: Halten Sie Betriebssysteme, Anwendungen und insbesondere E-Mail-Clients stets auf dem neuesten Stand, um Sicherheitslücken zu schließen.
- Schulungen: Sensibilisieren Sie Mitarbeiter/innen und andere Nutzer/innen für die Risiken und Erkennungsmerkmale von Cyberangriffen.
- Sicherheitsrichtlinien: Etablieren Sie klare Richtlinien für den Umgang mit E-Mail-Konten, zum Beispiel den Verzicht auf die Verwendung privater Geräte für berufliche E-Mails.
- Datenbackups: Erstellen Sie regelmäßig Backups wichtiger E-Mails, um im Falle eines Verlusts oder einer Sperrung des Kontos die Daten wiederherstellen zu können.

Falls es trotz Vorsorgemaßnahmen zur Kompromittierung eines E-Mail-Kontos kommt, sind schnelle und gezielte repressive Maßnahmen erforderlich, um Schäden zu begrenzen und weitere Risiken zu minimieren:

- Sperrung des kompromittierten Kontos: Sobald ein Vorfall bekannt wird, sollte der Zugang zum betroffenen Konto unverzüglich gesperrt werden.
- Passwortzurücksetzung: Das Passwort des Kontos muss umgehend geändert und dabei auf die Verwendung eines einzigartigen, starken Passworts geachtet werden.
- Überprüfung von Aktivitäten: Analysieren Sie die Aktivitäten des Kontos, um festzustellen, welche Daten betroffen sind und ob weitere Systeme kompromittiert wurden.
- Benachrichtigung der Betroffenen: Informieren Sie bei einem hohen Risiko betroffene Personen über den Vorfall gemäß Art. 34 DSGVO, insbesondere, wenn deren Daten kompromittiert wurden, und geben Sie Handlungsempfehlungen, zum Beispiel die Änderung von Passwörtern oder die Überprüfung von Transaktionen.

- Kontaktaufnahme mit den Behörden: Melden Sie den Vorfall bei der zuständigen Datenschutzbehörde gemäß Art. 33 DSGVO und gegebenenfalls den Strafverfolgungsbehörden, um rechtliche Schritte gegen die Täter/innen einzuleiten.
- Beseitigung der Schwachstellen: Identifizieren und beheben Sie die Ursachen der Kompromittierung, etwa durch die Schließung von Sicherheitslücken.
- Überwachung nach dem Vorfall: Beobachten Sie das Konto und angrenzende Systeme weiterhin, um Folgeangriffe zu verhindern.
- Incident Response Plan: Dokumentieren Sie den Vorfall und optimieren Sie Ihre Notfallpläne basierend auf den Erkenntnissen, um in Zukunft schneller reagieren zu können.

Kompromittierte E-Mail-Konten stellen eine ernst zu nehmende Bedrohung dar, da sie den Zugang zu sensiblen Informationen ermöglichen. Mit einem aufmerksamen Auge für Anzeichen wie ungewöhnliche Aktivitäten oder verdächtige Nachrichten und durch die Implementierung von Schutzmaßnahmen wie starken Passwörtern, Zwei-Faktor-Authentifizierung und regelmäßigen Schulungen lassen sich sowohl das Risiko minimieren als auch die Auswirkungen einer Datenschutzverletzung abmildern. Ein proaktiver Umgang mit E-Mail-Sicherheit ist entscheidend, um die Vertraulichkeit und Integrität personenbezogener Daten zu wahren.

4.4.3 Ausgewählte Meldungen von Datenschutzverletzungen

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

4.4.3.1 Diebstahl von Notebooks mit darauf befindlichen Gesundheitsdaten

↗ Art. 9, 33, 34 Abs. 1, 58 Abs. 2 Buchst. e in Verbindung mit Art. 34 Abs. 4 DSGVO

Im Berichtszeitraum beschäftigte ich mich intensiv mit der Meldung einer öffentlichen Stelle, bei der Notebooks gestohlen wurden. Auf diesen befanden sich Datenbankreplikationen, welche Gesundheitsdaten, insbesondere von Kindern, in sehr hoher Anzahl enthielten. Der Verantwortliche teilte mir mit, dass er im Rahmen einer Prüfung feststellte, dass bei den betroffenen Notebooks Mängel hinsichtlich der Verschlüsselung vorlagen, wodurch ein Zugriff auf die personenbezogenen Daten nicht ausgeschlossen werden konnte. Daraus ergab sich für mich, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge hat. Demnach sind die betroffenen Personen gemäß Art. 34 Abs. 1 DSGVO zu benachrichtigen, was mir der Verantwortliche so auch in Aussicht gestellt hatte. Die ursprüngliche Meldung dazu erfolgte zwar bereits im Jahr 2023, jedoch gingen mir im Berichtszeitraum ergänzende Informationen durch den Verantwortlichen zu, welche nach dessen Auffassung eine Änderung der bisherigen Risikoeinschätzung sowie eine Abweichung von der bisher vorliegenden Benachrichtigungspflicht nach Art. 34 Abs. 1 DSGVO ergäben. Ich stellte dem Verantwortlichen weitere Fragen bezüglich des zugrunde liegenden Sachverhalts. Nach intensiver Prüfung kam ich zu dem Ergebnis, dass weiterhin ein voraussichtlich hohes Risiko und somit eine Benachrichtigungspflicht der Betroffenen nach Art. 34 Abs. 1 DSGVO besteht. Zu meiner Risikobeurteilung trug insbesondere die Betroffenheit von Gesundheitsdaten bei, welche eine besondere Kategorie personenbezogener Daten

gemäß Art. 9 DSGVO darstellen. Zudem betreffen diese Daten Kinder, welche gemäß Erwägungsgrund 75 DSGVO einer besonderen persönlichen Schutzbedürftigkeit unterliegen. Ich stellte eine Anweisung nach Art. 58 Abs. 2 Buchst. e in Verbindung mit Art. 34 Abs. 4 DSGVO in Aussicht. Hiernach bin ich als Aufsichtsbehörde befugt, den Verantwortlichen anzuweisen, die von einer Verletzung des Schutzes personenbezogener Daten betroffenen Personen zu benachrichtigen. Nach der Anhörung des Verantwortlichen wurde die Anweisung noch im Berichtszeitraum von mir erlassen. Gegen diese Anordnung wurde nunmehr Klage eingereicht. Über den Fortgang des Verfahrens werde ich berichten.

4.4.3.2 Einbruch in Kindertageseinrichtungen und Diebstahl von Kameras

↗ Art. 34 Abs. 3 Buchst. c DSGVO

Eine gängige und sich häufende Fallkonstellation von Datenschutzverletzungen, welche mir gemeldet werden, stellen Einbrüche und Diebstähle in Kindertagesstätten dar. Dabei werden technische Geräte gestohlen, worunter sich oftmals auch Kameras befinden. So meldete mir ein Verantwortlicher im Berichtszeitraum, dass in der betroffenen Kindertageseinrichtung beschädigte Fenster und aufgebrochene Schränke vorgefunden wurden. Aus diesen wurden technische Geräte gestohlen, unter anderem zwei Kameras. Auf diesen befanden sich wiederum Fotos von den Kindern im Kita-Alltag. Der Verantwortliche teilte mir zunächst mit, dass die Betroffenen nicht benachrichtigt wurden, da nicht mehr nachvollzogen werden konnte, wie viele Fotos sich insgesamt auf den Kameras befanden und wer und wie viele Personen davon betroffen sind. Zudem ziele der Einbruch nach Aussage des Verantwortlichen primär auf die technischen Geräte ab. Hinsichtlich der getroffenen technischen und organisatorischen Maßnahmen sowie der Information an die Betroffenen trat ich in Kontakt mit dem Verantwortlichen. Auch wenn es bei dem Diebstahl vermutlich nur um die technischen Geräte ging, kann bezogen auf Kameras in der Regel dennoch nicht ausgeschlossen werden, dass unbefugte Dritte Zugriff auf die darauf befind-

lichen personenbezogenen Daten nehmen können. Dies begründet sich darin, dass diese oftmals keine Möglichkeit der Verschlüsselung besitzen. Deshalb sind dahingehend geeignete technische und organisatorische Maßnahmen von hoher Bedeutung, um die darauf befindlichen personenbezogenen Daten angemessen zu schützen. Diese können beispielweise darin liegen, die Fotos unverzüglich auf verschlüsselte Datenträger zu übertragen und sie anschließend von der Kamera bzw. der Speicherkarte zu löschen. Hinsichtlich der Aufbewahrung sollten für die Kameras zum Beispiel abgeschlossene Schränke genutzt werden. Der Verantwortliche teilte mir daraufhin mit, dass er ein Informationsschreiben an alle Eltern und Beschäftigten sowie einen Aushang angefertigt hat, um gemäß Art. 34 Abs. 3 Buchst. c DSGVO alle potenziell betroffenen Personen vergleichbar wirksam zu informieren. Zukünftig werden die Speicherkarten zugriffssicher und getrennt von den Kameras aufbewahrt. Die Fotos werden zeitnah von den Speicherkarten gelöscht.

4.4.3.3 Verlust von Proben für pathologische Untersuchungen

↗ Art. 4. Nr. 13, Art. 9 DSGVO

Der Verantwortliche einer nichtöffentlichen Stelle teilte mir im Rahmen einer vorläufigen Meldung nach Art. 33 Abs. 4 DSGVO mit, dass vermutlich der Verlust eines Paketes vorliegt, in welchem sich Proben für pathologische Untersuchungen befanden. Nachdem weitere Informationen vorlagen, teilte mir der Verantwortliche unverzüglich mit, dass sich dieser Verdacht bestätigte. Zudem trug er vor, dass es sich dabei spezifisch um eine für den Versand vorbereitete Transportbox zum Zweck der pathologischen Untersuchung handelte. Beim zu untersuchenden Material handelte es sich um Hautproben, welchen zudem Auftragsscheine für die Pathologie beilagen. Diese Hautproben wurden der Kategorie genetischer Daten nach Art. 4 Nr. 13 DSGVO zugeordnet. Nach Art. 9 DSGVO handelt es sich dabei um eine besondere Kategorie personenbezogener Daten, welche als besonders sensibel sowie besonders schutzwürdig gelten. Hierzu teilte mir der Verantwortli-

che zudem mit, dass eine Wiederholung der Probeentnahmen nicht vorgenommen werden kann, weshalb bei den betroffenen Personen etwaige maligne Erkrankungen zum damaligen Stand nicht ausgeschlossen werden konnten. Daraus ergibt sich, dass eine regelmäßige Verlaufskontrolle erforderlich ist. Die Betroffenen wurden in einem persönlichen Gespräch über den Vorfall informiert. Da nicht eindeutig aufgeklärt werden konnte, wie der Verlust eintrat, und mir der Verantwortliche mitteilte, dass der Prozess überprüft und modifiziert wird, nahm ich Kontakt mit ihm auf. Daraufhin teilte dieser mir ausführlich mit, inwiefern der Prozess angepasst wurde. Die Abläufe wurden umstrukturiert und angepasst. Unter anderem sind hierbei neue Dokumentationsvorgaben zu benennen, durch welche nun eine lückenlose Nachverfolgbarkeit besteht. Durch Veränderungen bezüglich der Aufbewahrung, der Überwachung sowie des Ortes der Paketübergabe wird ein Zugriff unbefugter Dritter unterbunden.

4.4.4 Vorbeugende Maßnahmen

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

- Daten sichern! Die Daten von Firmen und Organisationen müssen unbedingt gesichert sein. Diese Backups sollten selbst nicht von Cyberangriffen erfasst werden können
- Firewall richtig konfigurieren! Die Firewall sollte nur erforderliche Datenverbindungen zulassen. Auch ein Frühwarnsystem über ungewöhnlich hohen Datenverkehr kann Systemverantwortlichen dabei helfen, größeren Schaden abzuwenden.
- Notfallplan beachten! Für die Fälle von Cybererpressungen bzw. Hacker-Angriffen sollte ein Notfallplan vorliegen, der im Akutfall abzuarbeiten ist. Dazu gehört auch eine Regelung, wann der/die IT-Administrator/in, interne/r Datenschutzbeauftragte/r, die Daten-

schutzaufsichtsbehörde oder auch die Beschäftigten, Unternehmensleitung und Kundinnen bzw. Kunden 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 personenbezogene Daten betroffen sind
- Weiterbildung! IT-Verantwortliche und all jene, die in Unternehmen und Organisationen für die IT-Sicherheit zuständig sind, benötigen regelmäßig Weiterbildung.

5 Internationaler Datenverkehr

5.1 Datenschutz und Künstliche Intelligenz

↗ DSGVO, KI-Verordnung

Kaum ein anderes Thema hat im letzten Jahr so schnell an Bedeutung für den Datenschutz gewonnen wie Künstliche Intelligenz (KI). Losgetreten 2023 durch den durchschlagenden Erfolg von sogenannten „Large Language Models" (LLMs) wie ChatGPT, zeichnet sich nun ab, dass sich KI zunehmend in unseren Alltag integrieren wird. Die EU hat im August 2024 die KI-Verordnung erlassen, welche sich insbesondere mit der Eindämmung der Risiken bestimmter Formen von KI bzw. in bestimmten Einsatzgebieten von KI beschäftigt. Die DSGVO bleibt davon jedoch unberührt.

Mich erreichten im letzten Jahr vielfach Fragen aus der sächsischen Bevölkerung, Wirtschaft und öffentlichen Verwaltung, wie die DSGVO auf KI konkret anzuwenden ist. Der Bedarf nach rechtlicher Klarstellung ist hoch, nicht nur in Sachsen. Diese Unklarheiten betreffen insbesondere die Rechtsgrundlagen für das Training von KI-Modellen und deren Nutzung sowie die Verwendung möglicherweise rechtswidrig trainierter KI-Modelle.

Nach meiner Auffassung ist die DSGVO auch auf die Verarbeitung personenbezogener Daten in KI-Modellen anwendbar. So wurde beispielsweise ChatGPT mit Informationen auf öffentlichen Internetseiten trainiert. Eine Veröffentlichung von Daten im Netz ist aber für sich genommen kein hinreichendes Indiz, dass die betroffene Person die unbeschränkte Verwendung dieser Daten für das Training von KI-Modellen billigt.

Die Grundrechte insbesondere dieser Nutzenden müssen geschützt werden. Bei Verwendung von KI-Modellen ist auf die Verarbeitung personenbezogener Daten sowohl als Teil der Ausgabe des Modells als auch der Nutzenden zu achten. Die Vorgaben der DSGVO greifen jedenfalls dann nicht, wenn sichergestellt ist, dass keine personenbezogenen Daten verarbeitet werden. Die Verwendung rechtswidrig trainierter KI sollte daher durch sorgfältige Vorauswahl vermieden werden. Die europäischen Datenschutzbehörden werden 2025 diese und andere Fragen koordiniert über den Europäischen Datenschutzausschuss (EDSA) beantworten und Klarheit für datenschutzrechtskonforme KI in Europa schaffen. Zur Koordination in Deutschland hat die Konferenz der unabhängigen Datenschutzbeauftragten des Bundes und der Länder (DSK) nun einen neuen Arbeitskreis für KI geschaffen, an dem ich mich einbringen werde.

Was ist zu tun?

Im Netz verfügbare personenbezogene Daten dürfen nicht ohne Weiteres zum Training von KI verwendet werden. Wenn Zweifel an der Rechtskonformität eines Modells bestehen, sollte von der Verwendung abgesehen werden.

6 Sächsische Datenschutzbeauftragte

6.1 Zuständigkeit und Anforderungen an Beschwerden

6.1.1 Tracking der anderen Art

↗ § 12 Abs. 1 MStV, Art. 2 Abs. 2 Buchst. c DSGVO, Art. 85 Abs. 2 DSGVO

Wie wohl jede Aufsichtsbehörde werde auch ich immer wieder mit Sachverhalten konfrontiert, in denen Personen mit einem GPS-Tracker überwacht werden. Meist handelt es sich um Streitigkeiten unter (Ehe-)Partnern, und regelmäßig werden die Geräte an einem Fahrzeug angebracht mit dem Ansinnen nachzuvollziehen, wo sich die Partnerin oder der Partner gerade aufhält oder bewegt. Nicht selten wird das Gerät dann – beispielsweise bei einem Werkstattaufenthalt – entdeckt, und angesichts der bestehenden innerfamiliären bzw. partnerschaftlichen Spannungen ist auch schnell klar, wer den Tracker angebracht hat. Meine Einflussnahmemöglichkeiten als Datenschutzaufsichtsbehörde sind in diesen Fällen mit höchst persönlichem Bezug beschränkt, denn in bestehenden partnerschaftlichen Beziehungen greift regelmäßig die sogenannte Haushaltsausnahme des Art. 2 Abs. 2 Buchst. c Datenschutz-Grundverordnung (DSGVO), das heißt, die Datenschutz-Grundverordnung ist bei Ausübung zu ausschließlich persönlichen oder familiären Tätigkeiten nicht anwendbar. Anders gelagert war allerdings ein Fall, der im Berichtszeitraum an mich herangetragen worden ist. Der Beschwerdeführer hatte mir angezeigt, dass er in seiner neu erworbenen Jacke einen eingenähten GPS-Tracker gefunden hatte. Er hatte die Jacke über eine Verkaufsplattform erworben und

schon eine Weile getragen, als ihm ein im Nackenbereich befindlicher harter Gegenstand auffiel. Daraufhin hatte er das dort befindliche Markenlabel aufgetrennt und dabei den GPS-Tracker mit immerhin drei Batterien und einer englischen Nachricht entdeckt. Der Beschwerdeführer fühlte sich in seinen Persönlichkeitsrechten verletzt und sei geschockt gewesen, dass so etwas überhaupt möglich ist.

In der Nachricht hieß es sinngemäß, dass der GPS-Tracker für journalistische Zwecke installiert worden sei. Falls man ihn deaktivieren wolle, könne man eine dort angegebene Rufnummer kontaktieren. Die weiteren Recherchen führten dann in der Tat zu einer ARD-Dokumentation über Nachhaltigkeit in der Bekleidungsbranche, in der über den Einsatz der Ortungsgeräte berichtet worden war. Den Redakteuren sei es dabei um den Umgang mit von Kunden online erworbenen und anschließend zurückgesandten Kleidungsstücken gegangen. Ermittelt werden sollte dem Beitrag nach, ob und wo diese Kleidungsstücke tatsächlich wieder in den Verkauf gelangen. Nach der Darstellung sei nicht das Tracking von Personen beabsichtigt gewesen, sondern von Kleidungsstücken. Auch sei ein Personenbezug nicht herzustellen gewesen. Sobald ein verfolgtes Kleidungsstück in einem Wohngebiet gelandet sei, sei der Tracker nicht mehr verfolgt worden. Dies wäre dem Beitrag nach wohl auch bei der Jacke des Beschwerdeführers der Fall gewesen.

Das durch den Trackerfund beim Beschwerdeführer hervorgerufene Gefühl des Überwachtseins war für mich gleichwohl nachvollziehbar. Selbst wenn den tatsächlichen Umständen folgend seine Befürchtungen unbegründet gewesen sein sollten, ist es wie bei jeder Form der Überwachung: Es bleibt ein ungutes Gefühl, und eine Drucksituation ist es allemal. Der Beschwerdeführer musste sich auf die Aussagen und Zusicherungen der Journalisten in dem Fernsehbeitrag verlassen, ohne dabei vollkommen sichergehen zu können, dass tatsächlich kein Bezug zu ihm als Käufer und Träger der Jacke hergestellt werden konnte. Eine Kontaktaufnahme mit den Redakteuren hätte erst recht die Herstellung eines Personenbezugs ermöglicht.

Was ist zu beachten?
Beim GPS-Tracking im familiären Umfeld haben die Datenschutzaufsichtsbehörden ebenso wenig die Möglichkeit, Abhilfemaßnahmen zu ergreifen, wie beim GPS-Tracking im investigativen Journalismus.

Für mich als Datenschutzaufsichtsbehörde war hingegen keine Möglichkeit des Eingreifens gegeben. Die Tätigkeit (investigative Recherche) der verantwortlichen Redakteure unterfällt dem Medienprivileg (Art. 85 Abs. 2 DSGVO in Verbindung mit § 12 Abs. 1 Medienstaatsvertrag [MStV]), das heißt, die Datenschutz-Grundverordnung ist bis auf wenige Regelungen nicht anwendbar und eine Kontrollzuständigkeit meiner Behörde nicht gegeben.

6.2 Zahlen und Daten zu den Tätigkeiten 2024

6.2.1 Überblick zu den Arbeitsschwerpunkten

Betrachtet man sich die Anzahl und die Verteilung der neu angelegten Vorgänge in meiner Behörde, lassen sich einige Rückschlüsse bezüglich der Tätigkeitsschwerpunkte ziehen. So handelte es sich bei jedem vierten Vorgang um eine Beschwerde oder Kontrollanregung. Die Bearbeitung dieser Eingaben ist die Haupttätigkeit der Fachreferate. Weniger Zeit und Personal beansprucht in Summe die Prüfung der gemeldeten Datenschutzverletzung nach Artikel 33 Datenschutz-Grundverordnung. Diese Fälle machten etwa ein Fünftel aller Vorgänge aus. Beratungen sowie die Zusammenarbeit mit anderen Datenschutzaufsichtsbehörden gehören ebenfalls zu den Tätigkeitsschwerpunkten, was sich in den Vorgangszahlen gleichwohl widerspiegelt. Über ein Viertel aller Vorgänge betraf im Berichtszeitraum diese beiden Aufgabenbereiche.

6.2.2 Beschwerden und Kontrollanregungen

2024 erhielt ich insgesamt 1.255 Eingaben von Personen, die entweder von einem potenziellen Datenschutzverstoß betroffen waren oder als Nichtbetroffene darauf hinwiesen. Somit stieg das Aufkommen das dritte Jahr in Folge und be-

findet sich inzwischen wieder auf dem Niveau der ersten beiden Corona-Jahre. Der Zuwachs entfiel sowohl auf den nichtöffentlichen als auch den öffentlichen Bereich und betrug insgesamt rund 8 Prozent.

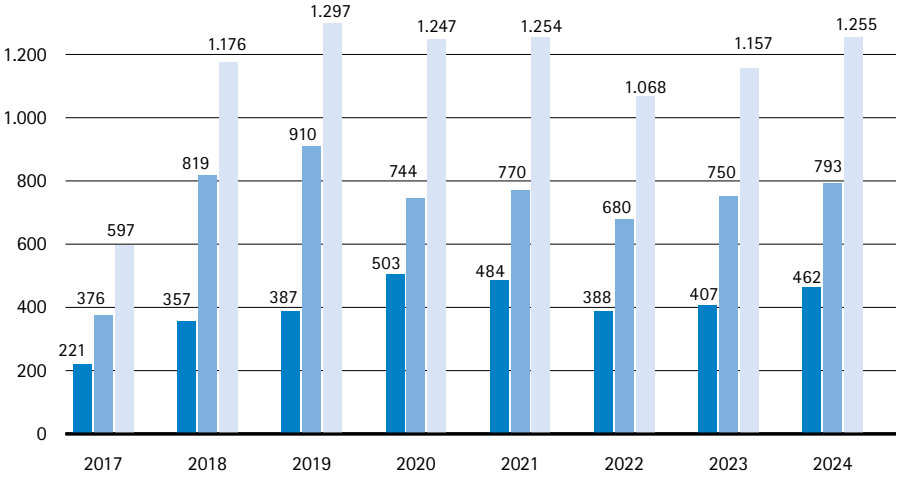


Abbildung 5:
Beschwerden und Kontrollanregungen

- öffentlicher Bereich
- nichtöffentlicher Bereich
- Beschwerden gesamt

6.2.3 Beratungen

Beratungen umfassen alle schriftlichen datenschutzrechtlichen Auskünfte gegenüber privaten und öffentlichen Stellen. Mit 736 Vorgängen stieg die Anzahl gegenüber 2023 (593) deutlich an. Unabhängig davon beantwortete meine Behörde auch 2024 wieder eine Vielzahl von Datenschutzfragen per Telefon. Diese Anfragen werden statistisch nicht erfasst. Der Anstieg bei den Beratungen betraf hauptsächlich den öffentlichen Bereich.

6.2.4 Meldungen von Datenpannen

2024 meldeten Verantwortliche 1.001 Datenschutzverletzungen – ein Plus von über fünf Prozent gegenüber dem Vorjahr und abermals ein neuer Höchststand. Zum Vergleich:

2023 gingen 949 Meldungen nach Artikel 33 Datenschutz-Grundverordnung 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 Abschnitt 4.4.

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: 11
- Verwarnungen: 47
- Anweisungen und Anordnungen: 40
- Geldbußen (nur nach DSGVO): 21
- Widerruf von Zertifizierungen: 0

6.2.6 Register der benannten Datenschutzbeauftragten

↗ Art. 37 Abs. 1 und 7 DSGVO

Im Berichtszeitraum gingen 1.092 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.

6.2.7 Zusammenarbeit mit europäischen Aufsichtsbehörden – Internal Market Information System

↗ Art. 4, 56–65 DSGVO

48 Aufsichtsbehörden aus dem Europäischen Wirtschaftsraum (EWR) sind Mitglieder des Europäischen Datenschutzausschusses (EDSA), darunter 18 deutsche. Über die Kommunikationsplattform der europäischen Aufsichtsbehörden, dem Internal Market Information System (IMI), habe ich auch im Berichtszeitraum aktiv an grenzüberschreitenden Verfahren mitgewirkt.

Tätigkeitsbericht Datenschutz 2023:
↗ sdb.de/tb2023

Weiterhin wurde jede Woche eine Übersicht über die neuen Verfahren im IMI erstellt, von denen ich durch notifications benachrichtigt werde (vgl. Tätigkeitsbericht 2023, 6.2.6, Seite 196 ff.). Die Anzahl der neuen Verfahren variiert: In der ersten Januarwoche 2024 waren es siebzehn neue Verfahren, in der 46. Kalenderwoche dagegen 87. Da die Zahl der Verfahren im IMI weiter gestiegen war, habe ich im November eine interne Verfahrensordnung erlassen, um die Arbeit effizienter zu gestalten.

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

Insgesamt habe ich im Berichtszeitraum diese Erklärung 205 Mal abgegeben. Dreimal musste ich auch klarstellen, dass ich mangels Hauptniederlassung des Verantwortlichen in Sachsen keine federführende Aufsichtsbehörde bin, da im IMI „alle deutschen Aufsichtsbehörden" bzw. „alle europäischen Aufsichtsbehörden" als federführende Aufsichtsbehörden bezeichnet waren. Vermutlich handelte es sich hier-

bei um technische Versehen. In 10 Verfahren meldete ich mich als betroffene Aufsichtsbehörde, in der Regel deshalb, weil in sächsischen Zweigniederlassungen des Verantwortlichen eine Datenverarbeitung erfolgt, die auch Gegenstand der Beschwerde ist. In 18 Verfahren im Rahmen der freiwilligen Amtshilfe antwortete ich auf Anfragen europäischer Aufsichtsbehörden. In den meisten Fällen ging es darum, welche Aufsichtsbehörden ein europaweit tätiges Unternehmen über eine Datenpanne informiert hatte und ob eine von ihnen deshalb Maßnahmen ergriffen hatte.

Im Berichtszeitraum wurden keine sächsischen Beschwerden mithilfe von IMI-Verfahren an die federführende Aufsichtsbehörde übermittelt. Ich habe mich auch in keinem Fall als federführende Aufsichtsbehörde gemäß Art. 56 Abs. 1 Satz 1 DSGVO im IMI gemeldet, da in keinem Verfahren der Beschwerdegegner seine einzige oder Hauptniederlassung gemäß Art. 4 Nr. 16 DSGVO in Sachsen hatte (Stand: 29.11.2024).

Überraschend verlief ein Verfahren gegen eine Firma für E-Mobilität mit einer einzigen Niederlassung in Leipzig. Als der Entwurf eines Bescheides gegen diese Firma im IMI eingestellt werden sollte, ergab sich aus dem Handelsregister, dass diese inzwischen von einer anderen Firma mit Sitz in Berlin aufgekauft worden war. Entsprechend dem Dokument des EDSA „Stellungnahme 8/2019 zur Zuständigkeit einer Aufsichtsbehörde im Falle einer Veränderung von Umständen, die die Hauptniederlassung oder die einzige Niederlassung betrifft" vom 9. Juli 2019 (Rn. 35) war die Zuständigkeit damit automatisch auf die Berliner Aufsichtsbehörde übergegangen. Im Rahmen eines Verfahrens zum Austausch relevanter Informationen im IMI wurde sie darüber informiert und die gesamte Akte übergeben. In diesem Verfahren bin ich jetzt wegen der Leipziger Niederlassung nur noch eine betroffene Aufsichtsbehörde gemäß Art. 4 Nr. 22 a DSGVO.

Unklar war die Bitte einer anderen europäischen Aufsichtsbehörde in einem Verfahren der freiwilligen Amtshilfe nach Art. 61 DSGVO, den Beschwerdeführer von einem Schreiben des Verantwortlichen zu informieren und der Aufsichts-

behörde dessen Reaktion zu übermitteln. Es war anhand der Angaben in diesem Verfahren nicht möglich, genau zu identifizieren, ob sich diese Anfrage an mich richtete, da gegen diesen Verantwortlichen nicht nur eine Sächsin oder ein Sachse, sondern auch viele andere Europäer/innen Beschwerde erhoben hatten. Vorsorglich übersetzte und übersandte ich das Schreiben an den sächsischen Beschwerdeführer und ersuchte im IMI vergeblich um Klarstellung. Es bleibt abzuwarten, ob diese Aufsichtsbehörde sich wegen der sächsischen Beschwerde wieder meldet.

Leider ohne Antwort blieb auch eine Anfrage an die spanische Datenschutzaufsichtsbehörde AEPD in dem Verfahren gegen eine dort allein ansässige Firma wegen einer sächsischen Beschwerde. Damals war unter anderem nach meinem Einspruch die Geldbuße von 30.000 auf 100.000 Euro heraufgesetzt worden (vgl. Tätigkeitsbericht 2023, 7.9, Seite 242 ff.). Der endgültige Bescheid wurde zwar in IMI gemäß Art. 60 Abs. 7 DSGVO veröffentlicht, wich aber inhaltlich – nicht im Ergebnis – vom durch die betroffenen Aufsichtsbehörden und damit auch von mir gebilligten Bescheidentwurf ab. In einem Verfahren zum Austausch relevanter Informationen wurde um Korrektur gebeten, aber eine Rückäußerung der spanischen Aufsichtsbehörde erfolgte nicht. Schließlich informierte ich den Beschwerdeführer vom Ausgang des Verfahrens gemäß Art. 60 Abs. 7 Satz 2 DSGVO. Dieses Verfahren nahm ich aber zum Anlass, die dahinterstehende grundsätzliche rechtliche Problematik des vom bindenden Entwurf abweichenden endgültigen Beschlusses im Arbeitskreis der Datenschutzkonferenz zur Diskussion zu stellen. Der Berliner Vertreter brachte die Frage im zuständigen Arbeitskreis des EDSA auf die Tagesordnung.

Verzögerungen gab es in einem anderen Verfahren, in dem ich einen Bescheidentwurf in einem formlosen Verfahren in IMI den übrigen betroffenen Aufsichtsbehörden vorstellte. Dieser bestand in einer Verfahrenseinstellung, da es sich nur um eine sehr geringe Datenschutzverletzung handelte und der Verantwortliche diese inzwischen beendet hatte. Erst drei Monate nach Ablauf der Äußerungsfrist kündigte eine andere europäische Aufsichtsbehörde einen Einspruch gegen

diese Entscheidung an, falls keine Verwarnung oder eine Abhilfeanordnung erginge. Ein im Ergebnis gleichlautender Bescheid, der auf die Einwände dieser Behörde eingeht, soll im IMI eingestellt werden, um eine Einigung herbeizuführen.
Am 1. März 2024 stellte ich erstmals, wie schon im vorangegangenen Tätigkeitsbericht (7.8, Seite 241 f.) angekündigt, einen endgültigen Beschluss für Sachsen gegen einen Online-Gastgeberdienst im IMI ein; dieser ist im Herbst auf der Website des EDSA veröffentlicht worden: sdb.de/tb2406
Zu zwei weiteren IMI-Verfahren finden Sie unter 7.7 und 7.8 zwei kurze Berichte.
Wie schon im vorangegangenen Jahr nahm ich gelegentlich die Beratung durch die Zentrale Anlaufstelle (ZASt) beim Bundesbeauftragten für den Datenschutz und die Informationsfreiheit bei schwierigen Fragen in Anspruch. Gerne besuchten einige meiner Mitarbeiter/innen eine IMI-Anfängerschulung und einen IMI-Workshop der ZASt in den Aufsichtsbehörden in Bonn und Wiesbaden. Ich hoffe, zu dem geplanten europaweiten IMI-Workshop auch Vertreter/innen meiner Behörde entsenden zu können.

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.
Weiterhin beteiligten mich die Landtagsfraktionen regelmäßig bei der Erarbeitung von Gesetzentwürfen und Änderungsanträgen. Hinzu kamen Stellungnahmen zu verschiedenen Vorhaben, die im Zusammenhang mit der Bundesgesetzgebung standen und mit denen sich auch die Datenschutzkonferenz befasste.

Da sich die Legislatur des Sächsischen Landtags 2024 dem Ende neigte, war die Zahl der Gesetzentwürfe, die noch vom Landtag verabschiedet werden sollten, enorm. Die wichtigsten im Jahr 2024 abgegebenen Stellungnahmen:

- Gesetz zur klinischen und epidemiologischen Krebsregistrierung im Freistaat Sachsen
- Gesetz zur Umsetzung europarechtlicher Vorgaben zum Einsatz von Informationstechnologie in der Verwaltung
- Gesetz über die Vergabe öffentlicher Aufträge im Freistaat Sachsen
- Neufassung der VwV A 14 – Qualifizierung Allgemeine Verwaltung
- Neufassung des Sächsischen Verfassungsschutzgesetzes
- Sächsische Gleichstellungsstatistikverordnung
- Sächsisches Sicherheitsüberprüfungsgesetz
- Sächsisches Hinweisgebermeldestellengesetz
- Sächsische Wohnteilhabeverordnung
- Verwaltungsvorschrift des Sächsischen Staatsministeriums des Innern über das Verwaltungsverfahren in Staatsangehörigkeitsangelegenheiten
- Viertes Gesetz zur Änderung des Polizeigesetzes des Freistaates Sachsen
- Vierte Verordnung zur Änderung der Sächsischen Urlaubs-, Mutterschutz- und Elternzeitverordnung

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

↗ DSGVO, SächsDSDG, SächsEGovG

Die zur Verfügung stehenden Haushaltsmittel (Personal- und Sachausgaben) zur Erfüllung meiner Aufgaben sind nach wie vor eng begrenzt. Das Arbeitsaufkommen bei Beschwerden, Beratungen und Datenpannen-Meldungen liegt weiterhin insgesamt auf hohem Niveau. Auch im Jahr 2024 wurden die Kapazitäten meiner Behörde größtenteils durch reaktive Tätigkeiten, wie die Bearbeitung von Beschwerden, die Begleitung von Rechtsetzungsvorhaben etc. beansprucht. Für meine als Aufsichtsbehörde zwingend erforderliche Fähigkeit, proaktiv kontrollieren und beraten zu können, bleiben mit einer Ausstattung von insgesamt 41 Stellen im Stellenplan nach wie vor zu wenige Kapazitäten übrig.

Insbesondere ist in dem für den nichtöffentlichen Bereich zuständigen Referat ein andauernder, sehr hoher Geschäftsanfall festzustellen. Die Mehrheit aller Petitionen/Eingaben/Anfragen/Auskunftsersuchen der Behörde geht in diesem Referat ein, das für nichtöffentliche Stellen, öffentliches Dienstrecht und Beschäftigtendatenschutz zuständig ist. Mit einer Kompensation der dauerhaften Mehrbelastung durch innerbehördliche Maßnahmen (zum Beispiel Umsetzung, Aufgabenverlagerung, Standardisierung) wurde reagiert, sie schafft aber aufgrund des außerordentlich hohen Geschäftsanfalls und fehlender freier Vakanzen kaum Abhilfe. Personelle Verstärkung wäre dringend erforderlich und wurde für den Haushalt 2025/2026 angemeldet.

Einen personellen Wechsel hatte ich zum Ende des Berichtszeitraums zu verzeichnen. Mein bisheriger Stellvertreter, Bernhard Bannasch, ist nach über 31 Jahren in der Behörde zum 31. Dezember 2024 in den Ruhestand versetzt worden. Neuer Stellvertreter ist Thomas Mauersberger, der weiterhin auch das Referat 4 Justiz/Polizei/Verfassungsschutz und Sächsisches Transparenzgesetz leitet.

Umzug der Dienststelle

Spätestens zum 1. April 2025 verlagert meine Behörde ihren Dienstsitz innerhalb Dresdens dauerhaft von der Devrientstraße 5 in die Maternistraße 17. Dafür wurden bereits im Jahr 2024 durch die vorhandenen Mitarbeiterinnen und Mitarbeiter, zusätzlich zum eigentlichen fachlichen Arbeitsanfall, die vorbereitenden technisch-organisatorischen Maßnahmen getroffen. Das bedeutete eine große, zusätzliche Anstrengung, die im Jahr 2025 weiter zunehmen wird.
Mit der dauerhaften Behördenunterbringung kommen die Aufgaben einer eigenständigen Liegenschaftsverwaltung neu auf die Dienststelle zu. Die bisherigen Synergieeffekte aus der räumlichen Nähe zur Verwaltung des Sächsischen Landtages entfallen endgültig. Zur Aufrechterhaltung des ordnungsgemäßen Dienstbetriebes ist die Wahrnehmung von Aufgaben wie Zutrittsmanagement, Funktions- und Zustandskontrollen der technischen Anlagen (insbesondere Einbruch- und Brandmeldeanlage), Wartungs-/Reparaturarbeiten, (Post-)Boten- und Kurierfahrten und Wahrnehmung von Verkehrssicherungspflichten dringend notwendig. Für diese Anforderungen sind derzeit keine personellen Ressourcen vorhanden. Auch dafür haben wir deshalb eine Anmeldung für den Haushalt 2025/2026 vorgenommen.

Digitalisierung der Behörde

Als oberste sächsische Landesbehörde bin ich im Bereich der Querschnittsverwaltung mit der Staatsregierung gut vernetzt und in den entsprechenden Gremien vertreten. Ich beteilige mich unter anderem an den landesweiten Projekten zur Einführung eines elektronischen Personalmanagement-Systems (ePM.SAX) und dem Digitalisierungsvorhaben „IT-Strategie HKR 2025" zur Etablierung eines zukunftsfähigen integrierten Kassen- und Rechnungswesens. Hier hat meine Behörde im Jahr 2024 den Teil der Einführung der elektronischen Eingangsrechnungsbearbeitung (eERB) im laufenden Betrieb unter stetig hohem Arbeitsanfall in den Bereichen Haushalt und Vergabe in hervorragender Weise bewältigt.

Mit der Einführung der vollelektronischen Akten- und Vorgangsbearbeitung im April 2024 in meiner Behörde wurde außerdem das Gesetz zur Förderung der elektronischen Verwaltung im Freistaat Sachsen (Sächsisches E-Government-Gesetz – SächsEGovG) umgesetzt. Die vollelektronische Akten- und Vorgangsbearbeitung erfolgt durch die Basiskomponente eVA.SAX – der elektronischen Vorgangs- und Aktenbearbeitung im Freistaat Sachsen. Somit wird der gesamte Lebenszyklus der bis März 2024 geführten Papier-Akte, bis auf Ausnahmen wie den Bereich der Ordnungswidrigkeitenverfahren, vollständig in elektronischer Form abgebildet. Dies reicht von der Ablage von aktenrelevantem Schriftgut, der elektronischen Bearbeitung von Vorgängen bzw. Geschäftsgängen bis hin zur Ablage einer abgeschlossenen Akte im elektronischen Langzeitspeicher. Je nach hinterlegter Aussonderungsart wird dann nach Ablauf der Aufbewahrungsfrist durch meine Behörde und das Sächsische Staatsarchiv bewertet, ob die Akte vernichtet oder zur Archivierung dem elektronischen Staatsarchiv zugeführt wird. Die Schulung aller Bediensteten hierfür und die Umsetzung der Einführung erfolgte ebenfalls im laufenden Dienstbetrieb. Das Ergebnis der Einführung werte ich als überaus positiv.

Was ist zu tun?
Die Erfüllung meiner Aufgaben als Sächsische Datenschutz- und Transparenzbeauftragte bleibt mit den vorhandenen personellen Ressourcen herausfordernd. Insbesondere für die Bearbeitung von Datenschutzvorgängen im nichtöffentlichen Bereich wird personelle Unterstützung benötigt.

6.2.10 Aufbau und Betrieb des IT-Labors

↗ Art. 32 DSGVO, TDDDG

In den Beiträgen 1.4 und 1.5 wurde über die ersten größeren Prüfungen berichtet, die mit der neu entstandenen IT-Laborumgebung durchgeführt wurden. Nachfolgend sollen Hintergründe und Aufbau der Umgebung näher erläutert werden.
Die Hauptaufgabe des IT-Labors liegt in der Prüfung und Analyse digitaler Anwendungen hinsichtlich ihrer datenschutzkonformen Umsetzung sowie der Bereitstellung dafür benötigter Voraussetzungen.
Daraus resultierende Teilaufgaben bestehen in der steten Sammlung und Einarbeitung in existierende Werkzeuge und Prüftools, der (Weiter-)Entwicklung von Prüfwerkzeugen,

dem Aufbau einer entsprechenden Laborumgebung sowie der Durchführung von Analysen und der Aufbereitung der Ergebnisse.

Entsprechende Untersuchungsgegenstände sind derzeit insbesondere Websites und mobile Anwendungen. Durchgeführt werden können hierbei sowohl statische Analysen (beispielsweise Einbettung von Drittanbieterbibliotheken) als auch insbesondere dynamische Analysen, das heißt, die Beobachtung der Anwendungen zur Laufzeit. Bei Letzterem liegt der Fokus auf der Analyse des Netzwerkverhaltens der digitalen Anwendung. Entscheidende Zeitpunkte sind dabei der erste Aufruf der Anwendung vor jeglicher Einwilligung, nach Ablehnung aller optionalen Datenverarbeitungsschritte sowie während der Nutzung der Anwendung.

Somit können klare Verstöße zwischen dargestellten Datentransfers (beispielsweise mittels Cookie-Banner) und der tatsächlichen Übertragung festgestellt werden. Neben der Analyse der Metadaten (zum Beispiel Verbindungspunkte, Datenpaketeigenschaften, Einsatz von Transportverschlüsselung und deren Eigenschaften) gehört hierzu auch die Analyse der versendeten Inhalte mit Fokus auf übertragene personenbeziehbare Daten und Identifikatoren.

Die dafür notwendige Umgehung der Transportverschlüsselung und eingesetzter Schutzmechanismen (beispielsweise Zertifikatpinning) gehört ebenso zu den Aufgaben des IT-Labors. Mobile Anwendungen können dabei sowohl auf physischen Geräten als auch in emulierten Umgebungen analysiert werden.

Als finaler Schritt gehört eine verständliche Aufbereitung, Sichtung und Speicherung der Analyseergebnisse zum Aufgabenbereich des IT-Labors. Neben manuellen Analysen für konkrete Fälle zählt auch die automatisierte Erstellung eines Überblicks über die datenschutzkonforme Umsetzung sächsischer digitaler Anwendungen zu den Aufgaben des IT-Labors. Im Berichtszeitraum konnte hierfür beispielsweise ein stetig wachsender Datensatz mit über 30.000 sächsischen Websites erstellt sowie eine entsprechende Umgebung entwi-

ckelt werden, welche eine automatisierte Analyse und übersichtliche Aufbereitung der Ergebnisse ermöglicht.
Zu den weiterführenden Aufgaben gehört die Ableitung möglicher Datenschutzaufsichtsmaßnahmen, die Aktualisierung und Pflege des Datensatzes, die Weiterentwicklung der Softwareumgebung und die weiterführende Kontrolle entsprechender digitaler Angebote.
Weitere Teilaufgaben umfassen unter anderem den Bereich der digitalen Forensik, beispielsweise die Sicherung und Wiederherstellung gelöschter Videos von Netzwerk-Videorekordern zur Beweissicherung, die Unterstützung der Referate in technischen Fragestellungen und die wissenschaftliche Kooperation und der einhergehende Wissensaustausch für die Entwicklung von Prüfwerkzeugen und die Diskussion technischer Neuerungen. Daraus resultierend entwickelt sich beispielsweise seit 2024 allmählich eine bereichsübergreifende Zusammenarbeit von Datenschutzaufsichtsbehörden und Wissenschaft, die sich mit den datenschutzrechtlichen Aspekten beim Mobilfunkstandard 6G beschäftigen. Dabei steht insbesondere die angestrebte Integration von Funkkommunikation und Funk-Sensorik, auch bekannt als Joint Communication and Sensing, im Fokus.

Was ist zu beachten?
Sowohl meine Behörde als auch andere Datenschutzaufsichtsbehörden haben in den vergangenen Jahren ihre Analysefähigkeiten und -kapazitäten erheblich erweitert und gestärkt. Verantwortliche sollten sich darauf einstellen, um dem Grundsatz der Rechenschafts- und Nachweispflicht (unter anderem Art. 5 DSGVO) jederzeit Folge leisten können.

6.3 Datenschutzaufsichtliche Befugnisse, verwaltungsrechtliche Entscheidungen

6.3.1 Datenschutzfragen in Zusammenhang mit der Arbeit des 2. Untersuchungsausschusses des 7. Sächsischen Landtags

↗ DSGVO, SächsDSDG, SächsVerf, UAusschG

Etliche Anfragen erreichten mich in Zusammenhang mit der Arbeit des 2. Untersuchungsausschusses des 7. Sächsischen Landtags, Einsetzungsgegenstand: „Mutmaßlich rechtswidrige Förderpraxis bei Asyl- und Integrationsmaßnahmen im Verantwortungsbereich von Staatsministerin Köpping aufklären".

1. Datenschutzgerechte Übersendung von Akten an den Untersuchungsausschuss

So ging es insbesondere um die Problematik der Übersendung von Unterlagen mit personenbezogenem Inhalt seitens des Sächsischen Rechnungshofs sowie der Sächsischen Aufbaubank an den benannten Untersuchungsausschuss.
Gegenüber den verantwortlichen Stellen habe ich dabei – mit der Bitte um Beachtung – auf Folgendes hingewiesen: Nach Art. 54 Verfassung des Freistaates Sachsen (SächsVerf) hat der Sächsische Landtag das Recht und auf Antrag von einem Fünftel seiner Mitglieder die Pflicht, Untersuchungsausschüsse einzusetzen, wobei der Gegenstand der Untersuchung im Einsetzungsbeschluss festzulegen ist. Dies ist in Bezug auf den streitgegenständlichen Vorgang nach zunächst erfolgter Beratung im Verfassungs- und Rechtsausschuss in einer Sondersitzung des Landtags am 9. Februar 2024 erfolgt. Der Untersuchungsausschuss hat sich daher ordnungsgemäß konstituiert. Auch soweit ein Untersuchungsausschuss auf einem Antrag einer Fraktion des Sächsischen Landtags beruht, handelt es sich mithin um einen Ausschuss des Sächsischen Landtags, nicht einer Fraktion oder Partei. Die Zusammensetzung des benannten Untersuchungsausschusses folgte den gesetzlichen Vorgaben.
Zur Erfüllung ihres Auftrags haben Untersuchungsausschüsse besondere Aufklärungsbefugnisse. Die Rechtsgrundlage hierfür findet sich neben der bereits genannten Regelung in der Verfassung des Freistaates Sachsen in § 14 Untersuchungsausschußgesetz (UAusschG).
Danach sind alle Behörden des Landes sowie Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts, die der Aufsicht des Landes unterstehen, unmittelbar zur Vorlage von Akten und zur Erteilung von Auskünften verpflichtet. Die Aktenvorlage, die Auskunftserteilung und die Aussagegenehmigung dürfen nur unter den Voraussetzungen des Art. 54 SächsVerf und den in § 14 UAusschG genannten Gründen verweigert werden. Das Bundesverfassungsgericht (BVerfG) hat den Stellenwert der Akten bei der Untersuchung politischer Vorgänge als besonders wichtiges Beweismittel betont

(BVerfG, Beschluss vom 17.06.2009 – 2 BvE 3/07). Danach müsse der Untersuchungsausschuss sich nicht mit Aktenauskünften zufriedengeben oder sein Verlangen auf bestimmte Aktenteile beschränken. Vielmehr solle er sich anhand der vollständigen Akten selbst ein Bild vom Umfang ihrer Entscheidungserheblichkeit machen können (vgl. 17. Juli 1984 – 2 BvE 11, 15/83). Der Vorlageanspruch beziehe sich grundsätzlich auf alle Akten, die mit dem Untersuchungsgegenstand in Zusammenhang stehen. Bei einem Ersuchen auf Aktenvorlage muss nicht bereits feststehen, dass die Unterlagen auch tatsächlich entscheidungserhebliches Material oder entsprechende Beweismittel enthalten. Es reiche aus, wenn sie Hinweise hierauf geben könnten.

Die Grenzen des Beweiserhebungsrechts bilden nach Art. 54 Abs. 4 SächsVerf der Kernbereich exekutiver Eigenverantwortung oder das Entgegenstehen gesetzlicher Regelungen, Rechte Dritter oder überwiegende Belange des Geheimschutzes. Das BVerfG hat mit Blick auf das Recht auf informationelle Selbstbestimmung, das bei Beweiserhebungen häufig berührt sei, deutlich gemacht, dass es nur im überwiegenden Interesse der Allgemeinheit und unter fallbezogener Anwendung des Grundsatzes der Verhältnismäßigkeit eingeschränkt werden darf. Das Beweiserhebungsrecht des parlamentarischen Untersuchungsausschusses und der grundrechtliche Datenschutz stünden sich auf der Ebene des Verfassungsrechts gegenüber und müssen im konkreten Fall einander so zugeordnet werden, dass beide so weit wie möglich ihre Wirkungen entfalten (Urteil vom 17. Juli 1984 – 2 BvE 11, 15/83).

Im Rahmen der gebotenen Abwägung sei auch zu prüfen, ob nach den Umständen eine öffentliche Beweisaufnahme gerechtfertigt sei oder die Grundrechte einen Ausschluss der Öffentlichkeit und sonstige Vorkehrungen zur Geheimhaltung erfordern. Die Bedeutung, die das Kontrollrecht des Parlaments sowohl für die parlamentarische Demokratie als auch für das Ansehen des Staates habe, gestattet in der Regel dann keine Verkürzung des Aktenherausgabeanspruchs zugunsten des Schutzes des allgemeinen Persönlichkeits-

rechts und des Eigentumsschutzes, wenn Parlament und Regierung Vorkehrungen für den Geheimschutz getroffen haben, die das ungestörte Zusammenwirken beider Verfassungsorgane auf diesem Gebiete gewährleisten, und wenn der Grundsatz der Verhältnismäßigkeit gewahrt ist (Bundesverfassungsgerichtsentscheidung a. a. O.).

Soweit Behörden des Landes zur Aktenvorlage nach § 14 UAusschG verpflichtet sind, haben sie für die zu übersendenden Dokumente eine Abwägung zwischen Kontrollrecht des Parlaments und Rechte Dritter vorzunehmen. Der Geheimhaltungsschutz durch Verfahrensgestaltung ist dabei zu berücksichtigen. Erst wenn dieser Schutz nicht ausreichend erscheint, kann in begründeten Fällen die Vorlage von Akten bzw. Aktenteilen verweigert werden. Die Hürden an Begründung und Rechtfertigung daran sind allerdings – so zeigt der Beschluss des BVerfG – recht hoch. Eine Ausnahme gilt für solche Informationen, deren Weitergabe wegen ihres streng persönlichen Charakters für die Betroffenen unzumutbar ist. Dies wurde etwa im Fall eines minderjährigen Opfers sexualisierter Gewalt bejaht (Verfassungsgerichtshof für das Land Nordrhein-Westfalen [VerfGH], Urteil vom 20.04.2021 – VerfGH 177/20). Die Weitergabe von Informationen, die den Kernbereich privater Lebensgestaltung betreffen, ist immer unzumutbar. In solchen Fällen kommt eine Aktenvorlage nur unter besonderen datenschutzrechtlichen Vorkehrungen in Betracht, die eine Identifizierbarkeit der Betroffenen wirksam ausschließen. Hierbei genügt regelmäßig eine anonymisierende Bearbeitung, wobei in bestimmten Ausnahmefällen aber auch eine Pseudonymisierung der vorzulegenden Akten geboten sein kann (VerfGH NRW a. a. O).

2. EuGH: Tätigkeit des Untersuchungsausschusses unterfällt der DSGVO

Der Europäische Gerichtshof hat mit Urteil vom 16.01.2024 in der Rechtssache C-33/22 klargestellt, dass das Tätigwerden eines parlamentarischen Untersuchungsausschusses in den Anwendungsbereich der DSGVO fällt. Hinsichtlich der eigentlichen Tätigkeit des Untersuchungsausschusses in

Bezug auf die Verarbeitung personenbezogener Daten zur Erfüllung des parlamentarischen Untersuchungsauftrags musste ich indes auf meine fehlende Kontrollbefugnis gegenüber dem Parlament verweisen: Die Zuständigkeit meiner Behörde nach § 14 Abs. 1 Satz 2 Sächsisches Datenschutzdurchführungsgesetz (SächsDSDG) erfasst über den Verweis auf § 2 Abs.1 Satz 3 und 4 SächsDSDG auch die Tätigkeit des Sächsischen Landtags, allerdings ohne dessen parlamentarische Funktionen. Hierzu zählt aber auch die Tätigkeit eines parlamentarischen Untersuchungsausschusses.

3. Art. 15 – Auskünfte: Keine offenkundig unbegründeten oder exzessiven Anträge

Im Zuge der Arbeit des Untersuchungsausschusses kam es nach Angaben des betroffenen Staatsministeriums schließlich zu einer Vielzahl von Auskunftsersuchen gemäß Art. 15 DSGVO, wozu aus Sicht des Ministeriums offensichtlich unter Nutzung eines Musterverfahrens aufgerufen worden war, mit dem Ziel der Überlastung der Verwaltung und dem Aufbau von tatsachlichem (Presse), politischem und persönlichem Druck, etwaige personenbezogene Daten nicht an den Ausschuss zu übermitteln. Insoweit stand im Raum, ob nicht Art. 12 Abs. 5 Buchst. b DSGVO hier erfüllt sein könnte, der bei offenkundig unbegründeten oder exzessiven Anträgen ein Leistungsverweigerungsrecht für den Auskunftspflichtigen begründen kann.

Ich hatte indes Zweifel, dass die Auskunftsanträge, die von einer Vielzahl von Privatpersonen an das Ministerium gerichtet wurden, hier durch eine solche zentral gesteuerte und zielgerichtete Überlastung motiviert waren, und dies aus folgenden Erwägungen: Im Zuge der Einsetzung des 2. Untersuchungsausschusses der 7. Wahlperiode wurden von den verantwortlichen Stellen in großem Umfang personenbezogene Daten an den Untersuchungsausschuss übermittelt. Die Daten bezogen sich auch auf die mit den Förderprogrammen finanzierten Personen in einzelnen Projekten. Diese Personen sahen die nicht abzuweisende Gefahr, dass ihre Privatadressen und weitere, auch sensible personenbezogene Daten von

der den Ausschuss einsetzenden Fraktion und damit möglicherweise auch für andere Zwecke verarbeitet werden. Das Anlegen von Listen von möglichen politischen Gegnerinnen und Gegnern ist ein in manchen Szenen nicht seltenes Mittel zur Vorbereitung von geplanten gesellschaftlichen Umstürzen. Zu erfahren, welche personenbezogenen Daten von einem Verantwortlichen verarbeitet und an wen übermittelt wurden, ist ein zentraler Grundsatz des Datenschutzrechts und war gerade im Falle dieses Untersuchungsausschusses für die betroffenen Personen die einzige Möglichkeit, um die Gefahren, die möglicherweise mit der Preisgabe ihrer Daten einhergingen, abzuschätzen und eventuell Vorkehrungen zu treffen. Dass sich dabei auch Personen an den Verantwortlichen wenden, deren Daten nicht gespeichert sind, bedeutet nicht, dass deren Anfrage auf eine Überlastung der Verwaltung gerichtet war. Oft wissen Betroffene nicht sicher, ob und welche Daten beim Verantwortlichen vorhanden sind. Auch die Nutzung von Musteranträgen für eine Auskunft ist kein Indiz für unbegründete oder übermäßige Anträge. So stellen beispielsweise die Datenschutzaufsichtsbehörden unter www.datenschutz.de/muster-formulierungshilfen eine Reihe von Formulierungshilfen zur Verfügung.

Was ist zu beachten?
Art. 54 Abs. 4 SächsVerf und § 14 UAusschG verpflichten bei der Aktenvorlage zu einer Abwägung zwischen dem Kontrollrecht des Parlaments und den Rechten Dritter.

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 Abs. 1 Sächsisches Datenschutzgesetz alte Fassung (§ 38 Abs. 3 Satz 1 SächsDSG a. F.),
- § 22 Abs. 1 Sächsisches Datenschutzdurchführungsgesetz (§ 22 Abs. 3 SächsDSDG),

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

Im Berichtszeitraum waren im öffentlichen Bereich insgesamt 69 Bußgeldverfahren anhängig. Davon wurden 11 mit einem Bußgeld abgeschlossen, wobei in 5 Verfahren Einspruch gegen den erlassenen Bußgeldbescheid eingelegt worden ist. Eine Entscheidung steht jeweils noch aus. In einem Verfahren aus dem vorherigen Berichtszeitraum ist der Bußgeldbescheid gerichtlich bestätigt worden und erlangte Rechtskraft. In 18 Verfahren erfolgte eine Einstellung bzw. wurde von der Verfolgung abgesehen. In 20 Verfahren wurde eine Verwarnung ohne Verhängung eines Verwarngeldes ausgesprochen, 1 Verfahren wurde an die zuständige Behörde abgegeben. 19 Verfahren befanden sich zum Ende des Berichtszeitraumes noch in Bearbeitung.

Die Summe der festgesetzten Buß- und Verwarngelder belief sich auf 14.580 Euro, die der rechtskräftigen auf 1.680 Euro. Die Differenz der Beträge erklärt sich aus dem Umstand, dass gegen eine Reihe von Bußgeldbescheiden Einsprüche eingelegt wurden, über die bislang noch nicht gerichtlich entschieden wurde.

Gegenüber dem vergangenen Berichtszeitraum ist die Zahl der neu eingegangenen Ordnungswidrigkeitenverfahren konstant geblieben. Ein Großteil der zu bearbeitenden Ordnungswidrigkeitenverfahren ist weiterhin sehr komplex. Die Verfahren beinhalten oftmals eine Vielzahl von Verstößen, was zu einem erhöhten Bearbeitungsaufwand führt. Zudem sind in dem Berichtszeitraum vermehrt Rechtsmittel gegen erlassene

Berichtszeitraum		01.01. – 31.12.2024
anhängig gesamt		**69**
davon	Verfahren aus vorherigem Berichtszeitraum	26
	neu eingegangene Verfahren	43
abgeschlossen		**50**
davon	mit Bußgeld	11
	mit Verwarnungsgeld	0
	mit Verwarnung ohne Verwarnungsgeld	20
	eingestellt/von Verfolgung abgesehen	18
	an zuständige Behörde abgegeben	1
noch in Bearbeitung		**19**
Summe festgesetzter Buß- und Verwarnungsgelder in Euro		**14.580**

Tabelle 6:
Ordnungswidrigkeiten-verfahren im öffentlichen Bereich

Bescheide eingelegt worden. Der Bearbeitungsaufwand dieser Fälle ist ebenfalls häufig sehr hoch und die Verfahrensdauer bei einer Beteiligung der Gerichte oft sehr lang.

Der Anteil von Ordnungswidrigkeitenverfahren, in denen Bedienstete der sächsischen Polizei in Verdacht standen/stehen, unbefugt dienstlich erlangte personenbezogenen Daten verarbeitet zu haben (ordnungswidrig gemäß § 48 Abs. 1 Nr. 1 SächsDSUG), ist von 80 Prozent im vorherigen Berichtszeitraum auf nunmehr 85 Prozent gestiegen. In den verbleibenden Verfahren bestand/besteht gegen Bedienstete unterschiedlichster sächsischer (Sozial-)Behörden der Verdacht, nicht offenkundige personenbezogene Daten unbefugt verarbeitet zu haben. Die beständig große Anzahl an Ordnungswidrigkeitenverfahren gegen sächsische Polizeibedienstete resultiert dabei einerseits aus dem anhaltenden, überdurchschnittlichen Anzeigeverhalten der Polizeidienststellen, welche datenschutzrechtliche Verstöße – auch dienstrechtlich – weiterhin konsequent verfolgen, deutet aber auch darauf hin, dass trotz einer intensiven Belehrung der Polizeidienststellen über den

Datenschutz nach wie vor Unklarheiten und Schwierigkeiten im Zusammenhang mit der Nutzung von dienstlich zur Verfügung stehenden Daten bestehen.

Auch in diesem Berichtszeitraum handelte es sich bei den Ordnungswidrigkeitenverfahren gegen sächsische Polizeibedienstete regelmäßig um privat motivierte Datenabrufe aus den polizeilichen Auskunfts- bzw. Informationssystemen zu Freunden/Freundinnen, Kollegen/Kolleginnen, Nachbarn/Nachbarinnen oder anderen Bekannten und/oder Datenübermittlungen an Dritte. Auch Recherchen zur eigenen Person, sogenannte „Eigenrecherchen", wurden im Berichtszeitraum wiederholt als Ordnungswidrigkeiten verfolgt. Hintergrund ist der Umstand, dass die/der Bedienstete auch in dieser Konstellation unbefugt nicht offenkundige Daten abruft (auf das Eigeninteresse oder eine Art „naturgemäße" Einwilligung kommt es nicht an, vgl. OLG Bamberg, Beschluss vom 27.04.2010, Az. 2 Ss 531/10) und sich in den zum Vorgang gespeicherten Unterlagen in aller Regel Daten zu Dritten finden (Anzeigeerstattende, Verdächtige, Geschädigte, Zeugen/Zeuginnen etc.). Persönliche Neugier bzw. eine private Motivation ersetzen in keinem Fall die zum Verarbeiten und/oder Abrufen nicht offenkundiger personenbezogener Daten erforderliche dienstliche Befugnis und Notwendigkeit.

Einen Fall, der im Berichtszeitraum herausragte, stelle ich nachfolgend vor:

Zahlreiche Datenabfragen eines Polizeibediensteten trotz Dienstabwesenheit

Im Jahr 2023 erreichte mich die Ordnungswidrigkeitenanzeige einer Polizeidienststelle. Der Anzeige lagen eine Reihe von Datenabfragen eines Polizeibediensteten in den polizeilichen Informationssystemen zugrunde, welche dieser über mehrere Monate hinweg ohne einen für die Dienststelle erkennbaren dienstlichen Anlass tätigte. Besonders auffällig war, dass sich der Bedienstete in dem Zeitraum, in welchem er die Abfragen durchführte, krankheitsbedingt nicht im Dienst befand. Für die Datenrecherchen in den polizeilichen Datenbanken nutzte der Beamte seinen Arbeitsplatz-Com-

puter in seinem Büro, welches dieser während der Zeit seiner Dienstabwesenheit mehrfach aufgesucht hatte. Weiterhin stach heraus, dass der Beamte Daten zu sich selbst, zu Personen aus seinem familiären Kreis sowie zu Personen aus seinem persönlichen Wohnumfeld recherchierte.

Der Verteidiger des Betroffenen äußerte sich hierzu und gab an, die Datenrecherchen seien im Rahmen von Vorermittlungen des Beamten geschehen. Seine Ermittlungen hätten sich gegen einen gewaltbereiten Personenkreis aus der Fanszene eines Fußballclubs gerichtet, welcher systematische Sachbeschädigung begehe, ansässige Bewohnerinnen und Bewohner bedrohe und sich kontinuierlich an der Schwelle zum Landfriedensbruch bewege. Die Datenrecherchen hätten der Einschätzung und Abwehr von Gefahren für die öffentliche Sicherheit und Ordnung gedient und wären damit dienstlich veranlasst gewesen.

Der betreffende Polizeibedienstete war für derartige Ermittlungen weder örtlich noch sachlich zuständig, da bestehende polizeiliche Sachverhalte zu den recherchierten Personen dem örtlichen Zuständigkeitskreis eines anderen Polizeireviers angehörten. Auch wenn sich für Polizeibedienstete aus deren Beruf eine gewisse Garantenstellung hinsichtlich der öffentlichen Sicherheit und Ordnung und Rechtsgüter der Allgemeinheit herleitet und Polizeibedienstete auch von sich aus tätig werden können, haben sie sich dabei innerhalb ihrer konkreten Aufgabenzuweisung zu bewegen. Dies heißt, der einzelne Beamte oder die Beamtin muss grundsätzlich nach seiner oder ihrer konkreten Dienstpflicht örtlich und sachlich für das geschützte Rechtsgut verantwortlich sein.

Aktenkundige Vermerke zu seinen Vorermittlungen fertigte der betreffende Polizeibedienstete nicht an. Im Rahmen der Ermittlungen wurde zudem festgestellt, dass der Bedienstete zu keinem Zeitpunkt Informationen im Zusammenhang mit der Fanszene an das zuständige Polizeirevier weitergegeben hatte und auch keine strafrechtlich relevanten Sachverhalte zur Anzeige gebracht hatte. Es schien mehr als unglaubwürdig, dass der Bedienstete den Einlassungen seines Verteidigers zufolge während seiner krankheitsbedingten

Was ist zu tun?
Bereits durch bloße Unkorrektheiten im Umgang mit personenbezogenen Daten durch öffentliche Stellen kann das Vertrauen der Allgemeinheit in die Zuverlässigkeit der Behörden empfindlich geschädigt werden. Um die Bediensteten der öffentlichen Stellen in Sachsen auch zukünftig zu ihrer besonderen Pflichtenwahrung sowie Vorbildwirkung zu ermahnen, bedarf es weiterhin einer konsequenten Ahndung von Ordnungswidrigkeiten im öffentlichen Bereich.

Dienstabwesenheit über Monate zu einer gewaltbereiten Personengruppe, welche die öffentliche Sicherheit bedrohe, ermittelt und anschließend jedoch keinerlei Informationen oder Erkenntnisse aus diesen Ermittlungen an das zuständige Polizeirevier weitergegeben oder sonstige dienstliche Maßnahmen veranlasst haben soll. Vielmehr war davon auszugehen, dass der Bedienstete die Recherchen aus einer rein privaten Motivation heraus tätigte. Die Einlassungen des Verteidigers wurden in der Folge als Schutzbehauptung gewertet, und es wurde ein Bußgeldbescheid wegen 15 unerlaubter Datenabrufe in den polizeilichen Auskunftssystemen gegen den Bediensteten erlassen. Im Berichtszeitraum befasste sich das zuständige Gericht mit dem Fall, nachdem der Bedienstete Einspruch gegen den Bescheid eingelegt hatte. Das zuständige Amtsgericht sah den Tatbestand ebenfalls für erwiesen an und bestätigte den Bußgeldbescheid.

6.4.2 Ordnungswidrigkeitenverfahren im nichtöffentlichen Bereich

↗ §§ 14, 30, 66, 130 OWiG; Art. 58 Abs. 2 Buchst. b DSGVO; Art. 83 DSGVO

Im Berichtszeitraum hatte ich 83 neue Ordnungswidrigkeitenanzeigen zu verzeichnen – die Anzahl bewegte sich damit etwas unterhalb des Niveaus des Vorjahres (92). Mehr als zwei Drittel der Anzeigen (58) bezogen sich dabei auf die Anfertigung von Videoaufnahmen (stationäre Kameras: 47, Dashcams: 11). Damit liegt der Schwerpunkt (70 Prozent) der bei mir eingegangenen Ordnungswidrigkeitenanzeigen auch weiterhin klar bei der Videoüberwachung (Vorjahr: 66 Prozent).

Insgesamt waren damit im Berichtszeitraum 176 Ordnungswidrigkeitenverfahren bei mir anhängig. Von diesen konnte ich 80 Fälle abschließen und habe dabei in 18 Verfahren 19 Bußgelder festgesetzt.

Gegen Privatpersonen habe ich insgesamt 14 Bußgelder festgesetzt. 12 Bußgelder betrafen den rechtswidrigen Einsatz von Dashcams durch Fahrzeugführer; in zwei Fällen habe ich

Berichtszeitraum		01.01. – 31.12.2024
anhängig gesamt		**176**
davon	Verfahren aus vorherigem Berichtszeitraum	93
	neu eingegangene Verfahren	83
abgeschlossen		**80**
davon	mit Bußgeld	18
	eingestellt/von Verfolgung abgesehen	55
	an zuständige Behörde abgegeben	7
noch in Bearbeitung		**96**
Summe festgesetzte Bußgelder in Euro		**199.000**

Tabelle 7:
Ordnungswidrigkeitenverfahren im nichtöffentlichen Bereich

den unrechtmäßigen Einsatz von Videokameras durch Mieter in Mehrfamilienhäusern (Etagenflur/Außenbereich einschließlich öffentlicher Verkehrsraum) geahndet. Die Höhe der Bußgelder bewegte sich zwischen 100 und 1.000 Euro.

Im Berichtszeitraum habe ich erstmals auch gegen juristische Personen Bußgeldverfahren geführt. Nachdem nach Inkrafttreten der Datenschutz-Grundverordnung (DSGVO) lange Zeit strittig war, ob und unter welchen Voraussetzungen direkt gegen juristische Personen Bußgelder festgesetzt werden können, hat der Europäische Gerichtshof hier mit seinem Urteil vom 5. Dezember 2023 (C-807/21, juris) nun Klarheit geschaffen: Die in Art. 83 DSGVO vorgesehenen Geldbußen können unmittelbar gegen juristische Personen verhängt werden, wenn diese als für die Datenverarbeitung Verantwortliche einzustufen sind. Eine solche Verbandshaftung erfordert weder das Verschulden einer Leitungsperson des Unternehmens (§ 30 Gesetz über Ordnungswidrigkeiten [OWiG]) noch eine Aufsichtspflichtverletzung (§ 130 OWiG). Vielmehr sind Unternehmen im Deliktsbereich der Datenschutz-Grundverordnung aus sich heraus schuldfähig. Die vom Europäischen Gerichtshof für den Bereich der Datenschutz-Grundverordnung entwickelten sachlich-rechtlichen

Grundzüge der Verbandsgeldbuße gestalten auch das diesbezügliche nationale Verfahrensrecht (hier § 66 OWiG). Der Bußgeldbescheid muss daher die natürliche Person, der eine Pflichtverletzung gegebenenfalls zur Last fällt, nicht bezeichnen.

Wegen gravierender Verstöße gegen die Kooperationspflicht (Art. 31 DSGVO) habe ich so gegen zwei Unternehmen Bußgeldbescheide in Höhe von 120.000 Euro und 22.080 Euro erlassen. Beide Unternehmen hatten über lange Zeit aufsichtsbehördliche Aufforderungen zur Auskunftserteilung und zur Unterlagenvorlage ignoriert und sich dabei auch nicht durch den Einsatz von Zwangsmitteln beeindrucken lassen. Im dem einen Fall sind die geforderten Auskünfte erst nach über zwei Jahren und vier Monaten und insgesamt fünf Zwangsgeldern (vier davon bezahlt) erteilt worden; in dem anderen Fall war das Unternehmen erst nach mehr als einem Jahr und vier Zwangsgeldfestsetzungen (drei davon bezahlt) bereit, mit der Aufsichtsbehörde zu kooperieren.

Die verbleibenden beiden Bußgeldfestsetzungen, 30.000 Euro und 20.000 Euro, betrafen unrechtmäßige Videoüberwachungen durch Unternehmen. Ein Unternehmen der Hotel- und Gaststättenbranche hatte mit zwei Außenkameras öffentliche Verkehrsflächen, eine angrenzende (eigene) Baustelle, einen den eigenen Gästen vorbehaltenen Parkplatz sowie Nachbargrundstücke permanent überwacht, wobei in den Kameras auch die Mikrofone aktiviert waren. Ein anderes Unternehmen hatte auf einer eigenen Baustelle eine Videokamera installiert und betrieben. Maßgeblich für die Ahndung mit einem Bußgeld war hier, dass die – dem Diebstahlschutz der Baustelle dienende – Kamera auch während der laufenden Bauarbeiten, das heißt, tagsüber aktiv war. Die von der Geschäftsführung vorgelegten Einwilligungserklärungen der betroffenen Mitarbeiter waren als unwirksam zu betrachten, da Einwilligungen im Arbeitsverhältnis wegen des bestehenden Abhängigkeitsverhältnisses nur dann als Rechtsgrundlage herangezogen werden können, wenn es sich um arbeitnehmernützige Verarbeitungen handelt, der Arbeitnehmer davon also einen Vorteil hat. Bei Überwachungsmaßnahmen ist das

aber grundsätzlich nicht der Fall. In dem konkreten Fall ist auch gegen den auf betreffendem Grundstück wohnenden Bauherrn als Beteiligtem (§ 14 OWiG) ein Bußgeld festgesetzt worden, da er die Installation der Kamera maßgeblich unterstützt und mitgetragen hatte.

Was ist zu beachten?
Gegen juristische Personen können unmittelbar Bußgelder festgesetzt werden, ohne dass es hierzu einer Feststellung bedarf, wer im Unternehmen eine Pflichtverletzung begangen hat.

Neben den oben genannten Bußgeldern habe ich in 18 Fällen noch datenschutzrechtliche Verwarnungen ausgesprochen (vgl. Art. 58 Abs. 2 Buchst. b DSGVO).

6.5 Öffentlichkeitsarbeit

6.5.1 Onlinekommunikation und Publikationen

Informationsangebot erweitert

Auf meiner Website datenschutz.sachsen.de ist das Informationsangebot nach Zielgruppen unterteilt. Es enthält Ausführungen zu rechtlichen Grundlagen sowie themenspezifische Inhalte, die fortwährend aktualisiert und anlassbezogen erweitert werden. So ging der Berichtszeitraum mit dem Superwahljahr in Sachsen einher: Am 9. Juni 2024 fand die Wahl zum Europäischen Parlament statt, parallel dazu die Kommunalwahlen. Wenige Monate danach – am 1. September 2024 – folgte die Wahl zum Sächsischen Landtag. Bereits bei der Vorbereitung, aber auch bei der Durchführung der Abstimmungen wurden enorme Mengen personenbezogener Daten verarbeitet – von Wahlberechtigten, Kandidatinnen und Kandidaten sowie Wahlhelferinnen und Wahlhelfern. Daher verwundert es nicht, dass sich betroffene Personen bei solchen Ereignissen üblicherweise auch an meine Behörde wenden. Eine Vielzahl an Fragen hatte ich deshalb proaktiv vor den Wahlen auf meiner Website beantwortet.

FAQ zum Datenschutz bei Wahlen:
↗ datenschutz.sachsen.de/wahlen.html

Weiterhin kontaktieren mich Behörden regelmäßig zum Auskunftsrecht der Datenschutz-Grundverordnung (DSGVO). Weil bei diesem Thema oftmals Unsicherheiten und Unklarheiten vorhanden sind, habe ich einen neuen Leitfaden

Handlungsleitfaden für Kommunen und Verwaltungen zur Auskunftserteilung nach Art. 15 DSGVO:
↗ sdb.de/tb2403

erarbeitet (siehe 3.2.2). Die Handreichung richtet sich an sächsische öffentliche Stellen, die Verantwortliche im Anwendungsbereich der Datenschutz-Grundverordnung sind und betroffenen Personen Auskunft nach Artikel 15 DSGVO erteilen müssen.

Lange Zeit nutzten vor allem Behörden und Unternehmen Videoüberwachung für sicherheitsrelevante Bereiche – auch weil die Technik verhältnismäßig teuer war. Inzwischen ist Überwachungstechnik jedoch günstig, und man kann aus einer unüberschaubaren Anzahl unterschiedlicher Produkte wählen. Mit der wachsenden Verbreitung von Kameras gingen auch mehr Beschwerden dazu in meiner Behörde ein. Dass nur im Durchschnitt etwa jede dritte Videoüberwachung datenschutzrechtlich in Ordnung ist, verdeutlicht die Unwissenheit bei vielen Verantwortlichen.

Deshalb habe ich mit meiner Behörde die Broschüre „Achtung Kamera!" erarbeitet und herausgegeben. Der Ratgeber für Verantwortliche und Betroffene war Anfang 2024 erschienen und umfasste in der 1. Auflage 1.000 Exemplare. Ein knappes halbes Jahr später waren diese bereits vergriffen. Die große Nachfrage sowie die hohen Fallzahlen sprachen klar für eine zweite Auflage. Sie erschien Mitte 2024. In ihr ist auch die Entscheidung des Sächsischen Verfassungsgerichtshofs von Ende Januar berücksichtigt.

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

In „Achtung Kamera!" sind die rechtlichen Anforderungen und Grenzen der Videoüberwachung aufgeführt – sowohl für nichtöffentliche Stellen, wie Privatpersonen und Unternehmen, als auch für öffentliche Stellen, insbesondere für Kommunen und die sächsische Polizei. Auf über 110 Seiten werden zudem die häufigsten Verarbeitungssituationen besprochen, unter anderem die Videoüberwachung von Beschäftigten, in der Nachbarschaft, in Kleingärten, auf Baustellen, in der Gastronomie, im Handel, in Freizeiteinrichtungen, in medizinischen Einrichtungen, im ÖPNV, in Autos, mit Drohnen etc.

Immer wieder werden Fälle bekannt, in denen Dritte geschwärzte Daten aus Dokumenten und Dateien wiederherstellen konnten. Dadurch können die Persönlichkeitsrechte der

Betroffenen verletzt werden. Zudem ist der Verantwortliche in der Pflicht – sofern schützenswerte personenbezogene Daten offenbart werden –, die Datenpanne gemäß Art. 33 DSGVO der zuständigen Aufsichtsbehörde zu melden. Damit es gar nicht erst zu Verstößen kommt, sollten Beschäftigte, die mit Schwärzungen und der Veröffentlichung von Dokumenten betraut sind, über mögliche Fehlerquellen und Lösungen Bescheid wissen. In einem Artikel auf meiner Website gebe ich Hinweise, beispielsweise, was im Umgang mit PDF-, Office- und Bilddateien zu beachten ist (vgl. auch 4.1.4).

Datenschutzkonformes Schwärzen: Darauf sollten Sie achten!:
↗ sdb.de/tb2405

Betrieb der Mastodon-Instanz social.sachsen.de

Meine Behörde betreibt seit über einem Jahr einen eigenen Mastodon-Server unter social.sachsen.de. Mastodon ist eine datensparsame Alternative zu Facebook und X. Auch öffentliche Stellen aus Sachsen können auf meiner Instanz einen Account für ihre Öffentlichkeitsarbeit erhalten. Dazu genügt eine E-Mail an socialmedia@sdtb.sachsen.de.

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 zudem die Möglichkeit, den „News-Feed" eines (Behörden-)Profils beispielsweise auf der jeweiligen (Behörden-)Website einzubinden, 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 social.sachsen.de/@sdtb.rss für mein Profil.

Wer sich privat einen Mastodon-Account einrichten und darüber kommunizieren möchte, findet beispielsweise auf 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.

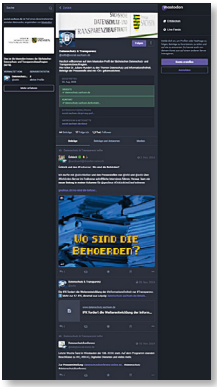


Abbildung 6:
Profil der SDTB auf Mastodon

Was ist zu tun?
Angesichts der Tatsache, dass die Nutzung vieler kommerzieller Social-Media-Plattformen datenschutzrechtlich problematisch ist, sollten öffentliche Stellen damit beginnen, datenschutzfreundliche und rechtskonforme Lösungen zu nutzen.

6.5.2 Presse- und Medienarbeit

Die Kommunikation mit Medienvertreterinnen und Medienvertretern ist ein wichtiger Bestandteil der Öffentlichkeitsarbeit meiner Behörde. Je nach Publikation erreiche ich damit sowohl Bürgerinnen und Bürger als auch Fachpublikum, insbesondere betriebliche und behördliche Datenschutzbeauftragte.

Die meisten Anfragen richteten Journalistinnen und Journalisten aus dem Bereich der Print- und Onlinemedien an mich. Wie im Vorjahr erhielt ich am häufigsten Fragen zur Videoüberwachung, beispielsweise von Bahnhöfen, Ferienwohnungen, Parkplätzen, Turnhallen und Geschäften. Etliche Medien haben zudem die Veröffentlichungen der 1. und der 2. Auflage der Broschüre „Achtung Kamera!" zum Anlass genommen, über Videografie in Sachsen zu berichten. Darüber hinaus kontaktierten mich Redakteurinnen und Redakteure verstärkt zum Einsatz des videogestützten Personen-Identifikations-Systems (PerIS, siehe 1.1) durch die Polizei. Außerdem erkundigten sich Medienvertreter/innen bei mir unter anderem zum Datenschutz bei der elektronischen Patientenakte, zur Speicherung personenbezogener Daten beim Verfassungsschutz, zu Datenpannen bei sächsischen Kommunen, über die Rechtmäßigkeit von KI-Anwendungen sowie zu vielen weiteren Themen.

Verhältnismäßig wenige Anfragen betrafen mein Amt als Transparenzbeauftragte sowie meinen Vorsitz bei der Konferenz der Informationsfreiheitsbeauftragten in Deutschland (IFK), den ich 2024 innehatte.

Außerdem veröffentlichte ich eine Reihe von Pressemitteilungen, beispielsweise zum Datenschutz bei Wahlen und zu den Ergebnissen der Prüfung von 30.000 sächsischen Websites auf mögliche Datenschutzverstöße (siehe 1.4 und 1.5).

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

6.5.3 Fortbildungen, Infoveranstaltungen und fachlicher Austausch

Reges Interesse am Datenschutz verzeichnete ich auch 2024 auf verschiedenen Veranstaltungen. So war ich unter anderem an der Evangelischen Hochschule Dresden zu Gast. Dort vermittelte ich den Studierenden in einem Vortrag die Grundzüge des Datenschutzrechts. Außerdem nahm ich wieder am „Tag der offenen Tür des Sächsischen Landtags" teil. An meinem Stand informierten sich Besucherinnen und Besucher sowohl über den rechtskonformen Umgang mit personenbezogenen Daten als auch über die Möglichkeiten, wie sie mithilfe des Transparenzgesetzes amtliche Informationen erhalten können. Beides war auch Thema beim E-Learning-Kurs „Wer sieht mich?", der unter anderem von der Sächsischen Landeszentrale für politische Bildung organisiert wurde. Die Veranstaltung unterstützte ich wie im Vorjahr mit einem Vortrag. Gerne folgte ich auch den Einladungen einer kirchlichen Initiative und eines Wirtschaftsverbandes. Von Gesetzes wegen bin ich (beratendes) Mitglied im IT-Kooperationsrat, im Landespräventionsrat und im statistischen Beirat. Auch diese Sitzungen nutzte ich für den fachlichen Austausch.

Fortbildung von Beschäftigten

Die Mitarbeiterinnen und Mitarbeiter nahmen vor dem Hintergrund der behördeninternen Entwicklung verstärkt an Fortbildungen zur elektronischen Akten- und Vorgangsbearbeitung teil. Insgesamt standen im Berichtsjahr die besuchten Fortbildungsmaßnahmen, im Gleichklang mit dem allgemeinen Aufgabenwandel, im Fokus von Digitalisierung, KI und Internetrecht.

Mehr Schulungen

Auch im aktuellen Berichtszeitraum waren Mitarbeiterinnen und Mitarbeiter meiner Dienststelle, trotz des steigenden Arbeitsaufkommens, im Sinne der Prävention vielfältig im Bereich der Beratung bzw. Aus- und Fortbildung unter-

Abbildung 7:
Tag der offenen Tür des Sächsischen Landtags am 3. Oktober 2024

Abbildung 8:
Podiumsgespräch zum Thema „Soziale Medien und Datenschutz – Wie geht das zusammen?" beim DatenTag der Stiftung Datenschutz am 19.09.2024 in Berlin

wegs und hielten 18 Fortbildungsseminare. 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 sowohl in Präsenzform als auch online oder hybrid statt.

Ausbildung von Rechtsreferendarinnen und Rechtsreferendaren

Im Jahr 2024 waren mir ferner zwei Rechtsreferendare zur Ausbildung zugewiesen. Der Austausch mit jungen Menschen im Bereich des Datenschutzes ist für mich eine enorme Bereicherung. Die zugewiesenen Aufgaben ermöglichten den Juristen einen breiten Einblick in meine Arbeit.

7 Zusammenarbeit der Datenschutzaufsichtsbehörden, Datenschutzkonferenz

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

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. Im Berichtszeitraum hatte zunächst das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein den Vorsitz inne, ab Mitte Mai 2024 übernahm diese Aufgabe der Hessische Beauftragte für Datenschutz und Informationsfreiheit.

Abbildung 9:
108. Konferenz der DSK am 14. und 15. November 2024 in Wiesbaden

7.1 Materialien der Datenschutzkonferenz – Entschließungen

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

- Menschenzentrierte Digitalisierung in der Daseinsvorsorge sicherstellen! (19.12.2024)
- Vorsicht bei dem Einsatz von Gesichtserkennungssystemen durch Sicherheitsbehörden (20.09.2024)
- Recht auf kostenlose Erstkopie der Patientenakte kann durch eine nationale Regelung nicht eingeschränkt werden! Datenschutzaufsichtsbehörden sehen konkreten Handlungsbedarf aufseiten der Heilberufskammern (11.09.2024)
- Besserer Schutz von Patientendaten bei Schließung von Krankenhäusern (15.05.2024)

7.2 Materialien der Datenschutzkonferenz – Beschlüsse

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

- Übermittlungen personenbezogener Daten an die Erwerberin oder den Erwerber eines Unternehmens im Rahmen eines Asset-Deals (11.09.2024)
- DSGVO privilegiert wissenschaftliche Forschung (11.09.2024)
- Datenschutzrechtliche Grenzen des Einsatzes von Bezahlkarten zur Leistungsgewährung nach dem Asylbewerberleistungsgesetz (AsylbLG) (19.08.2024)
- Anforderungen an die Sekundärnutzung von genetischen Daten zu Forschungszwecken (15.05.2024)
- Nationale Zuständigkeiten für die Verordnung zur Künstlichen Intelligenz (03.05.2024)

7.3 Materialien der Datenschutzkonferenz – Orientierungshilfen

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

- Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von digitalen Diensten (OH Digitale Dienste) (November 2024)
- Orientierungshilfe der DSK zu ausgewählte Fragestellungen des neuen Onlinezugangsgesetzes (November 2024)
- Datenverarbeitung im Zusammenhang mit funkbasierten Zählern (16.08.2024)
- Orientierungshilfe der DSK zu Künstlicher Intelligenz und Datenschutz (06.05.2024)
- Orientierungshilfe der Aufsichtsbehörden zur Einholung von Selbstauskünften bei Mietinteressent:innen Version 1.0 (24.01.2024)

7.4 Materialien der Datenschutzkonferenz – Anwendungshinweise

Anwendungshinweise sollen beim praktischen Vollzug der Datenschutz-Grundverordnung unterstützen.

- Standard-Datenschutzmodell (SDM) Version 3.1

7.5 Materialien der Datenschutzkonferenz – Stellungnahmen

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

- Stellungnahme der DSK zum Gesetzesentwurf der Bundesregierung: Entwurf eines Ersten Gesetzes zur Änderung des Bundesdatenschutzgesetzes (12.04.2024)

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.

- Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive (07.10.2024) – nur in Englisch
- EU-US Data Privacy Framework FAQ for European individuals (16.07.2024) – nur in Englisch
- EU-US Data Privacy Framework FAQ for European businesses (16.07.2024) – nur in Englisch
- Guidelines 01/2023 on Article 37 Law Enforcement Directive (19.06.2024) – nur in Englisch
- Template Complaint Form to the U.S. Office of the Director of National Intelligence's Civil Liberties Protection Officer (CLPO) (24.04.2024) – nur in Englisch
- Rules of Procedure on the Data Protection Framework redress mechanism for national security purposes (24.04.2024) – nur in Englisch
- Rules of Procedure for the "Informal Panel of EU DPAs" according to the EU-US Data Privacy Framework (24.04.2024) – nur in Englisch
- Information Note on the Data Protection Framework redress mechanism for national security purposes (24.04.2024) – nur in Englisch
- EU-US Data Privacy Framework Template Complaint Form for Submitting Commercial Related Complaints to EU DPAs (24.04.2024) – nur in Englisch

7.7 Anfrage an die irische Aufsichtsbehörde wegen des Verbots einer Facebook-Fanpage der sächsischen Staatskanzlei

↗ Art. 56, Art. 58 Abs. 2 f, Art. 60 DSGVO

Tätigkeitsbericht Datenschutz 2023:
↗ sdb.de/tb2023

Mit Bescheid vom 5. Juli 2023 untersagte ich der Sächsischen Staatskanzlei die Nutzung der Facebook-Fanpage. Nicht nur die Sächsische Staatskanzlei ging dagegen gerichtlich vor, sondern auch Meta erhob dagegen Drittanfechtungsklage (vgl. Tätigkeitsbericht 2023, 1.2). Unter anderem behauptete sie darin auch, dass nicht ich, sondern die irische Aufsichtsbehörde DPC (Data Protection Commission) für dieses Verfahren federführend zuständig sei, da Meta allein für die Datenverarbeitung durch die Fanpage verantwortlich sei, und beantragte aus diesem Grund die Aufhebung der Einstellungsanordnung. Ich halte diese Auffassung für unzutreffend und habe die irische Aufsichtsbehörde daher lediglich von dem Verfahren informiert.

Dies tat ich mithilfe eines Verfahrens der freiwilligen Amtshilfe nach Art. 61 DSGVO im Internal Market Information System (IMI, vgl. auch 6.2.7). Sowohl die übrigen europäischen Aufsichtsbehörden als auch die irische Aufsichtsbehörde wurden von den wesentlichen Verfahrensgegenständen informiert. Zum einen wurde die oben genannte Untersagungsanordnung in einer inoffiziellen Übersetzung zur Kenntnis eingestellt. Zum anderen wurde, da die Klageschrift von Meta mit über 80 Seiten zu umfangreich war, um sie im Hause zu übersetzen, eine Zusammenfassung der wichtigsten Argumente von Meta eingestellt. Bei dieser Gelegenheit wurde nicht nur die DPC, sondern auch die übrigen europäischen Aufsichtsbehörden um Auskunft gebeten, ob ihnen Klagen von Meta gegen solche Anordnungen von Aufsichtsbehörden gegen Facebook-Fanpages von privaten oder öffentlichen Stellen bekannt seien. Da die deutschen Aufsichtsbehörden über die Datenschutzkonferenz sich über das Verfahren austauschen konnten, richtete sich die Anfrage

ausdrücklich nicht an diese. Nach Aktivierung des Verfahrens im IMI am 18. Oktober 2024 bis zum Abschluss des Verfahrens am 28. November 2024 erhielt ich sechs Antworten von anderen europäischen Aufsichtsbehörden. Keine führte ein solches Verfahren, in dem Meta Drittwiderspruchsklage erhoben hat. Allerdings teilte eine Aufsichtsbehörde mit, dass sich Meta in einem Verfahren zur Datenschutzfolgenabschätzung einer Regierungs-Fanpage dieses Landes mit ähnlichen Argumenten gemeldet habe, da die Behörde sieben hohe und ein geringes Risiko für den Datenschutz bei deren Betrieb gefunden hatte. Deren Bericht war freundlicherweise im IMI hochgeladen worden.

7.8 Amtshilfeverfahren nach Artikel 61 DSGVO bei Videoüberwachung eines Hauses in den sächsischen Wäldern

↗ Art. 61 DSGVO

In einem Fall wegen der Videoüberwachung eines bewohnten Grundstücks durch auf dem Nachbargrundstück angebrachte Videokameras konnte ich Datenschutzverletzungen durch die auf die Grundstückseinfahrt und den Komposthaufen der Nachbarn gerichtete Wildkameras trotz intensiver Ermittlungen nicht ahnden, weil die Inhaber in einem anderen europäischen Land residierten, ohne über eine zustellungsfähige Anschrift in Sachsen oder der restlichen Bundesrepublik zu verfügen. Ein One-Stop-Shop-Verfahren, bei dem eine federführende Aufsichtsbehörde im Verbund mit betroffenen Aufsichtsbehörden den Fall bearbeitet hätte, kam hier mangels grenzüberschreitender Datenverarbeitung nach Art. 56 Abs. 1, 4 Nr. 2 DSGVO nicht infrage.

Glücklicherweise eröffneten Leitlinien des EDSA[1] den Weg zu einem Verfahren der freiwilligen Amtshilfe durch eine andere europäische Aufsichtsbehörde in nicht grenzüberschreitenden Verfahren, bei denen (vermutlich) die Verarbeitung der Daten in deren Zuständigkeitsbereich erfolgt. Das Ferienhaus auf dem überwachenden Grundstück wurde zwar nur einen Teil des Jahres genutzt, die Kameras waren aber immer betriebsbereit, und ihre Bilder wurden deshalb offensichtlich am Wohnsitz der Eigentümer verarbeitet. Entsprechend dem in der Leitlinie geschilderten Verfahren zeigte sich die andere Behörde bei einem ersten formlosen Kontakt außerhalb des Internal Market Information System (IMI, vgl. auch 6.2.7) kooperativ, wünschte aber, dass ich die Verantwortlichen kontaktierte, um zu erfahren, ob die Bilder der Kameras an deren europäischem Wohnsitz verarbeitet würden. Dies tat ich, wenn auch leider vergeblich. Davon informierte ich die andere europäische Aufsichtsbehörde durch Aktivierung einer Anfrage im IMI. Rasch erklärte sich diese zur Untersuchung des Falls bereit.

[1] „Internal EDPB Document 1/2019 on handling cases with only local impacts under Article 56.2 GDPR, Version 2.0 vom 14.05.2019", S. 5, Rn. 10 und internes EDSA-Dokument 06/2020 („Internal EDPB Document 6/2020 on preliminary steps to handle a complaint: admissibility and vetting of complaints" vom 15.12.2020, Rn. 27.

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

↗ Art. 57 Abs. 1 u DSGVO, Art. 59 Satz 1 DSGVO

noyb, „GDPR-a culture of non-compliance" (2024):
↗ sdb.de/tb2407

Die von Max Schrems gegründete gemeinnützige Organisation noyb hat in einem Bericht, welcher auf Umfragen bei Verantwortlichen beruht, festgestellt, dass Datenschutzbeauftragte in Unternehmen sich mehr Bußgeldentscheidungen oder Abhilfeanordnungen von Datenschutzbehörden wünschen. Nationale und europäische Aufsichtsbehörden beklagen sich über mangelnde personelle Ausstattung (siehe sdb.de/tb2408). Aussagekräftige jährliche Statistiken über die Rahmenbedingungen und Aktivitäten der europäischen einschließlich der deutschen Aufsichtsbehörden könnten einen Zusammenhang zwischen der Durchsetzung der Datenschutz-Grundverordnung (DSGVO) und der personellen Ausstattung der Behörden verdeutlichen.

Die DSGVO selbst verpflichtet die Aufsichtsbehörden aber nur dazu, interne Verzeichnisse über Verstöße gegen die DSGVO und dagegen ergriffene Maßnahmen zu führen (Art. 58 Abs. 1 Buchst. u DSGVO). Auch sollen Tätigkeitsberichte veröffentlicht werden, in denen eine solche Liste enthalten ist (Art. 59 Satz 1 DSGVO). Da im europäischen Kontext einheitliche Definitionen der geforderten statistischen Angaben eine Voraussetzung für vergleichbare Zahlen sind, wurde ein „Drafting Team" von einer Expertengruppe des Europäischen Datenschutzausschusses (EDSA) eingerichtet, an welcher auch eine Vertreterin meiner Behörde teilnahm. Anfang November wurde das von diesem Team erarbeitete Papier mit Vorschlägen für statistische Erhebungen vom EDSA einstimmig angenommen. In Deutschland gibt es bei der Datenschutzkonferenz eine Arbeitsgruppe im Arbeitskreis „Organisation & Struktur". Diese Gruppe, in der meine

Behörde ebenfalls vertreten ist, entwickelt für die deutschen Datenschutzaufsichtsbehörden einen statistischen Fragebogen, damit die Arbeit künftig noch transparenter und vergleichbarer wird.

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

8.1 Die polizeiliche Weiterverarbeitung von Daten im Licht aktueller verfassungsgerichtlicher Entscheidungen

↗ §§ 18 Abs. 1 Nr. 2, 77 Abs. 1 BKAG; §§ 79 Abs. 2–5, 80 Abs. 2, 91 Abs. 3 SächsPVDG

Die polizeiliche Speicherpraxis hinsichtlich personenbezogener Daten aus Strafverfahren ist ein Thema, das mich immer wieder beschäftigt und im Austausch mit den Polizeivollzugsdienstbehörden regelmäßig erörtert wird. Regelmäßig erreichen mich Beschwerden von Personen, die die Rechtmäßigkeit der Speicherung sie betreffender Daten in polizeilichen Informationssystemen anzweifeln (vgl. Tätigkeitsbericht 2023, 8.3, Seite 254 ff.). Auch im Berichtszeitraum wandten sich Petenten an mich. Obwohl die Speicherung personenbezogener Daten einen Grundrechtseingriff darstellt und nur auf Grundlage einer gesetzlichen Vorschrift erfolgen darf, deren Voraussetzungen und verfassungskonforme Anwendung im Einzelfall – etwa zur Prüfung geltend gemachter Betroffenenrechte oder zur Durchführung einer datenschutzrechtlichen Prüfung – ohne Weiteres belegbar sein müssen, zieht sich eine nachvollziehbare Beantwortung diesbezüglicher Fragen durch die Polizei teilweise über Monate hin.

Tätigkeitsbericht Datenschutz 2023:
↗ sdb.de/tb2023

Ein Fall offenbarte rechtliche Schwierigkeiten bei der Speicherung in besonderem Maß. Ein junger Mann, der bei einer gefährdeten Großveranstaltung arbeiten wollte und des-

sen Zuverlässigkeit deshalb rechtlich zulässig unter Einbeziehung polizeilicher Erkenntnisse überprüft wurde, erfuhr, dass er aufgrund einer polizeilichen Speicherung als nicht zuverlässig eingeschätzt worden war. Der Eintrag zu seiner Person betraf ein ca. fünf Jahre zurückliegendes Vorkommnis, das zur Einleitung eines Ermittlungsverfahrens gegen ihn geführt hatte. Der Petent war Teilnehmer einer Demonstration gewesen, aus deren Reihen es zu Straftaten gekommen war; zunächst stand der Verdacht eines schweren Landfriedensbruchs im Raum. Die Polizei hat, ohne den Verfahrensausgang zu kennen und obwohl zum Petenten keine einzige anderweitige polizeiliche Erkenntnis vorlag, Daten des Petenten für künftige Zwecke gespeichert und dabei eine Aussonderungsprüffrist von zehn Jahren verfügt; das ist die gesetzliche Höchstfrist für Speicherungen bis zu einer Aussonderungsprüfung. Darüber hinaus wurde dem Petenten auch ein sogenannter ermittlungsunterstützender Hinweis zugeordnet, der die Zugehörigkeit zu bestimmten Tätergruppen oder Deliktsfeldern markiert und für abrufende Bedienstete sofort erkennen lässt; er war als „politisch motivierter Straftäter" gespeichert. Das Ermittlungsverfahren war relativ zügig durch die zuständige Staatsanwaltschaft nach § 170 Abs. 2 Strafprozessordnung (StPO) eingestellt worden, Anklage wurde nicht erhoben. Es lagen zu wenige Anhaltspunkte und erst recht keine Belege dafür vor, dass durch ein Verhalten des Petenten ein Straftatbestand erfüllt worden war. Unter solchen Umständen ist eine Speicherung der Daten über zehn Jahre von keiner Rechtsgrundlage gedeckt. Die Festlegung der Aussonderungsprüffrist von zehn Jahren war ganz offensichtlich ohne Berücksichtigung der Umstände des Einzelfalls erfolgt, denn dies hätte im Rahmen der gebotenen Verhältnismäßigkeitsprüfung eine Festlegung der maximalen Aussonderungsprüffrist verhindert. Im Rahmen der durch einen Antrag des Petenten auf Löschung seiner Daten und meine Kontrolle ausgelösten Prüfung hat die Polizei die Daten gelöscht. Eine polizeiliche Weiterverarbeitung von Daten aus Strafverfahren wie im Beispielfall – hier in Form der Speicherung für künftige Zwecke – war bereits

nach alter bzw. aktueller Rechtslage nicht mit den gesetzlichen und verfassungsgerichtlichen Vorgaben in Einklang zu bringen. Für die Zukunft gilt das aus folgenden Gründen umso mehr.

Ich hatte im Tätigkeitsbericht 2023 zu erwartende verfassungsgerichtliche Entscheidungen unter anderem zu polizeilichen Informationssystemen erwähnt, aufgrund derer eine kritische Überprüfung der schon bislang rechtlich problematischen polizeilichen Speicherpraxis notwendig und eine grundlegende Überarbeitung erforderlich sein würden. Dem Sächsischen Verfassungsgerichtshof (SächsVerfGH) lagen eine ganze Reihe von Vorschriften des Sächsischen Polizeivollzugsdienstgesetzes (SächsPVDG) zur Prüfung vor. Im hier interessierenden Zusammenhang erklärte das Verfassungsgericht des Freistaates in seinem Urteil vom 25. Januar 2024 (Az.: Vf. 91-II-19), dass die zentrale Vorschrift zur polizeilichen Weiterverarbeitung von Daten aus Strafverfahren in § 80 Abs. 2 SächsPVDG nicht mit der Sächsischen Verfassung vereinbar ist, weil sie insoweit nicht bestimmt und erkennen lässt, unter welchen Voraussetzungen Daten aus Strafverfahren über das Ursprungsverfahren hinaus weiterverarbeitet werden dürfen.

Das Bundesverfassungsgericht (BVerfG) hat mit Urteil vom 1. Oktober 2024 (Az.: 1 BvR 1160/19) unter anderem festgestellt, dass § 18 Abs. 1 Nr. 2 Bundeskriminalamtgesetz (BKAG, § 18 Abs. 1 BKAG ist nahezu identisch mit § 80 Abs. 2 SächsPVDG, die Verfassungsbeschwerde vor dem BVerfG war aber nur hinsichtlich der Weiterverarbeitungsvariante bzgl. beschuldigter Personen zulässig und daher nur insoweit inhaltlich zu prüfen) nicht mit dem Grundgesetz vereinbar ist. Es fehlt an einer „hinreichend normierten Speicherungsschwelle", wie das BVerfG formuliert. Zudem fehlen Vorgaben zur Speicherdauer.

In beiden Fällen messen die Verfassungsgerichte die jeweilige Weiterverarbeitungsvorschrift am Grundrecht auf informationelle Selbstbestimmung und kritisieren den Mangel an der gesetzlichen Festlegung der Voraussetzungen bzw. Speicherungsschwelle für eine Weiterverarbeitung der Da-

ten (beschuldigter Personen) aus einem Strafverfahren für künftige polizeiliche Zwecke. Aus den Begründungen der Urteile lassen sich verfassungsrechtliche Vorgaben für die Gestaltung entsprechender Vorschriften durch den Gesetzgeber, aber auch für die Polizei als für die Datenspeicherung verantwortliche Stelle ableiten:

- Die Verwendung von personenbezogenen Daten, insbesondere ihre Speicherung, kann nicht als solche abstrakt gerechtfertigt werden, sondern nur insoweit, als sie hinreichend gewichtigen, konkret benannten Zwecken dient.
- Eine bloße abstrakte Eignung als künftiger Spuren- oder Ermittlungsansatz ist nicht ausreichend.
- Für eine verfassungsrechtliche Rechtfertigung der vorsorgenden Speicherung erforderlich sind jedenfalls die Festlegung angemessener Speicherzwecke und Speicherschwellen sowie die Bestimmung einer angemessenen Speicherdauer.
- Die Speicherschwelle muss den Zusammenhang zwischen den vorsorgend gespeicherten personenbezogenen Daten und der Erfüllung des Speicherzwecks in verhältnismäßiger Weise absichern und den spezifischen Gefahren der vorsorgenden Speicherung angemessen begegnen.
- Bei der Speicherung von Daten für die Verhütung und Verfolgung vom Speicherzweck erfasster Straftaten ist dies bei personenbezogenen Daten nur gegeben, wenn eine hinreichende Wahrscheinlichkeit dafür besteht, dass die Betroffenen eine strafrechtlich relevante Verbindung zu möglichen Straftaten aufweisen werden und gerade die gespeicherten Daten zu deren Verhütung und Verfolgung angemessen beitragen können. Diese Prognosen müssen sich auf zureichende tatsächliche Anhaltspunkte stützen. Als taugliche Prognosekriterien können insbesondere die Art, Schwere und Begehungsweise der vormaligen Tat sowie die Persönlichkeit des Betroffenen und sein bisheriges strafrechtliches Erscheinungsbild infrage kommen.

- Die Dauer der zulässigen Speicherung wird insbesondere geprägt durch das Eingriffsgewicht, die Belastbarkeit der Prognose in der Zeit sowie durch andere sich aus dem Grundsatz der Verhältnismäßigkeit ergebende Gesichtspunkte. Die Prognose verliert über die Zeit ohne Hinzutreten neuer relevanter Umstände grundsätzlich an Überzeugungskraft. Die verfassungsrechtlich gebotene kompensatorische Einhegung einer Befugnis zur vorsorgenden Speicherung gebietet daher ein Regelungskonzept, das entsprechend diesen Gesichtspunkten differenzierte Prüfungs- und Aussonderungsfristen setzt. Auch muss die vorsorgende Speicherung grundsätzlich zeitlich begrenzt sein.

Damit ergibt sich neben der Notwendigkeit einer gesetzgeberischen Überarbeitung von § 80 Abs. 2 SächsPVDG meines Erachtens auch das Erfordernis, § 91 Abs. 3 SächsPVDG an die verfassungsgerichtlichen Vorgaben anzupassen, denn in dieser Vorschrift finden sich – zu vage – Bestimmungen über die sogenannten Aussonderungsprüffristen, das heißt über die in der Praxis erfolgende Speicherdauer. Das BVerfG hat in diesem Zusammenhang § 77 Abs. 1 BKAG, der insoweit der sächsischen Regelung des § 91 Abs. 3 SächsPVDG entspricht, als ungenügend bewertet. Zwar betraf die Prüfung des BVerfG in erster Linie Speicherungen in dem beim Bundeskriminalamt (BKA) koordinierten Informationsverbund der Polizeien des Bundes und der Länder, an dem darüber hinaus auch besondere Strafverfolgungsbehörden beteiligt sind. Die grundsätzlichen Ausführungen des Gerichts zum Eingriffsgewicht von Datenspeicherungen für künftige Zwecke und die daraus abgeleiteten Anforderungen an Regelungen zur Dauer der Speicherung sind aber nach meiner Überzeugung auf Speicherungen, die zunächst „nur" der gesamten Landespolizei zur Verfügung stehen, übertragbar.
Bis zu einer Neuregelung, längstens bis 30. Juni 2026, gilt nach dem Urteil des SächsVerfGH § 80 Abs. 2 SächsPVDG nur nach Maßgabe des § 79 Abs. 2 bis 5 SächsPVDG weiter; die dort formulierten Bestimmungen gelten temporär also

Was ist zu tun?
Polizeiliche Speicherungen für künftige Zwecke sind Grundrechtseingriffe, vor denen die rechtlichen Voraussetzungen genau zu prüfen und die Umstände des Einzelfalls zu berücksichtigen sind. Bislang geltende Vorgaben werden aufgrund verfassungsgerichtlicher Entscheidungen eine gesetzliche Konkretisierung erfahren. Die neuen Regelungen sollten, angemessen umgesetzt, zu einer spürbaren Verbesserung der Qualität der Speicherpraxis führen.

auch für die Weiterverarbeitung von Daten aus Strafverfahren nach § 80 Abs. 2 SächsPVDG.
Meine Dienststelle befindet sich in einem steten Austausch mit dem Staatsministerium des Innern über die Auswirkungen der erwähnten verfassungsgerichtlichen Entscheidungen. Für die Unterstützung bei der Erarbeitung von gesetzlichen Regelungen und untergesetzlichen Vorschriften stehe ich zur Verfügung.

8.2 Datenabfragen im Rahmen der Onlinewache der Polizei Sachsen: Anzeige erstatten!

↗ § 47 Nr. 3 BDSG, § 111 OWiG

Im letzten Berichtszeitraum erhielt ich den Hinweis eines Bürgers, dass im Rahmen der Anzeigenerstattung bei der Onlinewache der Polizei Sachsen personenbezogene Daten als Pflichtangaben erhoben werden, die für die Anzeigenbearbeitung nicht erforderlich seien. Konkret handelt es sich um die Angabe des Geburtslandes sowie die Angabe des Familienstandes.
Ich bat das Landespolizeipräsidium im Staatsministerium des Innern (SMI) um Erläuterung der Rechtsgrundlage und insbesondere der Erforderlichkeit dieser Datenerhebungen für die Anzeigenbearbeitung bzw. das Ermittlungsverfahren. Das SMI teilte mit, dass die Onlineanzeige keine Eigenentwicklung der sächsischen Polizei, sondern ein Verfahren der Länder Saarland und Rheinland-Pfalz sei, welches für Sachsen im Rahmen der Auftragsdatenverarbeitung bereitgestellt werde. Eine Änderung dieses Verfahrens bedürfe daher der Abstimmung mit den beteiligten Ländern. Zudem sei gesetzliche Grundlage für die erhobenen Daten § 111 Gesetz über Ordnungswidrigkeiten (OWiG). Die Angabe des Geburtslandes sei zwar nicht zwingend über § 111 OWiG gedeckt, gleichwohl sei die Abfrage hilfreich, da man ausgehend vom Geburtsort nicht in jedem Fall eindeutig auf das Geburtsland schließen könne. Zur Anga-

be des Familienstandes bestehe gemäß § 111 Abs. 1 OWiG eine gesetzliche Pflicht, und sie sei erforderlich, um zum Beispiel Aussageverweigerungsrechte zu prüfen.

§ 111 Abs. 1 OWiG bestimmt, dass ordnungswidrig handelt, wer einer zuständigen Behörde, einem zuständigen Amtsträger oder einem zuständigen Soldaten der Bundeswehr über seinen Vor-, Familien- oder Geburtsnamen, den Ort oder Tag seiner Geburt, seinen Familienstand, seinen Beruf, seinen Wohnort, seine Wohnung oder seine Staatsangehörigkeit eine unrichtige Angabe macht oder die Angabe verweigert. Die Norm stellt allerdings keine allgemeine Datenerhebungsbefugnis der Strafverfolgungsbehörden dar und begründet ebenso wenig eine Auskunftspflicht für Anzeigeerstattende, sondern setzt eine speziell zu diesem Zweck geschaffene Rechtsvorschrift voraus. Nur diese kann darüber bestimmen, wem gegenüber und in welchem Umfang eine Verpflichtung zur Offenbarung bestimmter Identitätsdaten besteht. § 111 Abs. 1 OWiG regelt also nur die Konsequenzen, die aus einer Verweigerung von Informationen erwachsen, zu deren Angabe betroffene Personen aufgrund einer anderen gesetzlichen Vorschrift verpflichtet wären. Die Erhebung personenbezogener Daten durch die Strafverfolgungsbehörden – hier im Rahmen von Angaben im Formular der Onlinewache – muss darüber hinaus zur Aufgabenerfüllung der Strafverfolgungsbehörden erforderlich sein, da diese bei der Verarbeitung personenbezogener Daten dem Grundsatz der Erforderlichkeit (§ 47 Nr. 3 Bundesdatenschutzgesetz [BDSG]) unterliegen. Es ist nicht erkennbar, dass beispielsweise Angaben über den Familienstand oder das Geburtsland der/des Anzeigeerstattenden zur Bearbeitung der Anzeige erforderlich sind.

Ich habe dem SMI meine Rechtsauffassung erläutert und darauf hingewiesen, dass für die Bearbeitung von Anzeigen offensichtlich nicht alle der im Rahmen der Onlineanzeige abgefragten Daten erforderlich sind. Unter Umständen „hilfreiche" Angaben (wie das Geburtsland und der Familienstand) können, wenn im Einzelfall erforderlich, nachgefragt oder optional gemacht werden. Ich habe daher vorgeschlagen, die Pflichtangaben auf einen tatsächlich erforderlichen Datensatz zu

beschränken und weitere Angaben unmissverständlich als „freiwillige" Angaben zu kennzeichnen, deren Nichterteilung die Erstattung /Absendung der Onlineanzeige nicht verhindert. Das SMI nahm meine Hinweise zu Kenntnis und zeigte Bereitschaft, diese in die interne Beratung einzubeziehen und an die Entwickler und Betreuer der Onlinewache außerhalb Sachsens weiterzuleiten.

Leider liegt mir keine weitere Stellungnahme bzw. Ergebnismitteilung des SMI vor. Ich konnte allerdings zeitnah feststellen, dass die Eingabemaske der Onlinewache dahingehend abgeändert wurde, dass es dem Anzeigeerstattenden nun freigestellt ist, Angaben zum Geburtsland und Familienstand zu tätigen, was ich sehr begrüße.

Was ist zu tun?
Die Erhebung von Angaben zum/zur Anzeigeerstatter/in im Rahmen der Onlineanzeige muss im Einzelfall zur polizeilichen Bearbeitung der Anzeige erforderlich sein, da Strafverfolgungsbehörden bei der Verarbeitung personenbezogener Daten dem Grundsatz der Erforderlichkeit (§ 47 Nr. 3 BDSG) unterliegen.

8.3 Speicherung eines DNA-Identifizierungsmusters in der DNA-Analyse-Datei des Bundeskriminalamtes

↗ § 81g StPO

Tätigkeitsbericht Datenschutz 2022:
↗ sdb.de/tb2022

Im Tätigkeitsbericht für das Jahr 2022 (8.3, Seite 205 ff.) berichtete ich über einen Fall, in dem unterschiedliche Bearbeitungszeiten von DNA-Proben bzw. -tatortspuren dazu geführt hatten, dass ein exklusiv für ein einzelnes Strafverfahren wegen eines geringfügigen Delikts (Hausfriedensbruch) erhobenes DNA-Identifizierungsmuster zur Feststellung der Beteiligung des Petenten auch an einer anderen Tat (Sachbeschädigung, Zerstörung einer Fensterscheibe) geführt hatte. Wegen der chronologischen Besonderheiten des Einzelfalls war dagegen datenschutzrechtlich nichts einzuwenden; das Landeskriminalamt Sachsen (LKA) hatte auch bestätigt, dass es die Probe aus dem Verfahren wegen Hausfriedensbruchs – gesetzesgemäß – nicht für Zwecke künftiger Strafverfolgung speichere.

Allerdings verblieb das DNA-Identifizierungsmuster, das aus Tatortspuren der Sachbeschädigung gewonnen und ur-

sprünglich keiner Person zuzuordnen gewesen war, in der DNA-Analyse-Datei (DAD) beim Bundeskriminalamt (BKA). DNA-Identifizierungsmuster aus an Tatorten gefundenen Spuren dürfen in der DAD gespeichert werden, § 81g Abs. 5 Nr. 2 Strafprozessordnung (StPO). Auf diese Rechtsgrundlage stützt sich auch das Landeskriminalamt. Mit dem positiven Ergebnis des Abgleichs im Jahr 2021 (siehe oben genannten Beitrag aus 2022) war für das Landeskriminalamt aus einer Spur einer ursprünglich unbekannten Person ein DNA-Identifizierungsmuster geworden, das einer konkreten Person – dem Petenten – zugeordnet werden konnte.

Dies wirkte sich auf die Ermittlungen in einem Verfahren im Jahr 2023 aus. Am Tatort wurden Spuren festgestellt und einer DNA-Analyse unterzogen. Das erlangte DNA-Identifizierungsmuster wurde daraufhin mit dem Datenbestand der DAD abgeglichen. Dabei wurde eine Übereinstimmung der aktuellen Spur mit dem Muster aus dem Sachbeschädigungsverfahren festgestellt, das nach wie vor in der DAD gespeichert war – und zum Petenten führte. Der Petent fragte sich nun, ob entgegen den Versicherungen, die ihm 2021 gemacht worden waren, sein damals generiertes DNA-Identifizierungsmuster doch für Zwecke der späteren Strafverfolgung in anderen Verfahren genutzt wird.

Die Vermutung trifft zwar nicht direkt zu, mittelbar aber, jedenfalls in den Konsequenzen, durchaus. Denn im Ergebnis wurde aufgrund des beim Petenten erhobenen DNA-Identifizierungsmusters eine ursprünglich anonyme bzw. pseudonyme Speicherung in der DAD personenbeziehbar. Der – ebenfalls aus einer unerheblichen Straftat stammende – „Spurendatensatz" verwandelte sich insoweit in einen „Personendatensatz", als dem LKA, als für den „Spurendatensatz" zuständiger und für die Zugriffsberechtigten der DAD erkennbaren Polizeidienststelle, die Person hinter dem Muster bekannt geworden war. Mit dem Verbleib des DNA-Identifizierungsmusters aus dem Sachbeschädigungsverfahren konnte dieses praktisch – wie im Ermittlungsverfahren 2023 geschehen – für künftige Strafverfahren verwendet werden.

Rechtlich ist ein solches Vorgehen äußerst problematisch, denn die fortdauernde Speicherung wirkt sich exakt wie die Speicherung eines Personendatensatzes nach § 81g Abs. 1 bzw. § 81g Abs. 5 Nr. 1 StPO aus, die allerdings nur unter hohen Voraussetzungen zulässig ist und entweder richterlich angeordnet oder dem Betroffenen mitgeteilt werden muss, der dann eine richterliche Entscheidung herbeiführen kann. Weder wurde gegen den Petenten die Speicherung seines DNA-Identifizierungsmusters nach § 81g Abs. 1 StPO richterlich angeordnet, noch erfolgte eine Umwidmung seines vorliegenden DNA-Identifizierungsmusters nach den Vorgaben von § 81g Abs. 5 Nr. 1 StPO.

Damit würden sämtliche vom Gesetzgeber in § 81g Abs. 1 und 3 bzw. 5 Satz 4 StPO vorgeschriebenen grundrechtsschützenden Vorkehrungen (Voraussetzung sind das Vorliegen einer mindestens erheblichen Straftat, eine begründete Negativprognose und eine richterliche Anordnung bzw. Unterrichtung des Betroffenen) umgangen, wenn DNA-Identifizierungsmuster, die aus Tatortspuren gewonnen und als Spurendatensatz in der DAD gespeichert werden, auch nach Zuordnung zu einer bestimmten Person einfach weitergespeichert und verwendet würden.

Dass damit Rechte Betroffener verletzt würden und die in der Systematik der Vorschrift des § 81g StPO zum Ausdruck kommende Intention des Gesetzgebers unberücksichtigt bliebe, liegt auf der Hand.

Dementsprechend sieht auch die Errichtungsanordnung des BKA zur DAD auf Grundlage von § 81g Abs. 5 Satz 2 Nr. 2 StPO die Speicherung des DNA-Identifizierungsmuster (nur) „unbekannter Spurenleger" vor. Kann das BKA irgendwann ein gespeichertes DNA-Identifizierungsmuster einer zunächst unbekannten Person einem (namentlich bekannten) Beschuldigten oder Verurteilten oder einer gleichgestellten Person zuordnen, unterrichtet das BKA hiervon das zuständige LKA, die zuständige Bundespolizeibehörde oder das Zollkriminalamt unter Mitteilung der gespeicherten Verfahrensdaten. Erfolgt die Zuordnung durch ein LKA, die Bundespolizei oder das Zollkriminalamt, kann die vorgenannte Verpflichtung des

BKA dadurch erfüllt werden, dass das LKA, die Bundespolizei oder das Zollkriminalamt den Datenbesitzer unterrichtet, so die Errichtungsanordnung des BKA.

Aus der gesetzgeberischen Konzeption des § 81g StPO und der Errichtungsanordnung des BKA zur DAD ergibt sich, dass ein ursprünglich keiner Person zuordenbarer Spurendatensatz in der DAD nach der Zuordnung zu einer bestimmten Person entweder nach § 81g Abs. 5 Nr. 1 StPO unter den Voraussetzungen von § 81g Abs. 1 StPO und der Unterrichtung des Betroffenen zur Speicherung für künftige Strafverfolgung „umgewidmet" oder mangels Vorliegen der Voraussetzungen von § 81g Abs. 1 StPO und dem Verlust der „Anonymität" als Spurendatensatz in der DAD gelöscht werden muss. Verantwortlich dafür, die Löschung in die Wege zu leiten, wäre im vorliegenden Fall das LKA Sachsen.

Eine Antwort des LKA Sachsen auf meine Nachfragen, die ich im Berichtszeitraum Ende September übersandt hatte, steht noch aus. Angesichts der Rechtslage und der damit in Einklang stehenden untergesetzlichen Bestimmungen des BKA in der Errichtungsanordnung zur DAD, wird allerdings an einer Löschung oder gesetzeskonformen Umwidmung des DNA-Identifizierungsmusters des Petenten in der DAD kein Weg vorbeiführen.

Was ist zu beachten?
Eine Speicherung von DNA-Identifizierungsmustern aus Tatortspuren ist ohne das Vorliegen der Voraussetzungen von § 81g Abs. 1 StPO zulässig, wenn der sogenannte Spurenleger unbekannt ist. Ist ein DNA-Identifizierungsmuster einer bestimmten Person zuordenbar, ist eine weitere Speicherung in der DAD nur unter den Voraussetzungen von § 81g Abs. 1 StPO und unter Beachtung der Benachrichtigungspflicht erlaubt.

8.4 Zur Zulässigkeit von behördlichen Bildaufzeichnungen von „Elterntaxis" vor einer Schule zur Beweissicherung in einem Bußgeldverfahren

↗ § 100h Abs. 1 Nr. 1 StPO in Verbindung mit § 46 Abs. 1 OWiG

Ein Petent wandte sich an mich mit dem Vortrag, dass Eltern bzw. andere Personen, die Schüler/innen eines sächsischen Gymnasiums morgens mit dem Pkw zur Schule bringen, bei dem Ausladevorgang ihrer Kinder vom Ordnungsamt foto-

grafiert würden. Folgend werde dann gegen sie ein Bußgeldverfahren wegen des Vorwurfs der Behinderung anderer Verkehrsteilnehmer/innen eingeleitet; und zwar auch dann, wenn dieser Ausladevorgang nur wenige Sekunden gedauert und mangels Behinderung anderer Verkehrsteilnehmer/innen keinerlei Bußgeldtatbestand erfüllt habe. Das angefertigte Bildmaterial würde dabei als Beweismittel genutzt werden. Das von mir um Stellungnahme gebetene Ordnungsamt bestätigte den Sachverhalt dahingehend, dass nur Fotos von Fahrzeugen gefertigt worden seien, bei denen zunächst der Verdacht einer Verkehrsordnungswidrigkeit (Behinderung anderer Verkehrsteilnehmer durch Außer-Acht-Lassen der im Verkehr erforderlichen Sorgfalt) bestanden habe. Zu dem Zeitpunkt, als die Mitarbeitenden des Gemeindevollzugsdienstes die Fotos anfertigten, seien sie der Auffassung gewesen, dass die konkreten Tatbestände erfüllt seien. Die Bilder hätten in dem Verwarnungs- sowie in dem Bußgeldverfahren ausdrücklich der Beweissicherung gedient.

Eine behördlich durchgeführte Bildaufnahme, bei der der/die Fahrer/in und das Kennzeichen seines/ihres Fahrzeugs identifizierbar sind, stellt einen Eingriff in das allgemeine Persönlichkeitsrecht in seiner Ausprägung als Recht auf informationelle Selbstbestimmung dar (BVerfG, Urteil vom 11.08.2009 – 2 BvR 941/08) und bedarf einer Rechtsgrundlage. Diese findet sich in § 100h Abs. 1 Nr. 1 Strafprozessordnung (StPO) in Verbindung mit § 46 Abs. 1 Gesetz über Ordnungswidrigkeiten (OWiG). Danach dürfen auch ohne Wissen der betroffenen Personen außerhalb von Wohnungen Bildaufnahmen hergestellt werden, wenn dies zur Erforschung des Sachverhalts und damit von Ermittlungszwecken dient. § 100h Abs. 1 Nr. 1 StPO kann als Ermächtigungsgrundlage für einen Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen allerdings nur in Betracht kommen, wenn die Bildaufzeichnungen zeitlich nach dem Vorliegen eines Anfangsverdachts für die Begehung einer Straftat oder – über die Verweisung in § 46 Abs. 1 OWiG – auch für eine Ordnungswidrigkeit ausgelöst werden (OLG Bamberg, Beschluss vom 16. November 2009 – 2 Ss OWi 1215/2009). Damit

muss die Betroffeneneigenschaft einer Fahrerin bzw. eines Fahrers bereits durch entsprechend konkrete Anhaltspunkte begründet sein. Ein Generalverdacht dahingehend, dass an bestimmten Stellen oder zu bestimmten Zeiten regelmäßig oder häufig bestimmte Verkehrsverstöße begangen werden, reicht nicht aus. Ein Anfangsverdacht ist nur dann gegeben, wenn zureichende tatsächliche Anhaltspunkte für das Vorliegen einer vorwerfbaren Ordnungswidrigkeit bestehen. Diese Anhaltspunkte müssen zudem objektivierbar sein, um die Rechtmäßigkeit der Feststellung des Anfangsverdachts überprüfbar und damit transparent zu machen (OLG Düsseldorf, Beschluss vom 9. Februar 2010 – IV-3 RBs 8/10). Vorliegend hätten zum Zeitpunkt der verfahrensgegenständlichen Bildaufnahmen somit tatsächliche Anhaltspunkte für das Vorliegen einer Verkehrsordnungswidrigkeit bestehen müssen. Die vom Ordnungsamt als Beweismittel vorgelegten zwei Lichtbilder zeigten jedoch lediglich ein vor dem Haupteingang der Schule haltendes Fahrzeug, ein aussteigendes Schulkind sowie einen passierenden anderen Pkw. Der Zeitstempel wies jeweils minutiös die gleiche Uhrzeit auf. Eine unvermeidbare Behinderung anderer Verkehrsteilnehmer/innen war weder tatsächlich (zum Beispiel aufstauende Fahrzeuge) noch zeitlich (Haltevorgang länger als 3 Minuten) erkennbar. Mangels konkreten Anfangsverdachts schied somit § 100h Abs. 1 Nr. 1 StPO in Verbindung mit § 46 Abs. 1 OWiG als taugliche Rechtsgrundlage für die Anfertigung der Bildaufnahmen aus.

Die Rechtsgrundlage in § 100h Abs. 1 Nr. 1 StPO ermächtigt zu erheblichen Grundrechtseingriffen und hat damit schwerwiegende Folgen. Demgemäß sind hohe Anforderungen an die Zuverlässigkeit der Ermittlung des konkreten Anfangsverdachts zu stellen. Dies habe ich dem verantwortlichen Ordnungsamt entsprechend erläutert und es aufgefordert, die Mitarbeiter unverzüglich dahingehend zu sensibilisieren, dass vor dem Start der Bildaufzeichnung zureichende tatsächliche und konkret ausgestaltete Anhaltspunkte für eine Verkehrsordnungswidrigkeit vorliegen müssen, die sich gegen eine/n bestimmte/n Fahrzeugführer/in richten. Eine

Was ist zu beachten?
Die Rechtsgrundlage in § 100h Abs. 1 Nr. 1 StPO ermächtigt Strafverfolgungs- und Ordnungswidrigkeitenbehörden zu erheblichen Grundrechtseingriffen und hat damit schwerwiegende Folgen. Demgemäß sind hohe Anforderungen an die Zuverlässigkeit der Ermittlung des konkreten Anfangsverdachts zu stellen.

Vermutung, es könnte sich um eine entsprechende Ordnungswidrigkeit handeln bzw. sich im Nachgang aus dem angefertigten Bildmaterial ergeben, reicht indes nicht aus.

8.5 Kontrolle von Gefangenenpost in der Justizvollzugsanstalt

↗ §§ 33, 35 SächsStVollzG

Gleich mehrere Eingaben im Berichtszeitraum betrafen eine Problematik, die in verschiedenen Justizvollzugsanstalten (JVA) des Freistaates aufgetreten ist. Gefangene wandten sich an mich und teilten inhaltlich etwa gleichlautend mit, dass sie ihre eingehende Post nur noch in Form von Kopien der Originalschreiben ausgehändigt bekämen. Sie äußerten Bedenken gegen diese Abweichung von dem bis dahin üblichen Verfahren, in dem eingehende Schreiben nicht inhaltlich kontrolliert und nicht kopiert wurden.
Auf meine Nachfragen in den betroffenen JVA erläuterten mir diese die Hintergründe der Maßnahme. Die Anstalten erklärten inhaltlich übereinstimmend, dass das gehäufte Auffinden von mit sogenannten „NPS" (Neue psychoaktive Substanzen) getränktem Papier innerhalb der Anstalt und dessen Konsum zur Gefährdung der Sicherheit und Ordnung in der Anstalt führe. Die bundesweit in JVA verbreitete Form des NPS-Konsums sei das Rauchen der getränkten Blätter. Der Konsum von NPS könne schwere gesundheitliche Folgen nach sich ziehen und bis zum Tod des Konsumenten führen. Überprüfungen der Beschaffenheit der eingehenden Post bzw. der bei Aushändigung an den Gefangenen mittels Sichtkontrolle sichergestellten Papiere, die unter dem Verdacht standen, mit NPS getränkt zu sein, hätten den Verdacht bestätigt. Auch im Rahmen von Haftraumkontrollen seien Papierstücke und andere Unterlagen (zum Beispiel Prospekte) als mit NPS-getränkt sichergestellt worden. Der Konsum des Stoffes habe bei mehreren Gefangenen zum Teil lebensbedrohliche

Situationen verursacht. Gefangene hätten intensivmedizinisch betreut und in jedem Fall notfallmedizinisch behandelt werden müssen. Es habe auch einen Todesfall gegeben. Die Gesundheit der Gefangenen und die Sicherheit und Ordnung der Anstalt würden aber nicht nur unmittelbar durch den Konsum von NPS, sondern auch durch Auseinandersetzungen um Angebot, Besitz und Handel von Betäubungsmitteln gefährdet. Die Intensität der Auseinandersetzungen habe zugenommen und zu erheblichen Verletzungsbildern geführt. Die Einbringung des NPS in die JVA erfolge nachweislich auch über die Gefangenenpost. Dabei werde nicht nur das Briefpapier selbst, sondern auch der Briefumschlag als Träger der NPS genutzt. Die eingehende Post werde nicht abgeschrieben und somit auch nicht gespeichert. Die Postsendungen würden kopiert, ohne dass diesbezüglich ein Zwischenspeichern möglich wäre. Die Originalschreiben würden zur Habe des Gefangenen genommen. Die von mir kontaktierten JVA stützen die Maßnahmen auf §§ 33, 34, 35 Sächsisches Strafvollzugsgesetz (SächsStVollzG), wonach unter anderem bei Gefährdung der Sicherheit oder Ordnung Schriftwechsel überwacht und eingehende Schreiben angehalten werden können.

Gegen das Vorgehen der JVA bestehen keine datenschutzrechtlichen Bedenken.

Angesichts der durch die Einbringung von NPS in die JVA bestehenden Gefährdung der Sicherheit und Ordnung der Anstalt, vor allem aber von Leib und Leben der Gefangenen, ist die von den Anstalten gewählte Verfahrensweise eine angemessene Maßnahme zur Gefahrenabwehr; es handelt sich weder um eine „Strafe" noch um eine Umgehung der Unschuldsvermutung. Das Sichten der eingehenden Post in Abwesenheit der Gefangenen und das Kopieren der eingehenden Schriftstücke mit anschließender Aushändigung nur der Kopien sind Einschränkungen, die die Anstalt auf §§ 33 Abs. 2 Satz 2 und 35 Abs. 1 Nr. 1 SächsStVollzG stützen kann, wobei das Kopieren als eine sogenannte Minusmaßnahme gegenüber einem Anhalten der Schreiben in Form der gänzlichen Vorenthaltung angesehen werden kann. Die Re-

gelungen stellen gesetzliche Befugnisse zur Beschränkung des Schriftwechsels dar, die bei einer konkreten Anwendung unter Berücksichtigung der Umstände des Einzelfalls selbstverständlich angemessen und verhältnismäßig ausgeübt werden müssen. Die Gefährdung der Sicherheit der Anstalt und der Gesundheit der Gefangenen durch NPS ist so erheblich, dass ich die mit dem Kopieren der eingehenden Gefangenenpost einhergehenden Unannehmlichkeiten für die Gefangenen als verhältnismäßig und zumutbar ansehe. Zu berücksichtigen ist dabei, dass die Gefangenen die Inhalte der ihnen zugehenden Schreiben zur Kenntnis nehmen können und der gedankliche Austausch mit dem Absender der Post weiterhin möglich bleibt.

Weil die Problematik nicht nur in einer JVA virulent war, habe ich gegenüber dem Sächsischen Ministerium der Justiz und für Demokratie, Europa und Gleichstellung als Aufsichtsbehörde für die sächsischen Anstalten angeregt, im Erlasswege eine einheitliche Vorgehensweise im Umgang mit eingehender Gefangenenpost in den JVA des Freistaates sicherzustellen und dabei darauf hinzuwirken, dass die Beeinträchtigungen für die Gefangenen (zum Beispiel Verzögerungen im Postlauf, optische Abstriche bei original farbigen Schriftstücken, Speicherung/Aufbewahrung der Originale mit weiten Zugriffsmöglichkeiten seitens der Anstalt) möglichst gering bleiben.

Das Ministerium überlässt es der jeweiligen Anstaltsleitung, nach pflichtgemäßem Ermessen über das „Ob" von oben beschriebenen Kontrollen und den betroffenen Personenkreis zu entscheiden. Für den Fall, dass Gefangenenpost aus den oben beschriebenen Gründen kontrolliert wird, werden die Anstalten per Erlass gebeten,

- die durch die notwendigen Maßnahmen eingetretene Verzögerung des Postlaufs so gering wie möglich zu halten,
- eingehende Originalschreiben lediglich maschinell zu kopieren,
- keine Speicherung der Kopien vorzunehmen,

- den Gefangenen mitzuteilen, ob und welche (Wert-) Gegenstände der eingehenden Post entnommen und zu ihrer Habe genommen werden, sowie
- farbige Schriftstücke, Karten, beigefügte Fotos, Bilder oder Zeichnungen in Farbkopie an die Gefangenen auszureichen.

Was ist zu tun?
Beschränkungen von Grundrechten und besonders geschützten Geheimnissen sind im Strafvollzug unter gesetzlich bestimmten Voraussetzungen möglich. Insbesondere wenn die Sicherheit oder Ordnung der Anstalt nachweislich gefährdet ist, sind Beschränkungsmaßnahmen zulässig bzw. geboten. Die Maßnahmen müssen im Einzelfall verhältnismäßig sein.

Nach Auskunft des Ministeriums besitzen die in den JVA zum Einsatz kommenden Kopierer zwar eine Festplatte, die für das Zwischenspeichern großer Dokumente gebraucht werde. Diese Dokumente würden aber nach Ausdruck automatisch gelöscht. Damit besteht auch kein Grund zu der von Petenten geäußerten und zunächst nicht ganz unberechtigt erscheinenden Befürchtung, dass inhaltlich unverfängliche Schreiben über einen langen Zeitraum auf Datenträgern gespeichert werden und von der JVA verwendet werden könnten.

8.6 Veröffentlichung von Übersichtsbildern von Ansammlungen auf Social-Media-Kanälen der Polizei

↗ § 57 Abs. 1 Satz 2 SächsPVDG, § 11 Abs. 2 Satz 2 SächsVersG

Eine langwierige und im Berichtszeitraum nicht abgeschlossene Diskussion mit dem Staatsministerium des Innern (SMI) betraf die Veröffentlichung eines Übersichtsbildes, das eine größere Gruppe niederländischer Fußballfans auf ihrem Fanmarsch vor einem Spiel bei der Europameisterschaft in Leipzig zeigte. Wir wurden durch einen Hinweis auf das Foto aufmerksam gemacht, das die Polizei Sachsen auf ihrem Profil auf der Plattform X (vormals Twitter) veröffentlicht hatte. Im Post der Polizei fand sich zum Bild folgender Begleittext:

> „Falls sich jemand fragt, was hier los ist: es ist alles okay. Es ist nur der Fan Walk der niederländischen Fans zum #Leipzig Stadium. #NEDFRA."

Meine an das Landespolizeipräsidium (LPP) gerichtete Frage nach der Rechtsgrundlage für die Aufnahme und die Veröffentlichung des Bildes sowie mein Hinweis auf die Rechtslage, nach der die Polizei zwar laufende Übersichtsbildübertragungen von Versammlungen und Ansammlungen (nicht als Versammlung zu qualifizierende Zusammenkünfte) vornehmen, aber keine Aufzeichnungen von Übersichtsbildern fertigen darf, waren der Auftakt für eine noch andauernde Kontroverse über den rechtlichen Rahmen polizeilicher Öffentlichkeitsarbeit. Seitens des Staatsministeriums wird die Diskussion nicht aus dem LPP geführt, sondern vom Kommunikationsreferat des Ministeriums, das außerhalb der Organisationsstruktur des LPP agiert.

Das stellt sich auf den Standpunkt, dass einzelne Personen auf dem veröffentlichten Lichtbild nicht erkennbar seien, insoweit gebe es auch keinen Grundrechtseingriff. Die Veröffentlichung durch das Kommunikationsreferat des Ministeriums sei als staatliches Informationshandeln ohne besondere gesetzliche Eingriffsermächtigung zulässig gewesen. Das Foto sei nicht in Ausübung hoheitlicher Gewalt im Rahmen der Gefahrenabwehr durch die sächsische Polizei aufgenommen, sondern von der Stadt zur Verfügung gestellt worden. Bei der Öffentlichkeitsarbeit gehe es gerade nicht um Gefahrenabwehr. Spezielle Rechtsvorschriften aus dem Gefahrenabwehrrecht, hier dem Sächsischen Polizeivollzugsdienstgesetz (SächsPVDG), kämen deshalb nicht zur Anwendung.

Ich habe das Ministerium aufgefordert, das Bild auf dem X-Profil der Polizei Sachsen zu löschen und künftig von der Veröffentlichung von Lichtbildern von Ansammlungen oder Versammlungen auf Social-Media-Kanälen der Polizei Sachsen abzusehen, und zur Begründung auf die Rechtslage verwiesen. Das X-Profil ist ein Profil der sächsischen Polizei („Polizei Sachsen", „Hier postet das Social-Media-Team der Polizei Sachsen"), wobei das Social-Media-Team der Polizei Sachsen in das Referat Kommunikation im SMI eingebettet ist und dort die Kanäle der sächsischen Polizei in den sozialen Netzwerken betreut. Das Staatsministerium ist – jedenfalls als „oberste Dienstbehörde und Führungsstelle der Polizei"

(§ 99 Abs. 1 SächsPVDG) und Behörde, in der sowohl das LPP Sachsen als auch das Kommunikationsreferat des Staatsministeriums angesiedelt ist – Verantwortlicher im Sinne von Art. 4 Nr. 7 Datenschutzgrundverordnung (DSGVO) für die Speicherung des gegenständlichen Bildes vom Marsch der niederländischen Fußballfans am 21. Juni 2024 in Leipzig und für seine Verbreitung auf dem X-Account der Polizei Sachsen. Wenn das Ministerium auf einem Kanal der „Polizei Sachsen" Öffentlichkeitsarbeit betreibt, müssen die gesetzgeberischen Vorgaben für die Polizei eingehalten werden. Die intraministerielle Organisationsstruktur und Zuständigkeit für Öffentlichkeitsarbeit (auch der Polizei) sind dabei ohne Belang.

Ob auf dem Lichtbild einzelne Personen identifizierbar waren oder nicht – diese Frage war und ist umstritten – ist im Ergebnis unerheblich, denn der sächsische Gesetzgeber verbietet der Polizei die Fertigung von Aufzeichnungen von Übersichtsbildern von Ansammlungen und damit selbstverständlich auch eine Verwendung solcher Bilder durch die Polizei generell.

Die Polizei darf gemäß § 57 Abs. 1 Satz 1 SächsPVDG bei abstrakten Gefahren im Zusammenhang mit öffentlichen Veranstaltungen oder Ansammlungen unter freiem Himmel, die nicht dem Sächsischen Versammlungsgesetz (SächsVersG) 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. Nach Satz 2 der Vorschrift ist der Polizei eine Identifikation von Personen oder Aufzeichnung der Übertragung nicht erlaubt.

Aufzeichnungen im Sinne der genannten Vorschriften sind Bilder, die in Abgrenzung zu flüchtigen Livebildern der bloßen Übersichtsbildübertragung gespeichert werden und über den Moment der Entstehung hinaus vorliegen. Hierunter zählen sowohl Einzelbilder – wie das streitgegenständliche – als auch Videosequenzen.

Das damit bezüglich des Fanmarschs einschlägige gesetzliche Verbot von Bildaufzeichnungen bezieht sich zunächst auf das eigene Tätigwerden der Polizei, die unmittelbarer Adressat der Regelung in § 57 Abs. 1 SächsPVDG ist; es schließt aber – selbstverständlich – auch das Verbot für die Polizei ein, Bilder, die sie nach § 57 SächsPVDG selbst nicht anfertigen dürfte, ohne spezielle Rechtsgrundlage (etwa im Rahmen der Strafverfolgung nach strafprozessualen Vorschriften) bei Dritten zu erheben oder von dritter Seite anzunehmen und für eigene Zwecke zu verwenden. Andernfalls würde der klare, in den oben genannten Vorschriften zum Ausdruck kommende gesetzgeberische Wille umgangen. Dies gilt – erst recht – auch im Bereich der Öffentlichkeitsarbeit, in dem, soweit überhaupt erforderlich, eine Information der Öffentlichkeit über polizeilich relevante Auswirkungen einer Veranstaltung oder Ansammlung ohne Weiteres auch ohne (unzulässig verarbeitete) Lichtbilder derselben erfolgen kann.

Der sächsische Gesetzgeber hat mit § 57 Abs. 1 Satz 2 SächsPVDG und § 11 Abs. 2 Satz 2 SächsVersG klare Bestimmungen getroffen, die (umstrittene) Beurteilungen des Einzelfalls zur Erkennbarkeit von einzelnen Personen auf Übersichtsbildern obsolet machen: eine Aufzeichnung von Übersichtsbildern sowohl von Ansammlungen als auch von Versammlungen ist stets und ausnahmslos unzulässig, wobei völlig unerheblich ist, ob im Einzelfall einzelne Personen identifizierbar sind.

Vorschriften des Polizeirechts, insbesondere Bestimmungen über die Verarbeitung von personenbezogenen Daten oder über die Unzulässigkeit von Bildaufzeichnungen von Personengruppen, wirken sich unmittelbar auch auf die Zulässigkeit der polizeilichen Verwendung dieser Daten bzw. Bilder in einem anderen Sachzusammenhang – etwa, wie hier, im Rahmen der polizeilichen Öffentlichkeitsarbeit – aus. Die gesetzlichen Verbote in § 57 Abs. 1 Satz 2 SächsPVDG bzw. § 11 Abs. 2 Satz 2 SächsVersG greifen insoweit vollumfänglich durch: was der Polizei bei der Erfüllung ihrer Kernaufgaben nicht erlaubt ist, ist ihr erst recht nicht im Rahmen allgemeiner, kaum regulierter Behördentätigkeiten gestattet.

Die gefahrenabwehrrechtlichen Vorschriften des SächsPVDG erfassen naturgemäß nicht unmittelbar Tätigkeiten der polizeilichen Öffentlichkeitsarbeit ohne Gefahrenabwehrbezug, ihre Ge- und Verbote strahlen aber auf die Öffentlichkeitsarbeit aus und entfalten so mittelbare Wirkung. Alles andere wäre offensichtlich absurd: die Polizei könnte mit dem Hinweis auf Öffentlichkeitsarbeit Maßnahmen durchführen und etwa Lichtbilder fertigen, die ihr im Rahmen der Erfüllung ihrer gesetzlichen Aufgaben als Strafverfolgungs- oder Gefahrenabwehrbehörde aufgrund einschlägiger spezieller Vorschriften nicht erlaubt wären.

Grundrechtsträger müssen sich sicher sein können, dass die Polizei über den Weg der Öffentlichkeitsarbeit keine Daten und Angaben in ihren Informationsbestand aufnimmt, deren Speicherung und Verwendung ihr nach polizeigesetzlichen Bestimmungen untersagt ist. Dies gilt ebenso bzw. erst recht für eine weltweite Verbreitung solcher Informationen, insbesondere auf Kanälen in Netzwerken, die aus einem Staat außerhalb der EU betrieben werden.

Polizeiliche Öffentlichkeitsarbeit – gerade als „Polizei Sachsen" auf Social-Media-Kanälen – bleibt eine (wenn auch nicht gefahrenabwehrende) polizeiliche Tätigkeit und findet nicht im rechtsfreien Raum statt. Daten- und Bildverarbeitungen, die der Polizei als Gefahrenabwehrbehörde untersagt sind, sind ihr auch im Bereich der Öffentlichkeitsarbeit nicht gestattet; insofern entfalten gefahrenabwehrrechtliche Vorschriften Ausstrahlungswirkung (siehe oben). Im Ausgangsfall war im Übrigen ein Zusammenhang der Veröffentlichung des Bildes mit polizeilicher Tätigkeit nicht erkennbar – weder gab es an die Öffentlichkeit gerichtete Hinweise auf Verkehrsbeschränkungen im Stadtbereich noch auf sonstige Konsequenzen des Fan-Walks. Der Post sollte ausweislich des Begleittextes zum Lichtbild offensichtlich allein der Unterhaltung der Follower dienen. Eine Polizeibehörde wird aber nicht journalistisch tätig, auch wenn sie Öffentlichkeitsarbeit betreibt (OVG für das Land Nordrhein-Westfalen, Urteil vom 17. September 2019 – 15 A 4753/18 –, Rn. 110, juris).

Was ist zu tun?
Behörden haben im Rahmen ihrer Öffentlichkeitsarbeit spezialrechtliche Vorgaben aus dem Bereich ihrer gesetzlichen Aufgabenerfüllung zu berücksichtigen. Der Polizei ist die Aufzeichnung von Übersichtsbildübertragungen von An- und Versammlungen gesetzlich untersagt. Dieses Verbot führt zur Unzulässigkeit der Verwendung von Übersichtsbildern für Zwecke der polizeilichen Öffentlichkeitsarbeit.

Meiner Aufforderung zur Löschung des umstrittenen Posts kam das SMI zwischenzeitlich nach. Hinsichtlich der Aufforderung, künftige Veröffentlichungen von Übersichtsbildern von Ansammlungen oder Versammlungen auf Social-Media-Kanälen zu unterlassen, wird die Diskussion fortgesetzt.
Die datenschutzrechtliche Zulässigkeit der Nutzung sozialer Medien wie Facebook, X oder Instagram durch öffentliche Stellen wurde in diesem Verfahren nicht problematisiert. Das Verfahren der Sächsischen Staatskanzlei/Meta gegen die SDTB wegen Anordnung der Abschaltung einer Facebook-Fanpage ist nach wie vor ohne Entscheidung vor dem Verwaltungsgericht anhängig (vgl. auch 7.7).

8.7 Neufassung des Sächsischen Verfassungsschutzgesetzes

↗ § 24 SächsVSG neue Fassung, in Kraft ab 16.08.2025

Bereits vor einigen Jahren existierten Pläne, das in seiner Grundstruktur noch weitestgehend bestehende Sächsische Verfassungsschutzgesetz (SächsVSG) aus dem Jahr 1992 grundlegend zu überarbeiten beziehungsweise neu zu fassen. Das sichtbar in die Jahre gekommene Gesetz war immer wieder nur punktuell geändert worden, wenn verfassungsgerichtliche Entscheidungen den Gesetzgeber dazu zwangen. Aus verschiedenen Gründen aber kam es trotz teilweise konkreter Ansätze nicht zu Gesetzesentwürfen, die den Weg in das parlamentarische Verfahren gefunden hätten.
Spätestens eine Grundsatzentscheidung des Bundesverfassungsgerichts (BVerfG) im Jahr 2022 (Az.: 1 BvR 1619/17) zu Datenerhebungs- und Übermittlungsbefugnissen von Verfassungsschutzbehörden, die wiederum eine Anpassung des SächsVSG erforderten, bildete schließlich den Anlass, eine vollumfängliche Neufassung des Gesetzes auf den Weg zu bringen.
Wie bereits in weiter zurückliegenden Gesetzgebungsvorhaben, in denen das Sächsische Staatsministerium des Innern (SMI) als oberste Staatsbehörde im Bereich der inneren

Sicherheit involviert war, wurde ich frühzeitig zu den geplanten Vorschriften angehört. Der Austausch mit dem Ministerium gestaltete sich über einen längeren Zeitraum sehr intensiv und konstruktiv. Auch wenn – möglicherweise aber auch gerade weil – in einzelnen Punkten Meinungsverschiedenheiten zutage traten, war die frühzeitige Beteiligung meiner Dienststelle aus meiner Sicht für das Vorhaben sehr förderlich. Ein frühzeitiger Austausch über geplante Rechtsvorschriften kann bei einer sachorientierten Kommunikation dabei unterstützen, die wesentlichen Ziele des Entwurfs in den Fokus zu stellen, Schwachstellen und Unklarheiten zu identifizieren und zu beheben, Missverständnisse auszuräumen und dementsprechend Diskussions- und Änderungsbedarf im Fortgang des Gesetzgebungsvorhabens zu verringern. Dieses Vorhaben steht exemplarisch dafür, dass bei einer solchen Kooperation alle Beteiligten – vor allem aber auch die potenziell betroffenen Grundrechtsträger/innen – nur gewinnen können.

Der Referentenentwurf der Staatsregierung vom 11. Januar 2024 wurde mit einigen Änderungen am 12. Juni 2024 durch den Sächsischen Landtag beschlossen. Verkündet wurde das Gesetz am 16. August 2024, in Kraft treten wird es ein Jahr später, am 16. August 2025. Bis dahin gelten die Vorschriften des aktuellen Verfassungsschutzgesetzes, die selbstverständlich verfassungskonform auszulegen und unter Berücksichtigung der verfassungsgerichtlichen Rechtsprechung anzuwenden sind.

Datenschutzrechtliche Aspekte

Das meines Erachtens insgesamt sehr ausgewogene Gesetz setzt die Vorgaben des BVerfG zur Festlegung der Eingriffsschwellen für nachrichtendienstliche Befugnisse um, wobei die Eingriffsvoraussetzungen höher werden, je tiefer die Maßnahmen in Grundrechte der Betroffenen eingreifen. Der Freistaat Sachsen ist eines der wenigen Bundesländer, die dem aus den Entscheidungen des BVerfG resultierenden Änderungsbedarf relativ zeitnah nachgekommen sind.

Sehr zu begrüßen sind Regelungen zur Beschränkung der Weiterverarbeitung erhobener personenbezogener Daten für vom Erhebungszweck abweichende Zwecke sowie eine Begrenzung der Speicherung von mit nachrichtendienstlichen Mitteln erhobenen Daten, deren Erhebung nur unter besonderen Voraussetzungen zulässig ist.

Ebenso erfreulich ist aus datenschutzrechtlicher Sicht, dass der Gesetzgeber von einer Verlängerung der Höchstspeicherfrist für personenbezogene Daten in Dateien oder Akten abgesehen hat. Eine angemessene Begrenzung der Speicherfrist ist für betroffene Personen insbesondere vor dem Hintergrund bedeutsam, dass der verfassungsbehördliche Datenbestand zunehmend bei gesetzlich vorgesehenen Zuverlässigkeitsüberprüfungen einbezogen wird. Für betroffene Personen, die regelmäßig nicht über die Speicherung ihrer Daten in Dateien des Verfassungsschutzes informiert werden, kann eine Erfassung erhebliche Konsequenzen mit sich bringen, etwa, wenn aufgrund der Speicherung Bedenken an ihrer Zuverlässigkeit aufkommen, die zur Versagung beantragter Genehmigungen führen oder sie von der Teilnahme an bestimmten Veranstaltungen ausschließen.

Der sächsische Gesetzgeber hat auch an anderer Stelle eine eigenständige Regelung vorgenommen, die von den Hinweisen der nach der Entscheidung des BVerfG aus dem Jahr 2022 eingerichteten Bund-Länder-Arbeitsgruppe (BLAG) zu gesetzgeberischen Konsequenzen aus dem Urteil rechtsstaatlich angemessen abweicht. Der im Gesetz enthaltene Katalog von besonders bedeutsamen Rechtsgütern, deren konkretisierte Gefährdung im Einzelfall Voraussetzung für Übermittlungen von Daten durch das Landesamt für Verfassungsschutz an andere Behörden ist, umfasst ausschließlich Rechtsgüter, die das BVerfG in diesem Kontext in gefestigter Rechtsprechung erwähnt. „Die Menschenwürde" ist – entgegen den Äußerungen der BLAG – kein solches Rechtsgut; ihr Schutz ist vielmehr ein Verfassungsgrundsatz, ihre Gestalt ist allerdings kaum konturiert und erfährt in vielfältigsten Konstellationen Wechselwirkungen mit staatlichen, gesetzlich legitimierten Handlungen und Aktivitäten privater

Dritter. Eine konkretisierte Gefahr für „die Menschenwürde" ließe sich nicht mit einer Klarheit bestimmen, die als Grundlage für Grundrechtseingriffe unabdingbar ist.
Bemerkenswert ist nach in den letzten Jahren geführten Diskussionen um sogenannte Prüffälle, in denen Verfassungsschutzbehörden möglicherweise verfassungsfeindliche Bestrebungen zwar schon beobachten dürfen, eine extremistische, verfassungsfeindliche Ausrichtung der Bestrebung aber noch nicht erwiesen ist, dass der Gesetzgeber eine diesbezügliche Unterrichtung der Öffentlichkeit unter Bezeichnung der Bestrebung und der Nennung personenbezogener Daten nicht erlaubt. Auch in diesem Punkt ändert sich die derzeitige Rechtslage nicht.

Datenübermittlung an Strafverfolgungsbehörden und sonstige Behörden

Vergleichsweise komplex gerieten im Gesetz die Vorschriften zu Übermittlungen personenbezogener Daten durch das Landesamt für Verfassungsschutz (LfV). Grund hierfür sind die aus den Vorgaben des BVerfG folgenden notwendigen Differenzierungen hinsichtlich der Empfänger der Daten und der Zwecke der Übermittlung im Einzelfall. Die bislang geltenden Normen mussten grundlegend überarbeitet und geschärft werden. Weil Verfassungsschutzbehörden die für ihre Aufgabenerfüllung erforderlichen Daten in aller Regel heimlich erheben und dabei je nach Maßnahme tief in Grundrechte betroffener Personen eingreifen, müssen die Zwecke, für die solche Daten an Strafverfolgungs-, Polizei- und Verwaltungsbehörden übermittelt werden, besonders gewichtig sein. Der Verfassungsschutz, der selbst keine Zwangs- und Vollstreckungsbefugnisse hat, darf nicht als (verdeckt agierender) Informationslieferant für Behörden fungieren, die ihre Maßnahmen mit Zwangsmitteln durchsetzen können, selbst aber nur unter besonders hohen Voraussetzungen die Daten erheben dürften, für deren Erhebung durch die Verfassungsschutzbehörde deutlich niedrigere Schwellen gelten.
Das neue SächsVSG formuliert in seinem § 24 detaillierte, empfänger- und zweckspezifische Übermittlungsvoraussetzungen.

Während des Gesetzgebungsverfahrens wurden gewisse begriffliche Unschärfen sichtbar, die sich aus den Formulierungen des BVerfG ergaben. Zum einen betrifft das den Begriff der „besonders schweren Straftat", für deren Verfolgung das LfV Daten an die Strafverfolgungsbehörden übermitteln darf, zum anderen die Frage, was genau unter den vom BVerfG erwähnten „operativen Anschlussbefugnissen" zu verstehen ist, für deren Anwendung mit nachrichtendienstlichen Mitteln erhobene Daten grundsätzlich nicht an Verwaltungsbehörden übermittelt werden dürfen. Das Gesetz untersagt in § 24 Abs. 2 Satz 1 Nr. 6 Buchst. b SächsVSG Übermittlungen für „Maßnahmen, die unmittelbar mit Zwangswirkung vollzogen werden".

Zwischenzeitlich hat das BVerfG über ähnlich gestaltete Vorschriften des Hessischen Verfassungsschutzgesetzes entschieden (Az.: 1 BvR 2133/22) und dabei Feststellungen getroffen, die zumindest für die Auslegung und Anwendung des neuen SächsVSG relevant sind.

Im Ergebnis stellt das Gericht fest, dass die Qualifizierung einer Straftat als besonders schwer in der Strafnorm selbst einen objektivierten Ausdruck finden muss, insbesondere in deren Strafrahmen und gegebenenfalls in tatbestandlich umschriebenen oder in einem Qualifikationstatbestand enthaltenen Begehungsmerkmalen und Tatfolgen. Danach kann auch eine Straftat mit einer angedrohten Höchstfreiheitsstrafe von mindestens fünf Jahren als besonders schwer eingestuft werden, wenn dies nicht nur unter Berücksichtigung des jeweils geschützten Rechtsguts und dessen Bedeutung für die Rechtsgemeinschaft, sondern auch unter Berücksichtigung der Tatbegehung und Tatfolgen vertretbar erscheint. Für Staatsschutzdelikte oder sonstige im Einzelfall gegen Verfassungsschutzgüter gerichtete Delikte gelten dabei keine speziellen Anforderungen. Daraus folgt, dass allein die Zielrichtung der Tat und der Umstand, dass sie aus einer verfassungsfeindlichen Bestrebung zur Durchsetzung der Ziele dieser Bestrebung begangen wird, noch keine Einordnung als besonders schwere Straftat im Sinne der Rechtsprechung des BVerfG begründen (vgl. § 3 Abs. 5 Nr. 11 SächsVSG neue Fassung).

Zu der Frage, unter welchen Umständen Übermittlungen an Verwaltungsbehörden mit operativen Anschlussbefugnissen beziehungsweise der Möglichkeit, Maßnahmen mit unmittelbarem Zwang durchzusetzen, zulässig sind, stellt das Gericht fest, dass die erhöhten Eingriffsschwellen bei der Übermittlung von mit nachrichtendienstlichen Mitteln erhobenen Daten an andere Behörden bereits dann gelten, wenn die empfangene Stelle grundsätzlich über operative Anschlussbefugnisse überhaupt verfügt. Es kommt also nicht darauf an, ob und inwieweit die Datenübermittlung im Einzelfall deren Einsatz direkt nach sich ziehen soll. Das Gericht stellt klar, dass es nicht auf die Ausübung unmittelbaren Zwangs ankomme, sondern nur auf unmittelbare mögliche Folgemaßnahmen. Die operative Befugnis bezeichnet somit (allein) die Möglichkeit, gegenüber betroffenen Personen Maßnahmen erforderlichenfalls auch mit Zwang durchzusetzen. Eine Unmittelbarkeit dergestalt, dass die Anschlussmaßnahme zu einer Einschränkung des Rechtsschutzes führt, weil sie ohne Anhörung des Betroffenen durchgesetzt werden kann (wie zum Beispiel eine Durchsuchung oder eine Festnahme), ist keine zwingende Voraussetzung für die strengeren Anforderungen an die Übermittlung.

Bei der Auslegung der Vorschriften des neuen Verfassungsschutzgesetzes und der Erarbeitung von Dienstvorschriften und Handlungsleitfäden für die Anwendung in der Praxis, die bis zum Inkrafttreten des Gesetzes am 16. August 2025 vorliegen sollten, werden das LfV und die Fachaufsicht diese Klarstellungen des BVerfG zu berücksichtigen haben. Wie gewohnt, stehe ich für eine Begleitung und Unterstützung dieses Prozesses zur Verfügung.

Was ist zu tun?
Das LfV und das SMI als zuständige Fachaufsichtsbehörde haben bei der Umsetzung der Vorschriften des neuen SächsVSG die Vorgaben des BVerfG zu berücksichtigen.

9 Rechtsprechung zum Datenschutz

9.1 Verwaltungsprozessuales: Konsequenzen der Rechtsprechung des Europäischen Gerichtshofs

↗ Art. 77 Abs. 1, 78 DSGVO; §§ 57 Abs. 2, 58, 74 Abs. 1 VwGO

Unter Bezugnahme auf eine Entscheidung des Europäischen Gerichtshofs (EuGH) in den Rechtssachen C-26/22 und C-64/22 hatte ich bereits in meinem Tätigkeitsbericht 2023 Ausführungen gemacht. Neben den materiell-inhaltlichen Fragen hatte das Gericht auch unter Würdigung der einschlägigen Vorschriften in Art. 77 und 78 Datenschutz-Grundverordnung (DSGVO) klargelegt, dass rechtsverbindliche Entscheidungen der Aufsichtsbehörde in Beschwerdeverfahren gemäß Art. 77 Abs. 1 DSGVO einer vollständigen inhaltlichen Überprüfung unterliegen (vgl. Tätigkeitsbericht 2023, 9.3 – am Ende – sowie den Urteilstext des EuGH, Rn. 36, 70). In mehreren verwaltungsgerichtlichen Verfahren des Berichtszeitraums griff die für diese Streitfälle gegen meine Behörde im Freistaat Sachsen zuständige Kammer des Verwaltungsgerichts Dresden erwartungsgemäß diesen Inhalt, dieser Entscheidung folgend, auf.

Tätigkeitsbericht Datenschutz 2023:
↗ sdb.de/tb2023

Verwaltungsprozessual wird die europagerichtliche Entscheidung seitens meiner Behörde dahingehend interpretiert, dass gegen Entscheidungen meiner Dienststelle im Beschwerdeverfahren gemäß Art. 77 Abs. 1 DSGVO innerhalb eines Monats nach Bekanntgabe der Entscheidung, des Verwaltungsakts, Klage zu erheben ist, § 74 Abs. 1 Satz 2, Abs. 2

Verwaltungsgerichtsordnung (VwGO). Ein Widerspruchsverfahren der betroffenen Personen, das heißt, der/des selbstbetroffenen Beschwerdeführerin bzw. -führers im Sinne von Art. 77 Abs. 1 DSGVO, ist gesetzlich nicht vorgesehen – eine Widerspruchserhebungen gegen die jeweilige aufsichtsbehördliche Entscheidung ginge ins Leere. Es ist direkt Klage zu erheben.

Regelmäßig belehrt meine Behörde über die erwähnte einmonatige Klageerhebungsfrist, die nur dann zu laufen beginnt, wenn die oder der Beteiligte über den Rechtsbehelf, das Gericht und die einzuhaltende Frist schriftlich oder elektronisch belehrt worden ist, § 58 Abs. 1 VwGO. Soweit eine entsprechende Belehrung in Fällen, auch wegen der Art, des Stadiums und des Inhalts des Verfahrens, unterblieben ist, ist zur Einlegung des Rechtsbehelfs gesetzlich die verlängerte einjährige Frist vorgesehen, vgl. § 58 Abs. 2 Satz 1 VwGO. Im Übrigen richtet sich der Fristlauf zur Klageerhebung, wie in anderen Fällen auch, verwaltungsprozessual nach § 57 Abs. 2 VwGO; §§ 222 Abs. 1, 224 Abs. 2, Abs. 3, 225 f. Zivilprozessordnung (ZPO), §§ 187 ff. Bürgerliches Gesetzbuch (BGB). Die Klage gilt dann als erhoben, wenn die Klageschrift bei Gericht eingeht oder zu Protokoll der Urkundsbeamtin oder des Urkundsbeamten der Geschäftsstelle des Verwaltungsgerichts gegeben worden ist, vgl. § 81 Abs. 1 VwGO.

Was ist zu tun?
In Beschwerdeverfahren gemäß Art. 77 Abs. 1 DSGVO ist betroffenen Personen Klage vor dem Verwaltungsgericht Dresden eröffnet. Die Klagefrist beträgt regelmäßig einen Monat nach Bekanntgabe der Entscheidung, es sei denn, eine Rechtsbehelfsbelehrung ist unterblieben.
Gegen Entscheidungen der Sächsischen Datenschutz- und Transparenzbeauftragten ist der direkte Klageweg eröffnet. Ein Widerspruchsverfahren ist nicht statthaft.

9.2 Löschung personenbezogener Daten auf Anordnung der Aufsichtsbehörde, EuGH-Urteil vom 14. März 2024, C-46/23

↗ Art. 17 Abs. 1, 58 Abs. 2 Buchst. d und g DSGVO

Zurückliegend ist meine Behörde bei der Prüfung von Datenschutzvorgängen im Zusammenhang mit dem Hinweis, dass personenbezogene Daten zu löschen seien, verschiedentlich mit dem Einwand konfrontiert worden, die betroffene Person selbst habe die Löschung nicht beantragt, was aber

für die Löschung notwendig sei. In einem Fall hielt mir dies auch eine größere Stadtverwaltung entgegen. Im Hinblick auf die umfassenden Befugnisse meiner Behörde gemäß Art. 58 Datenschutz-Grundverordnung (DSGVO) stellte sich diese Meinung als rechtsirrig dar.

In einem auf Antrag eines ungarischen Gerichts durchgeführten Vorabentscheidungsverfahrens hatte sich der Europäische Gerichtshof (EuGH) nun mit genau dieser Fragestellung auseinanderzusetzen gehabt.

In seiner Entscheidung vom 14. März 2024 urteilte der Gerichtshof klarstellend, dass Art. 58 Abs. 2 Buchst. d und g DSGVO dahingehend auszulegen sei, dass die Datenschutzaufsichtsbehörde befugt sei, die Löschung unrechtmäßig verarbeiteter personenbezogener Daten anzuordnen, und zwar auch dann, wenn die betroffene Person keinen entsprechenden Antrag gemäß Art. 17 Abs. 1 DSGVO gestellt habe. Nicht entscheidend sei zudem, ob die Daten bei der betroffenen Person selbst oder aus anderen Quellen bezogen worden, vgl. EuGH, Urteil in der Sache C-46/23 vom 14. März 2024, Rn. 54.

Die Entscheidung hat hohe praktische Relevanz in meiner Aufsichtspraxis. Um wirksame Abhilfe bei nicht ordnungsgemäßer personenbezogener Datenverarbeitung herbeizuführen, ist in vielen Fällen eine Löschung der Informationen erforderlich. Meine Behörde ist befugt, auch entsprechende Anordnungen zu treffen.

Was ist zu tun?

Soweit die Löschungsvoraussetzungen eingetreten sind, sollten Verantwortliche von sich aus dem entsprechenden Hinweis der Aufsichtsbehörde oder betroffener Personen folgen und die Löschung umsetzen.

9.3 Verpflichtung der Datenschutzaufsichtsbehörden im Fall eines Verstoßes gegen die DSGVO weitere Abhilfemaßnahmen und Bußgelder zu verhängen – EuGH-Urteil vom 26. September 2024, C-768/21

↗ Art. 57, 58 Abs. 2, 77 Abs. 1 DSGVO, Erwägungsgrund 129

Immer wieder wird meine Behörde seitens betroffener Personen mit der Forderung konfrontiert, Verantwortliche auch zu sanktionieren, selbst in den Fällen, in denen eine nicht ordnungsgemäße personenbezogene Datenverarbeitung von der datenverarbeitenden Stelle beendet wurde oder nicht weiter betrieben wird. Zum Teil wird dabei übersehen, dass die Datenschutzaufsichtsbehörde dem Amtsermittlungsgrundsatz unterliegt, dass sie unvoreingenommen und unparteiisch und am Verhältnismäßigkeitsgrundsatz orientiert zu entscheiden hat.

Auch andere deutsche Aufsichtsbehörden haben sich mit diesem praktisch häufig vorkommenden Verlangen weitergehender Abhilfemaßnahmen gegenüber Verantwortlichen auseinanderzusetzen. In einer Klage gegen die Datenschutzaufsichtsbehörde eines anderen Bundeslandes hatte die Mitarbeiterin eines öffentlich-rechtlichen Kreditinstituts unbefugt auf persönliche Daten von Kunden zugegriffen. Die Sparkasse hatte in der Folge Maßnahmen zur künftigen Vermeidung ergriffen, zwar die betroffene Person nicht informiert, jedoch die zuständige Datenschutzaufsichtsbehörde, die keine weiteren Maßnahmen gemäß Art. 58 Abs. 2 Datenschutz-Grundverordnung (DSGVO) für erforderlich hielt. Das Gericht konnte keine Datenweitergabe an Dritte feststellen. Die nachträgliche doch erfolgte Kenntnisnahme der betroffenen Person von dem Fehlverhalten führte dazu, dass diese die Datenschutzaufsichtsbehörde vor dem Verwaltungsgericht verklagte und Bußgelder gegenüber dem

Kreditinstitut verlangte. Mit Vorabentscheidungsersuchen zur Klärung, inwieweit die Datenschutzaufsichtsbehörde bei festgestelltem Datenschutzverstoß verpflichtet ist, Abhilfemaßnahmen gemäß Art. 58 Abs. 2 DSGVO zu ergreifen, wandte sich das mit der Klage befasste Verwaltungsgericht an den Europäischen Gerichtshof (EuGH), vgl. zum Sachverhalt den Entscheidungstext des Urteils des EuGH vom 26. September 2024, Rn. 14 bis 23.

In seiner Entscheidung führte der Gerichtshof aus, dass jede Aufsichtsbehörde nach Art. 57 Abs. 1 Buchst. f DSGVO verpflichtet sei, sich im Rahmen ihrer Zuständigkeit mit Beschwerden zu befassen, die jede Person gemäß Art. 77 Abs. 1 DSGVO einreichen kann, wenn sie der Ansicht ist, dass eine Verarbeitung sie betreffender personenbezogener Daten gegen diese Verordnung verstoße, den Beschwerdegegenstand in angemessenem Umfang zu untersuchen und der Beschwerdeführerin oder den Beschwerdeführer innerhalb einer angemessenen Frist über den Fortgang und das Ergebnis der Untersuchung zu unterrichten und die Aufsichtsbehörde habe eine solche Beschwerde mit aller gebotenen Sorgfalt zu bearbeiten. Ferner verwies das Gericht auf die Untersuchungsbefugnisse gemäß Art. 58 Abs. 1 DSGVO, vgl. Urteil a. a. O., Rn. 32 und 33.

Letztendlich stellte der Gerichtshof aber fest, dass Art. 57 Abs. 1 Buchst. a und f, Art. 58 Abs. 2 sowie Art. 77 Abs. 1 der Datenschutz-Grundverordnung dahingehend auszulegen seien, dass die Aufsichtsbehörde im Fall der Feststellung einer Verletzung des Schutzes personenbezogener Daten nicht verpflichtet sei, „nach Art. 58 Abs. 2 eine Abhilfemaßnahme zu ergreifen, insbesondere eine Geldbuße zu verhängen, wenn ein solches Einschreiten nicht geeignet, erforderlich oder verhältnismäßig" sei, „um der festgestellten Unzulänglichkeit abzuhelfen und die umfassende Einhaltung dieser Verordnung zu gewährleisten", vgl. das Urteil a. a. O., Rn. 50 f.

Meine Behörde wird sich an der Entscheidung orientieren, sie sieht sich aber auch in ihrer bisherigen Entscheidungspraxis bestätigt. In der Vergangenheit hatte sie betroffene Personen, die entgegen den Maßnahmen meiner Dienststelle

Was ist zu tun?
Als Sächsische Datenschutz- und Transparenzbeauftragte bin ich nicht verpflichtet, in jedem Fall eines Verstoßes gegen die DSGVO eine Abhilfemaßnahme zu ergreifen, insbesondere eine Geldbuße zu verhängen.

weitergehende Abhilfe verlangten, immer wieder auf Erwägungsgrund 129 der Datenschutz-Grundverordnung, auf den auch in der genannten Entscheidung referenziert wird, hingewiesen. In Anbetracht der bestehenden Ressourcen meiner Behörde sei diese zum einen gehalten, Verfahren innerhalb einer angemessenen Frist zu erledigen, vgl. Satz 4 des Erwägungsgrundes. Nach Satz 5 komme hinzu, dass zu ergreifende Maßnahmen im Hinblick auf die Gewährleistung der Einhaltung der Datenschutz-Grundverordnung erforderlich und verhältnismäßig zu sein hätten.

9.4 Zur Pflicht der Verantwortlichen bei Betriebs- und Dienstvereinbarungen – vgl. EuGH-Urteil vom 19. Dezember 2024, C 65/23

↗ Art. 5, Art. 6 Abs. 1 sowie Art. 9 Abs. 1 und 2, Art. 82 Abs. 1, Art. 88 Abs. 1 und 2 DSGVO

Wiederkehrend hat sich meine Behörde im Kontext des Beschäftigtendatenschutzes mit Regelungen in Dienstvereinbarungen und Betriebsvereinbarungen bei öffentlichen und nichtöffentlichen Stellen auseinanderzusetzen gehabt. Häufig hat sich dabei die Frage gestellt, welche konstitutive normative Wirkung die kollektivrechtlichen Bestimmungen haben bzw. ob man sich auf diese personenbezogene Datenverarbeitung im Sinne einer Rechtsgrundlage selbstständig stützen kann. Regelmäßig hat sich meine Behörde in beschäftigtendatenschutzrechtlichen Fragen dahingehend positioniert, dass unter Beachtung normenhierarchischer Überlegungen übergeordnete Vorschriften in Gesetzen einzuhalten sind. Durch den Europäischen Gerichtshof (EuGH) sehe ich die langjährige Praxis meiner Behörde bestätigt.
In einem durch das Bundesarbeitsgericht angestoßenen Vorabentscheidungsverfahren zur Auslegung von Art. 82 Abs. 1, Art. 88 Abs. 1 und 2 in Verbindung mit Art. 5, Art. 6

Abs. 1 sowie Art. 9 Abs. 1 und 2 der Datenschutz-Grundverordnung (DSGVO) hat sich der EuGH mit Urteil vom 19. Dezember 2024 - C 65/23 - zu dieser grundsätzlichen Frage festgelegt.

Danach sollen Betriebsvereinbarungen keine Umgehung der Verpflichtungen des Verantwortlichen bewirken können. Anderenfalls würde, so der Gerichtshof, das Ziel der Datenschutz-Grundverordnung, ein hohes Schutzniveau für die Beschäftigten im Fall der Verarbeitung ihrer personenbezogenen Daten im Beschäftigungskontext sicherzustellen, beeinträchtigt, vgl. EuGH, Urteil vom 19.12.2024 - C 65/23, Rn. 42. Insoweit hätten Betriebsvereinbarungen den allgemeinen Anforderungen der Art. 5 , Art. 6 Abs. 1 sowie Art. 9 Abs. 1, 2 DSGVO zu genügen, was auch das gesetzliche Merkmal der Erforderlichkeit einschließt, vgl. EuGH a. a. O., Rn. 22, 23, 43 und der Leitsatz unter Rn. 62.

Im Ergebnis verfügten, so das Gericht, Betriebsparteien über einen eng umgrenzten Spielraum, der nicht dazu führen dürfe, dass die Voraussetzung der Erforderlichkeit weniger streng angewandt oder gar darauf verzichtet werde. Auch konkret darauf bezogen, gebe es eine umfassende gerichtliche Kontrolle, vgl. EuGH a. a. O., Rn. 51 ff., insbesondere Rn. 60 und der zweite Leitsatz unter Rn. 62.

Die Entscheidung ist auf Dienstvereinbarungen, also kollektivrechtliche Vereinbarungen, bei öffentlichen Stellen, übertragbar. Meine Behörde wird daher die Frage der Erforderlichkeit bei solchen Vereinbarungen wie bisher in den Mittelpunkt der Prüfung stellen.

Was ist zu tun?

Betriebs- und Dienstvereinbarungen sind an den gesetzlichen Voraussetzungen zu bemessen, der Datenschutz-Grundverordnung und ergänzenden datenschutzgesetzlichen Vorschriften.

9.5 Zum Begriff der „Gesundheitsdaten" – EuGH-Urteil vom 4. Oktober 2024, C-21/23

Neben wettbewerbsrechtlichen Gesichtspunkten hat der Europäische Gerichtshof eine für die Arzneimittelvertriebspraxis bedeutsame Entscheidung getroffen.

Auch in meinem Zuständigkeitsbereich sind Onlineapotheken ansässig. Das diesbezügliche Beschwerdeaufkommen ist über die Berichtszeiträume gesehen nicht unbeträchtlich.

Bei der Rechtssache ging es um einen Streit zwischen zwei Apotheken aus der Bundesrepublik. Eine der Apotheken verkaufte apothekenpflichtige, aber rezeptfreie Medikamente über die Verkaufsplattform eines großen Onlinehändlers im Internet. Die andere Apotheke reichte hiergegen als Wettbewerberin (und Dritter) Klage ein und vertrat die Rechtsmeinung, dass die Kundendaten des Wettbewerbers nur mit datenschutzrechtlicher Einwilligung hätten erhoben werden können. Bei den personenbezogenen Daten ging es konkret um die verarbeiteten Namensangaben, die Anschrift bzw. Lieferadresse und die pharmazeutischen Produkte und die Frage, ob es sich hierbei um Gesundheitsdaten im Sinne von Art. 9 Datenschutz-Grundverordnung (DSGVO) handelt. Der Europäische Gerichtshof (EuGH) bejahte diese Frage, da die Kundendaten selbst bei Standardarzneimitteln geeignet seien, Aufschluss über die Gesundheit der Kunden zu geben, vgl. EuGH, Urteil vom 04.10.2024, C-21/23, Rn. 78 bis 80. Der Begriff der Gesundheitsdaten sei weit auszulegen und der indirekte Bezug genüge, EuGH a. a. O., Rn. 81, 82. Den Umstand, dass die frei verfügbaren Arzneimittel nicht für eine bestimmte Person, nämlich die Käuferin oder dem Käufer, bestimmt seien, hielt das Gericht im Ergebnis nicht für entscheidend, EuGH a. a. O, Rn. 88 ff. Schlussfolgernd setzt das Gericht gemäß Art. 9 Abs. 2 Buchst. a DSGVO die erfolgte ausdrückliche Einwilligung voraus, vgl. EuGH a. a. O., Rn. 93 sowie Rn. 9 und 27. Der besondere Umstand, dass sich die

Kundin oder der Kunde über die Plattform des internationalen Onlinehändlers anmeldet und die personenbezogene Datenverarbeitung zu ihrer oder seiner Person selbst bewusst durch seine Eintragungen veranlasst, spielte in den Überlegungen des Gerichts keine Rolle. Insoweit werden zukünftig in gleichgelagerten Fällen bei Gesundheitsdaten Onlineplattformen gehalten sein, entsprechende elektronische Prozessschritte für eine ausdrückliche Einwilligung vorzusehen, soweit kein anderer Ausnahmetatbestand in Betracht kommt. Offen bleibt nach dem Urteil, inwieweit die Entscheidung auch auf andere mögliche nach Art. 9 Abs. 1 DSGVO zu schützende Bezüge bei Internet-Geschäftsprozessen zu übertragen ist, etwa bei dem Verkauf von religiösen Artikeln, politischen Büchern oder Erotikartikeln über das Internet.

Neben der inhaltlichen datenschutzrechtlichen Entscheidung ist anzumerken, dass der Gerichtshof auch geurteilt hat, dass Verstöße gegen die Datenschutz-Grundverordnung von Wettbewerbern angegriffen werden können, soweit nationales Recht dies gestattet, vgl. EuGH a. a. O., Rn. 95, erster Leitsatz.

Was ist zu tun?

Der Begriff der „Gesundheitsdaten" ist nach dem EuGH weit zu verstehen. Soweit Gesundheitsdaten verarbeitet werden, haben Onlinehändler eine nach der DSGVO ordnungsgemäße Einwilligung vorzusehen.

Notizen

Herausgeberin
Sächsische Datenschutz- und Transparenzbeauftragte
Dr. Juliane Hundert
Maternistraße 17
01067 Dresden
Postanschrift: Postfach 11 01 32, 01330 Dresden
Telefon 0351/85471-101
Telefax 0351/85471-109
post@sdtb.sachsen.de
www.datenschutz.sachsen.de

Fotos
Titelbild: ©gremlin – istockphoto.com
Weitere Fotos: ronaldbonss.com (Seite 4), SDTB (Seite 167 o.), Christian Bluem (Seite 167 u.), HBDI (Seite 169)

Druck
siblog – Gesellschaft für Dialogmarketing, Fulfillment & Lettershop mbH

Auflage
1.000 Exemplare

Bezug
kostenlos
Zentraler Broschürenversand der Sächsischen Staatsregierung
Hammerweg 30
01127 Dresden
Telefon: +49 351 210-3671/-3672
publikationen@sachsen.de
www.publikationen.sachsen.de

Verteilerhinweis
Dieser Tätigkeitsbericht wird aufgrund der Verpflichtung nach Artikel 59 Datenschutz-Grundverordnung herausgegeben. Er darf weder von politischen Parteien noch von deren Kandidatinnen und Kandidaten oder deren Helferinnen und Helfern zum Zwecke der Wahlwerbung verwendet werden. Dies gilt für alle Wahlen. Missbräuchlich ist insbesondere die Verteilung auf Wahlveranstaltungen, an Informationsständen der Parteien sowie das Einlegen, Aufdrucken oder Aufkleben parteipolitischer Informationen oder Werbemittel. Untersagt ist auch die Weitergabe an Dritte zur Verwendung bei der Wahlwerbung.