Tätigkeitsbericht Datenschutz

Berichtszeitraum:
1. Januar bis 31. Dezember 2022

Meine Daten.
Meine Freiheit.

SÄCHSISCHE
DATENSCHUTZ- UND
TRANSPARENZBEAUFTRAGTE

Freistaat
SACHSEN

Tätigkeitsbericht Datenschutz 2022 der Sächsischen Datenschutz- und Transparenzbeauftragten

Berichtszeitraum:
1. Januar bis 31. Dezember 2022

Rechtsstand: 31. Dezember 2022

Liebe Leserinnen und Leser,

was macht eigentlich eine Datenschutzbeauftragte? Das wurde ich im ersten Jahr meiner Amtszeit als Sächsische Datenschutzbeauftragte häufiger gefragt – bei Veranstaltungen oder im privaten Umfeld. Dabei habe ich die Erfahrung gemacht, dass ganz unterschiedliche Vorstellungen von der Aufgabe „Datenschutz" verbreitet sind. Sammelt die Datenschutzbeauftragte alle Daten und passt auf sie auf? Welche „Daten" schützt sie?

Wenn ich erkläre, dass es um die ganz persönlichen Daten einer oder eines jeden Einzelnen geht und dass meine Aufgabe ist, staatliche Stellen oder Unternehmen darauf hinzuweisen, mit diesen Daten rechtmäßig und sorgsam umzugehen, dann ernte ich nicht selten eine freudige Reaktion. Den Menschen wird bewusst, dass sie mit mir und meiner Behörde jemanden haben, der für ihre Grundrechte eintritt und an den sie sich wenden können, wenn ihr Recht auf informationelle Selbstbestimmung beschränkt wird. Und den Bürgerinnen und Bürgern wird auch bewusst, dass sie in ihrer Freiheit und in ihrem Persönlichkeitsrecht beschränkt werden, wenn sie permanenter Überwachung ausgesetzt sind und keine Kontrolle mehr über ihre Daten haben.

Gerade deshalb müssen wir den Datenschutz im Zuge der Digitalisierung von Anfang an mitdenken. Mit „wir" meine ich vor allem die datenschutzrechtlich Verantwortlichen in Unternehmen und Behörden, aber auch die betroffenen Personen, die achtsamer mit (ihren) personenbezogenen Daten umgehen sollten, Stichwort: Selbstdatenschutz. Tatsächlich sind viele Vorgänge, mit denen ich mich im zurückliegenden Jahr befasst habe, darauf zurückzuführen, dass datenschutzrechtliche Aspekte im Vorfeld zu wenig berücksichtigt wurden. Der Betrieb von Facebook-Fanpages durch öffentliche Stellen ist ein Beispiel dafür. Bereits mein Amtsvorgänger riet frühzeitig von diesem Netzwerk ab, weil die Hürden für einen rechtskonformen Betrieb zu hoch liegen. Die Rechtsprechung und ein 2022 veröffentlichtes Gutachten der Datenschutzkonferenz

stützen diese Einschätzung. Es ist also für Verantwortliche höchste Zeit, sich von Facebook zu verabschieden und auf datenschutzfreundliche Alternativen zu setzen. Meiner Behörde können Sie zum Beispiel bei Mastodon folgen.

Um die mit der Digitalisierung verbundenen Chancen zu nutzen und Risiken zu vermeiden, müssen die informationstechnischen Systeme datenschutzgerecht gestaltet sein. Bei Websites ist das aus unterschiedlichen Gründen oftmals nicht der Fall. Die Praxis zeigte auch im vergangenen Jahr, dass viele Verantwortliche auf ihrer Website Dienste einbinden, die rechtswidrig personenbezogene Daten von Nutzerinnen und Nutzern verarbeiten. Mit diesen Daten können komplexe Persönlichkeitsprofile erstellt werden. Besonders problematisch ist dabei, dass diese Datenverarbeitung meist im Verborgenen geschieht, ohne dass Bürgerinnen und Bürger davon etwas bemerken.

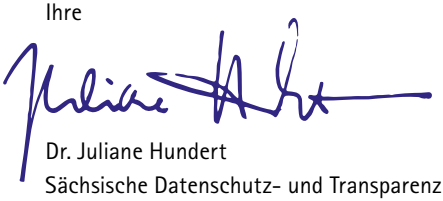
Wer also eine Website betreibt, sollte genau darauf achtgeben, welche Dienste im eigenen Internetauftritt eingebunden sind. Mehrere Beiträge in diesem Jahresbericht geben Tipps und Hinweise, was dabei datenschutzrechtlich zu berücksichtigen ist.

Außerdem hat sich im Berichtszeitraum vieles um den Schutz und die Verarbeitung von Gesundheitsdaten gedreht, beispielsweise um den Auskunftsanspruch bei Patientenakten oder die Übermittlung von Gesundheitsdaten an Inkassounternehmen. Auch die ergriffenen Maßnahmen zur Corona-Pandemie waren Anfang des Jahres 2022 noch ein Thema. Ich denke dabei an die einrichtungsbezogene Impfpflicht, an Werbung für die Corona-Schutzimpfung oder die Anerkennung einer Covid-19-Infektion als Berufskrankheit. Glücklicherweise hat sich die pandemische Lage entspannt, sodass auch die Eingaben mit Bezug zu Corona-Maßnahmen rückläufig waren. Es bleibt also zu hoffen, dass sämtliche coronabedingte Grundrechtseingriffe 2023 endgültig der Vergangenheit angehören können.

Hinzu kamen viele weitere Vorgänge aus anderen Bereichen, in denen Datenschutz besonders von Bedeutung ist, unter anderem im Zusammenhang mit Beschäftigten, in der Justiz und

bei der Polizei. Schon beim Überfliegen des Inhaltsverzeichnisses bekommen Sie einen ersten Eindruck von der Themenvielfalt. Sicherlich stoßen Sie dabei auf den einen oder anderen Beitrag, der Ihnen im Beruflichen oder Privaten weiterhilft.
Abschließend – und das ist mir ein wichtiges Anliegen – bedanke ich mich bei den Abgeordneten des Sächsischen Landtags sowie bei meinen Mitarbeiterinnen und Mitarbeitern für das Engagement und die ausgiebige Unterstützung in meinem ersten Amtsjahr. Ohne sie könnte ich meine vom Gesetzgeber zugewiesene Funktion als Grundrechtsschützerin nicht ausfüllen. Ebenso bedanke ich mich bei allen, die sich für die Einhaltung und Stärkung des Datenschutzes in Sachsen engagieren.
Liebe Leserinnen und Leser, der Datenschutz schützt Ihre Grundrechte und Ihre Freiheit. In diesem Sinne soll der vorliegende Tätigkeitsbericht Sie dabei unterstützen.

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
BauGB	Baugesetzbuch
BDSG	Bundesdatenschutzgesetz
BeamtStG	Beamtenstatusgesetz
BGB	Bürgerliches Gesetzbuch
BKV	Berufskrankheitenverordnung
BMG	Bundesmeldegesetz
BZRG	Bundeszentralregistergesetz
DGUV	Deutsche Gesetzliche Unfallversicherung
DSGVO	Datenschutz-Grundverordnung
GewO	Gewerbeordnung
GG	Grundgesetz für die Bundesrepublik Deutschland
GwG	Geldwäschegesetz
HGB	Handelsgesetzbuch
IfSG	Infektionsschutzgesetz
KomWG	Kommunalwahlgesetz
KunstUrhG	Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie
MsRG	Mietspiegelreformgesetz
MsV	Mietspiegelverordnung
OWiG	Gesetz über Ordnungswidrigkeiten
PAuswG	Personalausweisgesetz
SächsBG	Sächsisches Beamtengesetz
SächsDG	Sächsisches Disziplinargesetz
SächsDSG	Sächsisches Datenschutzgesetz
SächsDSDG	Sächsisches Datenschutzdurchführungsgesetz
SächsDSUG	Sächsisches Datenschutz-Umsetzungsgesetz
SächsEGovG	Sächsisches E-Government-Gesetz

SächsGAVO	Sächsische Gutachterausschussverordnung
SächsGemO	Sächsische Gemeindeordnung
SächsGVBl	Sächsisches Gesetz- und Verordnungsblatt
SächsJVollzDSG	Sächsisches Justizvollzugsdatenschutzgesetzs
SächsLKrO	Sächsische Landkreisordnung
SächsMeldVO	Sächsische Meldeverordnung
SächsMsZustG	Sächsisches Mietspiegel-Zuständigkeitsgesetz
SächsPolG	Polizeigesetz des Freistaates Sachsen
SächsPVDG	Sächsisches Polizeivollzugsdienstgesetz
SächsSchulG	Sächsisches Schulgesetz
SächsStatG	Sächsisches Statistikgesetz
SächsVerf	Verfassung des Freistaates Sachsen
SächsVwVfZG	Gesetz zur Regelung des Verwaltungsverfahrens- und des Verwaltungszustellungsrechts für den Freistaat Sachsen
SächsVwVG	Verwaltungsvollstreckungsgesetz für den Freistaat Sachsen
SchfHwG	Schornsteinfeger-Handwerksgesetz
SGB	Sozialgesetzbuch
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
TKG	Telekommunikationsgesetz
TTDSG	Telekommunikation-Telemedien-Datenschutz-Gesetz
UklaG	Gesetze über Unterlassungsklagen bei Verbraucherrechts- und anderen Verstößen
UmwG	Umwandlungsgesetz
UWG	Gesetz gegen den unlauteren Wettbewerb
VVG	Versicherungsvertragsgesetz
VwGO	Verwaltungsgerichtsordnung
VwVfG	Verwaltungsverfahrensgesetz
VwZG	Verwaltungszustellungsgesetz
WEG	Wohnungseigentumsgesetz
ZensG	Zensusgesetz 2022

Sonstiges

Abs.	Absatz
Alt.	Alternative
AKES	Automatisiertes Kennzeichenerkennungssystem
Art.	Artikel

Az.	Aktenzeichen
BfDI	Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
BGH	Bundesgerichtshof
BK	Berufskrankheit
BSI	Bundesamt für Sicherheit in der Informationstechnik
Buchst.	Buchstabe
BVerfG	Bundesverfassungsgericht
BVerfGE	Bundesverfassungsgerichtsentscheidung
BVerwG	Bundesverwaltungsgericht
BVerwGE	Bundesverwaltungsgerichtsentscheidung
DAD	DNA-Analyse-Datei
DGUV	Deutsche Gesetzliche Unfallversicherung
DSFA	Datenschutz-Folgenabschätzung
DSK	Konferenz der unabhängigen Datenschutzbeauftragten des Bundes und der Länder – Datenschutzkonferenz
EDSA	Europäischer Datenschutzausschuss
EGBGB	Einführungsgesetz zum Bürgerlichen Gesetzbuche
EU	Europäische Union
EuGH	Europäischer Gerichtshof
IMI	Internal Market Information System
LaSuB	Landesamt für Schule und Bildung
LG	Landgericht
LT-Drs.	Landtags-Drucksache
m. w. N.	mit weiteren Nachweisen
OLG	Oberlandesgericht
OVG	Oberverwaltungsgericht
PD	Polizeidirektion
Rn.	Randnummer
Rdnr.	Randnummer
Rs.	Rechtssache
SK	Sächsische Staatskanzlei
SMI	Sächsisches Staatsministerium des Innern
stRspr	Ständige Rechtsprechung
UG	Unternehmergesellschaft
VG	Verwaltungsgericht
VwV	Verwaltungsvorschrift

Sachgebietsregister

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

Verzeichnis von Verarbeitungstätigkeiten, Kooperationspflicht	6.3.1
Videografie und Bildverarbeitung	
• Behördliche Überwachung/Verarbeitung*	
• Beschäftigte, vgl. ansonsten Beschäftigtendatenschutz	2.2.21
• Dashcam, Drohnen	2.2.19
• Handel, Gewerbe	6.4.4
• Wohnbereiche	
• Sonstiges, Allgemeines	2.2.20, 2.2.22, 6.1.1, 6.4.4
Wahlrecht*	vgl. 2.2.1
Zertifizierung, Akkreditierungen, Prüfsiegel	

Richtlinie (EU) 2016/680

Polizei*	6.4.1, 8.4, 8.5, 8.6, 8.7
Ordnungswidrigkeitenbehörden*	6.4.1, 8.2
Strafverfolgung*	8.3, 8.8
Straf- und Justizvollzug*	8.1

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

Sächsischer Landtag als Parlament	
Verfassungsschutz	
Weitere datenverarbeitende Stellen	

1 Datenschutz im Freistaat Sachsen

1.1 Untersagung des Facebook-Auftritts der Sächsischen Staatskanzlei

↗ § 25 Abs. 1 Satz 1 TTDSG, Art. 26 Abs. 1 DSGVO

Facebook steht für seine intransparente Datenverarbeitung schon seit Langem in der Kritik. Dennoch wird die Plattform nicht nur von Unternehmen und Vereinen, sondern auch von etlichen öffentlichen Stellen gern als Kommunikationsinstrument genutzt. Datenschutzrechtlich halte ich das für unzulässig – sofern die Verantwortlichen keinen Nachweis für die rechtskonforme Nutzung erbringen können. Der Sächsischen Staatskanzlei (SK) beabsichtige ich deshalb, den Betrieb ihres Facebook-Auftritts zu untersagen. In einer Anhörung vom 9. August 2022 habe ich ihr bis zum 31. Oktober 2022 Gelegenheit gegeben, sich zur Sache zu äußern und im Übrigen das Folgende ausgeführt:

Die SK betreibt bis heute einen eigenen Auftritt bzw. eine sogenannte „Fanpage" bei Facebook. Auf dieser Seite informiert sie regelmäßig Nutzer und Nichtnutzer von Facebook über aktuelle politische Tätigkeiten in Form von Bildern, Videos und Textbeiträgen. Bei der Nutzung einer solchen Fanpage wurde im Berichtszeitraum auch die Funktion „Insights" verwendet, durch die der jeweilige Fanpage-Betreiber Statistiken zu Besucherzahlen, „Gefällt mir"-Angaben, Demografie der Besucher und der Reichweite seiner Beiträge erhält. Durch seine jeweiligen Einstellungen kann der

Fanpage-Betreiber die Intensität der erhaltenen Statistiken erhöhen oder verringern.

Die Statistiken ermöglichen dem Fanpage-Betreiber unter anderem, seine Inhalte anzupassen, indem sie den Erfolg oder Misserfolg von Postings und Informationskampagnen des Fanpage-Betreibers sichtbar machen, also wie viel Aufmerksamkeit oder weniger Aufmerksamkeit diese bei den Nutzern erzeugt haben. Hierdurch kann der Fanpage-Betreiber seine Postings und Informationskampagnen so ausrichten, dass ihre Reichweite auf der Facebook-Plattform erhöht wird. Zugleich hängt von der Sammlung und Auswertung der Nutzeraktivität auf der Fanpage und den von Facebook erstellten Nutzungsprofilen der Nutzer ab, ob Inhalte auch anderen Nutzern, die die Fanpage bisher nicht besucht haben, aber in dasselbe Profil passen wie jene Nutzer, welche dies getan haben, von Facebook vorgeschlagen werden. Facebook verknüpft diese Daten zu weiteren personenbezogenen Daten der Nutzer, insbesondere auch zu anderen Plattformen des Unternehmens und anderen Websites, die in das Werbenetzwerk des Unternehmens integriert sind. Auch hierdurch wird die Reichweite von Fanpages auf der Plattform beeinflusst. Darüber hinaus verwendet Facebook die gesammelten Daten der Nutzer für sein Werbenetzwerk, aus dem der wesentliche Umsatz seines Geschäftsmodells generiert wird.

Für die dafür genutzten Cookies ist eine Einwilligung des Nutzers erforderlich; die im Einwilligungsbanner vorab erteilten Informationen genügen jedoch den Anforderungen an eine informierte Einwilligung gemäß Art. 4 Nr. 11 und Art. 7 Abs. 3 Satz 3 DSGVO nicht. Bereits am 5. Juni 2018 entschied der Europäische Gerichtshof (EuGH) in der Rechtssache „Wirtschaftsakademie" (Rs. C-210/16), dass der Betreiber einer Facebook-Fanpage, also auch die Sächsische Staatskanzlei, dabei als gemeinsam Verantwortlicher im Sinne des Art. 26 Abs. 1 DSGVO mit Facebook (das sich am 28. Oktober 2021 in Meta umbenannt hat) anzusehen ist.

Nach meinen bisherigen Feststellungen hat die SK somit zum einen fahrlässig gegen ihre Rechenschaftspflicht nach

Art. 5 Abs. 2 DSGVO verstoßen, indem sie entgegen der gebotenen Sorgfalt ihren Facebook-Auftritt betrieben hat, ohne die Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten nach Art. 5 Abs. 1 DSGVO nachweisen zu können. Zum anderen hat sie fahrlässig gegen § 25 Abs. 1 Satz 1 Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) verstoßen, indem auf dem von der SK betriebenen Facebook-Auftritt ohne Erfüllung der Rechtsgrundlagen Informationen in den Endeinrichtungen der Endnutzer gespeichert werden und auf Informationen, die bereits in den Endeinrichtungen der Endnutzer gespeichert sind, zugegriffen wird. Schließlich hat die SK fahrlässig gegen Art. 5 Abs. 1 Buchst. a DSGVO verstoßen, indem auf dem von der Sächsischen Staatskanzlei betriebenen Facebook-Auftritt personenbezogene Daten erhoben und an Meta übermittelt werden, obwohl hierfür keine wirksame Rechtsgrundlage gegeben ist.

Mit Schreiben vom 12. Oktober 2022 nahm die SK erstmalig Stellung und bat um Fristverlängerung bis 31. Januar 2023. Sie teilte weiterhin mit, dass sie die Funktion „Insights" deaktiviert habe. Zudem regte sie an, das Verfahren bis zu einem Abschluss des Verfahrens des BfDI gegen das Bundespresseamt nicht weiter zu betreiben. Dieser hatte bereits am 17. Mai 2022 das Bundespresseamt wegen einer beabsichtigten Untersagung des Weiterbetriebs des Facebook-Auftritts der Bundesregierung ein Anhörungsschreiben übersandt. Vorausgegangen war ein Kurzgutachten der Datenschutzkonferenz vom 18. März 2022 zur datenschutzrechtlichen Konformität des Betriebs von Facebook-Fanpages, über das ich den Ministerpräsidenten des Freistaates Sachsen mit Schreiben vom 1. April 2022 informierte. Dieses wurde mittlerweile am 10. November 2022 unter Berücksichtigung des seit dem 1. Dezember 2021 geltenden Telekommunikation-Telemedien-Datenschutzgesetzes (TTDSG), des Urteils des Oberverwaltungsgerichts Schleswig vom 25. November 2021 (Az. 4 LB 20/13) und der aktuellen tatsächlichen Umsetzungen bei Facebook aktualisiert. In diesem wird unter anderem ausgeführt, dass auch bei

Aktualisiertes Kurzgutachten der DSK zu Facebook-Fanpages:
↗ sdb.de/tb2201

abgeschalteter „Insights"-Funktion zumindest für die nachgelagerte Datenverarbeitung auf Basis des Setzens und Auslesens von Cookies eine gemeinsame Verantwortlichkeit mit Meta besteht.

Was ist zu tun?
Öffentliche Stellen sollten angesichts der dargestellten datenschutzrechtlichen Bedenken ihren Facebook-Fanpage-Auftritt einstellen.

In meiner Antwort gewährte ich die Fristverlängerung und bat um eine detaillierte Darlegung der Deaktivierung der „Insights"-Funktion, da ich keine Möglichkeit habe, diese nachzuvollziehen. Ich werde in meinem nächsten Tätigkeitsbericht über den Fortgang berichten.

1.2 Zensus 2022: Kontrolle einer Erhebungsstelle

↗ SächsZensAG, ZensG

Im Mai 2022 startete in Sachsen mit dem Zensus 2022 erneut eine große Bevölkerungs-, Gebäude- und Wohnungszählung. Das Statistische Landesamt war für die Durchführung des Zensus zuständig.

Die gesetzliche Grundlage bildete insbesondere das vom Bundesgesetzgeber verabschiedete Zensusgesetz 2022, wonach für Befragte eine Auskunftspflicht bestand.

Weiterhin enthielt das Gesetz detaillierte Regelungen zum Datenschutz und zur Datenverarbeitung. Befragte Personen hatten beim Zensus zum Beispiel Angaben zu ihrer Wohnsituation, zur Bildung und Erwerbstätigkeit zu machen. Ein Teil der Erhebung war die Haushaltebefragung. Dabei nahmen Beauftragte des Statistischen Landesamts auch persönlich Kontakt zu den auskunftspflichtigen Personen auf.

Im Juni führte ich anlässlich des Zensus 2022 eine angekündigte Vor-Ort-Kontrolle in einer Erhebungsstelle durch. Die Kontrolle betraf maßgeblich die im Sächsischen Zensusausführungsgesetz festgelegten Anforderungen bei der Durchführung des Zensus. Ich habe dabei insbesondere die statistikrechtlichen Anforderungen der Abschottung durch Begehung der Erhebungsstelle geprüft; dies in räumlicher, personeller und verfahrenstechnischer Hinsicht. Auch Fragen zum Einsatz der Erhebungsbeauftragten waren Gegenstand der Vor-Ort-Kontrolle. Dabei wurde unter anderem die

Bestellung zur bzw. zum ehrenamtlichen Erhebungsbeauftragten sowie deren Belehrung und Einsatz stichprobenhaft überprüft, ferner die Übergabe und die Prüfung der Erhebungsdokumente, die Erfassung im Erhebungssystem sowie die Aufbewahrung der Fragebögen in der Erhebungsstelle.
Bei der Kontrolle vor Ort wurden keine datenschutzrechtlichen Mängel in der Erhebungsstelle festgestellt.
Im Nachgang der Kontrolle erfolgte, wie beim Termin erbeten, noch die Übersendung schriftlicher Unterlagen. Diese umfassten beispielsweise die Dienstanweisung über die Einrichtung und den Betrieb der örtlichen Erhebungsstelle für den Zensus 2022, die Niederschrift über die Belehrung über die statistische Geheimhaltung und das Datengeheimnis sowie eine Postordnung mit Anweisungen zum Umgang mit Post, welche an die Erhebungsstelle adressiert war.
Die Auswertung der vorgelegten Unterlagen ergab ebenfalls keinen weiteren Handlungsbedarf.
Daher konnte ich den Kontrollvorgang zeitnah abschließen. Mein herzlicher Dank galt allen Verantwortlichen für die engagierte und kompetente Unterstützung im Rahmen der Kontrolle.

1.3 Querschnittskontrollen bei Kommunen

↗ Art. 7 DSGVO, VwV Schulformulare

In der Vergangenheit hat meine Behörde regelmäßig Querschnittskontrollen bei Kommunen durchgeführt. Pandemiebedingt wurden diese Überprüfungen in den vergangenen Jahren ausgesetzt. Ich kann nun berichten, dass ich – auch dank einer verbesserten Personalsituation – meine Kontrolltätigkeit zunächst in einer Großen Kreisstadt wiederaufgenommen habe.
Vorrangig habe ich dabei Bürger- und Ratsinformationssysteme, Videoüberwachung, Bekanntmachungen und Veröffentlichungen im Internet sowie die Verarbeitung von Beschäftigtendaten und die Informationssicherheit überprüft. Diese Schwerpunkte resultieren aus der Anzahl von Peti-

tionen und Anfragen, die mich dazu insbesondere nach der Kommunalrechtsnovelle (vgl. 2.2.2) erreichten. Bei künftigen Kontrollen können die Schwerpunkte durchaus anders liegen. Im Ergebnis stellte ich bei der Kontrolle keine (wesentlichen) Verstöße fest, sodass ich den Fokus mehr auf die Beratung richten konnte. Zudem bestätigte sich mein Eindruck, dass mit Inkrafttreten der Datenschutz-Grundverordnung der Datenschutz auch in den Kommunalverwaltungen einen deutlich höheren Stellenwert erhalten hat.

1.4 Versand von Werbeschreiben für die Corona-Schutzimpfung

↗ Art. 6 Abs. 1 DSGVO, SächsMeldVO

Im Frühjahr des Jahres 2022 erreichten mich Anfragen zu einem Schreiben, unterzeichnet von der Staatsministerin für Soziales und Gesellschaftlichen Zusammenhalt und dem Ministerpräsidenten, in welchem zur Teilnahme an der Corona-Schutzimpfung geworben wurde. Für die Betroffenen war aus dem Schreiben ersichtlich, dass ihre Daten aus dem Einwohnermelderegister gezogen worden waren.

Ich habe dieses Vorhaben, in welches ich seitens des Sächsischen Staatsministeriums des Innern im Vorfeld einbezogen worden war, folgendermaßen bewertet.

Voraussetzung für den Versand der Werbeschreiben war zunächst die Schaffung einer entsprechenden normenklaren Regelung in der Sächsischen Meldeverordnung (SächsMeldVO), die wie folgt gefasst wurde:

> „§ 11a
> Regelmäßige Datenübermittlungen an das Sächsische Staatsministerium für Soziales und Gesellschaftlichen Zusammenhalt zur Unterstützung von Corona-Schutzmaßnahmen
> (1) [1]Zur Erhöhung der Impfbereitschaft im Rahmen der Durchführung von Schutzimpfungen gegen das Coronavirus SARS-CoV-2 durch Impfaufforderungen an die Personen, die älter als 60 Jahre sind, erstellt

und versendet ein Dienstleister individuell adressierte Schreiben des Sächsischen Staatsministeriums für Soziales und Gesellschaftlichen Zusammenhalt an den entsprechenden Personenkreis. [2]Zu diesem Zweck ist dem Dienstleister der Datensatz nach Absatz 2 von der Sächsischen Anstalt für kommunale Datenverarbeitung zu übermitteln. [3] Die Datenübermittlung ist vierteljährlich in Bezug auf die Personen, die zwischenzeitlich das 60. Lebensjahr vollendet haben, zu ergänzen. [4] Der Dienstleister ist vom Sächsischen Staatsministerium für Soziales und Gesellschaftlichen Zusammenhalt nach den einschlägigen vergaberechtlichen Bestimmungen auszuwählen und auf die Einhaltung der datenschutzrechtlichen Regelungen zu verpflichten.

(2) Folgende Daten sind zu übermitteln

1. Familiennamen (DSMeld-Blätter 0101 bis 0106),
2. Vornamen einschließlich des gebräuchlichen Vornamens (DSMeld-Blätter 0301 und 0302),
3. Doktorgrad (DSMeld-Blatt 0401),
4. Tag der Geburt (DSMeld-Blatt 0601),
5. Geschlecht (DSMeld-Blatt 0701),
6. derzeitige Anschrift der alleinigen oder Hauptwohnung in Sachsen (DSMeld-Blätter 1201 bis 1212).[2]"

Die getroffene Regelung begegnet im Lichte des Art. 6 Abs. 1 DSGVO betreffend die Verarbeitung personenbezogener Daten – und um solche handelt es sich bei den hier in Rede stehenden unzweifelhaft – keinen durchgreifenden Bedenken: Insoweit hat der nationale Normgeber eine gewisse Einschätzungsprärogative, nicht anders als sie hinsichtlich der Eignung und Erforderlichkeit sonstiger coronabezogener Maßnahmen in der Rechtsprechung der Verfassungs- und Verwaltungsgerichte anerkannt wird, wie das Bundesverfassungsgericht in seinem Beschluss vom 19.11.2021 – 1 BvR 781/21 u. a. [Bundesnotbremse I], ausführt:

„Verfassungsrechtlich genügt für die Eignung bereits die Möglichkeit, durch die gesetzliche Regelung den Gesetzeszweck zu erreichen (vgl. BVerfGE 152, 68 <130 f. Rn. 166>; 155, 238 <279 Rn. 102>; 156, 63 <116 Rn. 192>; stRspr). Bei der Beurteilung der Eignung einer Regelung steht dem Gesetzgeber ein Spielraum zu, der sich auf die Einschätzung und Bewertung der tatsächlichen Verhältnisse, auf die etwa erforderliche Prognose und auf die Wahl der Mittel bezieht, um die Ziele des Gesetzes zu erreichen (vgl. BVerfGE 109, 279 <336> m.w.N.; 152, 68 <131 Rn. 166>; siehe auch BVerfGE 156, 63 <116 Rn. 192>)." (Rdnr. 185)

Und:

„Dem Gesetzgeber steht grundsätzlich auch für die Beurteilung der Erforderlichkeit ein Einschätzungsspielraum zu (vgl. BVerfGE 152, 68 <136 Rn. 179>; 155, 238 <280 Rn. 105>; stRspr; hierzu auch BVerfG, Beschluss des Ersten Senats vom 19. November 2021 - 1 BvR 971/21 u.a. -, Rn. 123; ...). Der Spielraum bezieht sich unter anderem darauf, die Wirkung der von ihm gewählten Maßnahmen auch im Vergleich zu anderen, weniger belastenden Maßnahmen zu prognostizieren." (Rdnr. 204)

Das rechtfertigt – da die Problematik in sich neuartig ist und damit keine vorherigen statistischen Untersuchungen möglich waren – zunächst die der Verordnung zugrunde liegende Annahme, dass die dort geregelte Maßnahme zur Steigerung der Impfquote beim genannten Personenkreis geeignet und auch erforderlich ist.
Eine Kenntnis des Sächsischen Staatsministeriums für Soziales und Gesellschaftlichen Zusammenhalt über den Impfstatus war mit dem Schreiben nicht verbunden. Das Schreiben wurde unabhängig vom konkreten Impfstatus an den betreffenden Personenkreis versandt.

So sich die Beschwerden auch gegen den Inhalt des Schreibens wandten, habe ich darauf hingewiesen, dass dies nicht die Zuständigkeit meiner Behörde betrifft, und die Petenten hierzu direkt an das betreffende Ministerium verwiesen.
Hinsichtlich der Frage, inwieweit die Werbekampagne beim betreffenden Personenkreis zu einer Erhöhung der Impfquote gegenüber der Zeit vor Inkrafttreten der Verordnungsregelung geführt hatte und damit je nach Ausgang der Prüfung zu entscheiden war, ob die Regelung fortgeführt oder wieder aufgehoben werden sollte, stand ich ab Herbst mit der Staatsregierung im Austausch, letztlich mit dem Ergebnis, dass eine Datenverarbeitung basierend auf § 11a SächsMeldVO nicht weiter erfolgen wird.

1.5 Einrichtungsbezogene Impfpflicht: Portal zur Meldung nachweissäumiger Personen

↗ § 20a IfSG

Mit – interessanterweise vollständig identischen Schreiben – hatten sich Petenten aus gleich mehreren sächsischen Landkreisen und Kreisfreien Städten mit Anzeigen wegen der Errichtung und des Betriebs von Meldeportalen durch die Gesundheitsbehörden an mich gewandt und mitgeteilt, dass sie einen Brief ihres Gesundheitsamts erhalten hätten, in welchem über ihren Gesundheitsstatus in Bezug auf eine Immunisierung spekuliert würde.
Ich konnte bei den sodann angeführten umfangreichen Einwendungen indes allesamt keinen datenschutzrechtlichen Verstoß feststellen und habe wie folgt zu der Thematik Stellung genommen:
Nach dem Infektionsschutzgesetz müssen Personen, die beispielsweise in Krankenhäusern, Arztpraxen oder ambulanten Pflegediensten tätig sind, ab dem 15. März 2022 entweder geimpft oder genesen sein. Mit der sogenannten einrichtungsbezogenen Impfpflicht im Gesundheitsbereich sind zahlreiche datenschutzrechtliche Fragen verbunden, zum Beispiel, wel-

che Daten verarbeitet werden dürfen, welche Inhalte ein ärztliches Zeugnis haben muss oder ob Kopien von vorgelegten Nachweisen angefertigt werden dürfen.
Zu diesen und weiteren Fragen hat meine Behörde eine – aktualisierte – Handreichung herausgegeben, die auf der Website meiner Behörde veröffentlicht wurde.
Werden die Nachweise nicht entsprechend der vorgegebenen Fristen vorgelegt oder bestehen Zweifel an der Echtheit oder inhaltlichen Richtigkeit des vorgelegten Nachweises, hat die Leitung der jeweiligen Einrichtung oder des jeweiligen Unternehmens unverzüglich das Gesundheitsamt darüber zu benachrichtigen und dem Gesundheitsamt personenbezogene Daten zu übermitteln.
Das Bundesverfassungsgericht hat eine Verfassungsbeschwerde zurückgewiesen, die sich gegen § 20a, § 22a und § 73 Abs. 1a Nr. 7e bis 7h des Gesetzes zur Verhütung und Bekämpfung von Infektionskrankheiten beim Menschen (Infektionsschutzgesetz – IfSG) richtet, soweit darin die auf bestimmte Einrichtungen und Unternehmen des Gesundheitswesens und der Pflege bezogene Pflicht geregelt ist, eine COVID-19-Schutzimpfung, eine Genesung von der COVID-19-Krankheit oder eine medizinische Kontraindikation für eine Impfung nachzuweisen (sogenannte „einrichtungs- und unternehmensbezogene Nachweispflicht"). Die angegriffenen Vorschriften verstoßen nach der Entscheidung des Bundesverfassungsgerichts nicht gegen Art. 2 Abs. 2 Satz 1 Grundgesetz (GG) und Art. 12 Abs. 1 GG. Soweit die Regelungen in die genannten Grundrechte eingreifen, sind diese Eingriffe verfassungsrechtlich gerechtfertigt. Der Gesetzgeber hat im Rahmen des ihm zustehenden Einschätzungsspielraums einen angemessenen Ausgleich zwischen dem mit der Nachweispflicht verfolgten Schutz vulnerabler Menschen vor einer Infektion mit dem Coronavirus SARS-CoV-2 und den Grundrechtsbeeinträchtigungen gefunden. Trotz der hohen Eingriffsintensität müssen die grundrechtlich geschützten Interessen der im Gesundheits- und Pflegebereich Tätigen letztlich zurücktreten.

Da für die betreffenden Meldungen eine gesetzliche Grundlage besteht, bedarf es entgegen der Auffassung der Petenten für die Weitergabe ihrer personenbezogenen Daten keiner Einwilligung.

Eine Informationspflicht, wie von den Petenten ebenfalls behauptet, besteht ebenfalls nicht, dies ergibt sich hier aus Art. 14 Abs. 5 Buchst. c der DSGVO.

Auch der Betrieb des sächsischen Meldeportals begegnet keinen datenschutzrechtlichen Bedenken:

Über das digitale Meldeportal zur einrichtungsbezogenen Impfpflicht können die Einrichtungen/Unternehmen ihre Meldung der nachweissäumigen Personen nach § 20a IfSG an das zuständige Gesundheitsamt übermitteln.

Die behördlichen Datenschutzbeauftragten der Landkreise und der Kreisfreien Städte wurden von mir jedoch darauf hingewiesen, dass keine Verpflichtung für die Einrichtungen/Unternehmen besteht, das Meldeportal zur Übermittlung der personenbezogenen Daten zu nutzen, da es aktuell keine rechtliche Grundlage hierfür gibt. Ich habe gebeten, die Gesundheitsämter hierüber zu unterrichten.

2 Grundsätze der Datenverarbeitung

2.1 Datenverarbeitungsgrundsätze, Begriffsbestimmungen

2.1.1 Datenschutzrechtliche Einordnung gerichtlich bestellter Sachverständiger als eigenständige Verantwortliche

↗ § 839a BGB, Art. 4 Nr. 7 DSGVO, Art. 6 Abs. 1 Buchst. c DSGVO, Art. 9 Abs. 2 Buchst. f DSGVO

Vereinzelt erhalte ich Anfragen oder Beschwerden in Bezug auf die Datenverarbeitung durch gerichtlich bestellte Sachverständige. In einem Fall im letzten Berichtszeitraum teilte der Sachverständige einer betroffenen Person, die ihre Betroffenenrechte geltend zu machen suchte, mit, sie habe sich an das Gericht zu wenden. Als Sachverständiger sei er nicht Verantwortlicher im Sinne von Art. 4 Nr. 7 Datenschutz-Grundverordnung (DSGVO).

Entsprechende Auffassungen betrachte ich als nicht zutreffend. Die bzw. der gerichtlich bestellte Sachverständige unterliegt hinsichtlich ihrer bzw. seiner personenbezogenen Datenverarbeitung der datenschutzrechtlichen Zuständigkeit meiner Behörde, und ich übe diese aufsichtliche Kontrolle auch aus.

Nachstehende Überlegungen sind für diese Einordnung maßgebend: Durch den Gutachtenauftrag des Gerichts wird der oder dem Sachverständigen eine relativ eng begrenzte und vorgegebene Aufgabe (Auftrag) übertragen. Die bzw. der Sachverständige bestimmt aber selbst, welche Mittel sie bzw. er zur Beantwortung der Fragen einsetzt und ob und gege-

benenfalls welche Daten dazu noch (über die vom Gericht erhaltenen hinaus) verarbeitet werden müssen. Als Sachverständiger hat sie bzw. er das Gutachten selbst und eigenverantwortlich und – abgesehen vom Auftrag – weisungsfrei zu erstatten. Zudem wurde mit § 839a Bürgerliches Gesetzbuch (BGB) eine eigene Schadenersatzvorschrift für gerichtlich benannte Sachverständige geschaffen. Deren Handeln fällt damit nicht als „Gerichtshandlung" unter § 839 BGB.
Demnach erfolgt die personenbezogene Datenverarbeitung auf der Rechtsgrundlage von Art. 6 Abs. 1 Buchst. c und Art. 9 Abs. 2 Buchst. f DSGVO.
Soweit die oder der Sachverständige nach Abschluss ihrer bzw. seiner Tätigkeit für das Gericht über keine Daten bzw. Unterlagen zu den Betroffenen mehr verfügt, verarbeitet sie bzw. er in dieser Hinsicht auch keine personenbezogenen Daten und ist dann kein Verantwortlicher mehr.
Sollte die bzw. der Sachverständige allerdings auch nach Abschluss des Gutachtenauftrages noch Aufzeichnungen über die Betroffenen haben, hat sie bzw. er sich auch mit geltend gemachten Betroffenenrechten auseinanderzusetzen und deren Erfüllung nach den gesetzlichen Vorschriften sicherzustellen.

Was ist zu beachten?
Die bzw. der gerichtlich bestellte Sachverständige – vgl. etwa §§ 402ff. ZPO, §§ 72ff. StPO, § 118 SGG – ist eigenständiger Verantwortlicher. Sie bzw. er unterliegt hinsichtlich ihrer bzw. seiner personenbezogenen Datenverarbeitung der datenschutzrechtlichen Aufsicht.

2.1.2 Personenbeziehbarkeit von Informationen zu einer Kapitalgesellschaft

↗ Art. 2 Abs. 1, Art. 4 Nr. 1 DSGVO

Zurückliegend wandte sich der Geschäftsführer und Alleingesellschafter einer Unternehmergesellschaft (UG) an meine Behörde und machte seine Auskunftsrechte wegen der Einholung von Informationen zu seiner Gesellschaft geltend. Gegenstand war die Erhebung und Verarbeitung der Bonität der Gesellschaft durch ein anderes Unternehmen, den Verantwortlichen. Letzterer hatte dem Beschwerdeführer mitgeteilt, die Geschäftsbeziehung zu der Unternehmergesellschaft einstellen zu wollen.
Nachdem ich eine Stellungnahme des Verantwortlichen zum Beschwerdevorgang eingeholt hatte, teilte dieser mit, dass

er lediglich und ausschließlich Bonitätsinformationen zu der Unternehmergesellschaft eingeholt habe. Daraufhin entschied ich, die Beschwerde abzuweisen, da ich den Anwendungsbereich der Datenschutz-Grundverordnung (DSGVO) wegen des fehlenden Personenbezugs für nicht eröffnet hielt, vgl. Art. 2 Abs. 1, Art. 4 Nr. 1 DSGVO. Damit wiederum war der Beschwerdeführer nicht einverstanden und erhob Klage vor dem Verwaltungsgericht gegen meine Entscheidung. Eine gerichtliche Entscheidung stand im letzten Berichtszeitraum noch aus.

Für meine Einschätzung waren nachstehende Überlegungen ausschlaggebend: Die UG ist eine Sonderform der GmbH und ist gleichfalls im Handelsregister einzutragende Kapitalgesellschaft und haftungsbeschränkt. Sie kann bereits mit 1 Euro Stammkapital gegründet werden. Die Unternehmergesellschaft ist auch haftungsbeschränkt. Die Haftungsbeschränkung bedeutet, dass die Gesellschafter und die Geschäftsführer einer UG, von Ausnahmefällen abgesehen, ausschließlich mit dem Gesellschaftsvermögen und nicht mit ihrem Privatvermögen haften.

Zwar können Daten zu juristischen Personen im Einzelnen auch einen Personenbezug im Sinne der DSGVO aufweisen, im konkreten Fall lässt die Bonität einer UG jedoch, anders als etwa deren Vermögen oder Zahlungseingänge, keine Rückschlüsse auf personenbezogene Daten von deren Gesellschafter oder Geschäftsführer zu. Das ergibt sich anschaulich aus der prinzipiellen Möglichkeit, eine UG mit einem haftenden Stammkapital von 1 Euro auszustatten, mit der entsprechenden Bonität der UG. Auch im Einzelfall verfügte die UG nur über ein geringes Stammkapital. Bei dem Vorgang ergaben sich ferner auch keine konkreten Anhaltspunkte für einen ausnahmsweisen Personenbezug der Bonitätsdaten der UG auf den Geschäftsführer und Alleingesellschafter. Der Verantwortliche hatte auch dezidiert vorgetragen, den Beschwerdeführer entsprechend dessen eigenen Angaben, als Geschäftsführer bzw. Vertretungsberechtigten zu führen, sodass ich etwaige Rückwirkungen auf die Person des Beschwerdeführers ausschließen konnte. Damit war auch nicht

davon auszugehen, dass den Betroffenenrechten seitens des Verantwortlichen nicht in ausreichendem Maße nachgekommen war, wie der Beschwerdeführer es reklamierte.
Vor diesem Hintergrund hatte ich das aufsichtliche Verfahren geschlossen.

2.1.3 Interpretation der ePrivacy-Richtlinie

↗ ePrivacy-Richtlinie, TTDSG

Eigentlich sollte die ePrivacy-Verordnung gemeinsam mit der Datenschutz-Grundverordnung (DSGVO) als Schwesterverordnungen in Kraft treten. Die DSGVO deckt die Verarbeitung der Daten bei den Anbietern ab und ePrivacy schützt die Geräte und Verbindungen der einzelnen Nutzerinnen und Nutzer.
Es kam jedoch anders und statt der „ePrivacy-Verordnung" wurde die „ePrivacy-Richtlinie" verabschiedet, welche nicht direkt als europäisches Recht gilt, sondern in nationales Recht überführt werden muss. In Deutschland geschieht dies durch das „Telekommunikation-Telemedien-Datenschutz-Gesetz" (TTDSG). Der Plan, dieses Recht mit einer europäischen Verordnung durchzusetzen, existiert weiterhin. Jedoch ist noch unklar, wann dies stattfindet.
In der Zwischenzeit sind Fragen zu der aktuellen Richtlinie und möglicherweise zukünftigen Verordnung zu klären. Damit beschäftigt sich unter anderem der Europäische Datenschutzausschuss (EDSA). Zu bestimmten Fragen verfasst er Stellungnahmen, sogenannte Opinions, welche er anderen europäischen und nationalen Behörden zur Orientierung an die Hand gibt. Um diese Opinions zu verfassen, wendet der Ausschuss sich seinerseits an sogenannte „expert subgroups" – Gruppen von Experten, welche aus den verschiedenen Datenschutzbehörden der Länder zusammengestellt werden.
Eine der Fragen, die in den expert subgroups derzeit diskutiert werden, befasste sich mit der scheinbar einfachen Bedeutung des Satzfragments aus Artikel 5(3): „[…] Speicherung von Informationen oder […] Zugriff auf Informationen, die im Endgerät eines Teilnehmers oder Nutzers gespeichert sind […]".

Aber was ist denn genau ein „Endgerät"? Was bedeutet „Zugriff" und was heißt „Speicherung"?
So kurz der Text, so lang die Fragen, welche sich daraus ergeben. Schließlich werden in einem Computer alle Informationen gespeichert, wenn auch nur sehr kurz. Ohne Speicherung können Informationen nicht verarbeitet werden. Betrifft dieser Artikel somit alle Informationen, die übertragen werden, egal, wie flüchtig? Das war vermutlich vom Gesetzgeber nicht so beabsichtigt. Gleiches gilt für den „Zugriff". Wenn ein Nutzer einem Verantwortlichen ohne vorherigen Kontakt ein Datenpaket schickt, hat der Verantwortliche dann „Zugriff" auf diese Informationen erlangt? Das könnte die absurde Situation erzeugen, dass der Verantwortliche um Erlaubnis bitten müsste, um herauszufinden, ob er um Erlaubnis bitten muss. Das war sicherlich ebenfalls nicht so beabsichtigt. Die Rapporteure aus Frankreich, Italien und Sachsen haben also noch viel Arbeit vor sich.

2.2 Rechtmäßigkeitsvoraussetzungen der Datenverarbeitung

2.2.1 Übermittlung von Beschäftigtendaten zur Kommunalwahl

↗ § 10 Abs. 2 KomWG, Art. 17 DSGVO

Im Zusammenhang mit der Durchführung der Kommunalwahlen erreichte mich die Anfrage eines Bediensteten des Freistaates Sachsen. Dieser fragte an, ob sein Dienstherr auf Ersuchen einer Kommune, in welcher eine Kommunalwahl stattfinde, im Vorfeld dieser Kommunalwahl seine personenbezogenen Beschäftigtendaten an diese übermitteln durfte. Gemäß § 10 Abs. 2 Sächsisches Kommunalwahlgesetz (KomWG) sind zur Sicherstellung der Wahldurchführung Körperschaften und sonstige juristische Personen des öffentlichen Rechts verpflichtet, auf Ersuchen der Gemeinde, aus dem Kreis ihrer Bediensteten unter Angabe von Name, Vorname, Geburtsdatum und Anschrift zum Zweck der Be-

rufung als Mitglied eines Wahlvorstandes, Personen zu benennen, die im Gebiet der ersuchenden Gemeinde wohnen und volljährig sind. Die ersuchte Stelle hat den Betroffenen über die Datenübermittlung zu unterrichten.

Dem Betroffenen habe ich zunächst mitgeteilt, dass nach Auffassung meiner Behörde die übermittelnde Stelle keine Auswahl unter den Bediensteten, deren Daten sie an die ersuchende Stelle übermittelt, zu treffen hat, außer in Bezug auf das Gebiet der Gemeinde, in der die Personen wohnen. Soweit § 10 Abs. 2 KomWG ausführt, dass „… Personen zu benennen …" sind, bezieht sich dies somit nur auf die im Gebiet der Gemeinde wohnenden Personen und nicht auf eine Auswahl aus diesem Personenkreis.

Die übermittelnde Stelle muss auch nicht ermitteln, wie viele Wahlvorstände die ersuchende Gemeinde (gegebenenfalls noch) benötigt, um nur eine dementsprechende Anzahl von personenbezogenen Daten zu übermitteln. Eine derartige Einschränkung ist der Regelung des § 10 Abs. 2 KomWG nicht zu entnehmen. Auch nach § 6 Abs. 1 Satz 2 Sächsisches Datenschutzdurchführungsgesetz (SächsDSDG), ist die übermittelnde Stelle grundsätzlich nur verpflichtet zu prüfen, ob das Übermittlungsersuchen im Rahmen der Aufgaben des Empfängers, hier der ersuchenden Kommune, liegt.

Der Betroffene wandte gegen die Übermittlung seiner Daten durch den Dienstherrn ein, dass er in der ersuchenden Kommune nur seinen Neben- und nicht seinen Hauptwohnsitz habe und somit in der ersuchenden Kommune nicht zum Wahlvorstand berufen werden könne, vgl. § 15 Abs. 1 Satz 2 und § 16 Sächsische Gemeindeordnung (SächsGemO). Der Dienstherr hätte ihn daher vor der Datenübermittlung anhören müssen. Dazu habe ich dem Betroffenen mitgeteilt, dass der Dienstherr grundsätzlich nicht verpflichtet ist, vor Übermittlung personenbezogener Daten an die ersuchende Kommune die Betroffenen anzuhören. Erforderlich sei jedoch, dass der Dienstherr prüfe, welcher Bedienstete seinen Wohnsitz in der um Übermittlung ersuchenden Gemeinde hat.

In diesem Zusammenhang wäre zunächst zu klären, ob dem Dienstherrn die Daten zu Haupt- und Nebenwohnsitz der

Beschäftigten vorliegen und welcher Datensatz zur Übermittlung an die ersuchende Kommune herangezogen wurde. Sollte eine derartige Datenerhebung, das heißt des Haupt- und Nebenwohnsitzes, nicht erfolgen (zum Beispiel, weil dies für das Dienstverhältnis nicht erforderlich ist), bestünde auch keine Verpflichtung, diese Daten zusätzlich zu erheben. Vielmehr liegt es dann in der Verantwortung der um Übermittlung ersuchenden Stelle, dies aufzuklären.

Den Betroffenen habe ich in diesem Zusammenhang auf Art. 17 DSGVO hingewiesen. Danach kann der Betroffene vom Verantwortlichen (hier: ersuchende Kommune) die Löschung unrechtmäßig verarbeiteter personenbezogener Daten verlangen.

Was ist zu beachten?
Beschäftigte öffentlicher Stellen haben damit zu rechnen, dass sie seitens ihrer Dienstherren zur Berufung von Wahlvorständen den Gemeinden benannt werden.

Im Übrigen hat der Betroffene das Recht, der Verarbeitung seiner personenbezogenen Daten für künftige Wahlen zu widersprechen, vgl. § 10 Abs. 6 KomWG. Über dieses Widerspruchsrecht ist der Betroffene zu informieren.

2.2.2 Kommunalrechtsnovelle

↗ Art. 36 Abs. 4 DSGVO, SächsGemO, SächsLKrO

18. Tätigkeitsbericht:
↗ sdb.de/tb2111

Im 18. Tätigkeitsbericht hatte sich mein Amtsvorgänger unter 5.5.7 kritisch zu Ratsinformationssystemen und dem Zugang zu Sitzungsunterlagen und Niederschriften geäußert. Er musste auch feststellen, dass das Sächsische Staatsministerium des Innern (SMI) bereits im Jahr 2021 unter anderem dazu den Entwurf eines Dritten Gesetzes zur Fortentwicklung des Kommunalrechts vorbereitete, ohne dass meine Behörde beteiligt wurde. Er wies das SMI auf Art. 36 Abs. 4 DSGVO hin, wonach ich bei der Ausarbeitung von Amts wegen zu konsultieren sei – und nicht erst wie vorliegend auf Nachfrage.

In der Sache selbst sah ich die Einfügung eines § 36b in die Sächsische Gemeindeordnung (SächsGemO) bzw. § 32b in die Sächsische Landkreisordnung (SächsLKrO) zur Veröffentlichung von Informationen aus Sitzungen des Gemeinderats kritisch. Ich wies auf das Urteil des Sächsischen Oberverwaltungsgericht vom 30. August 2019 (4 C 12/17) hin. Dort wird im Leitsatz ausgeführt:

„Unterlagen, die vom Landrat zur Vorbereitung der Sitzungen des Kreistags an die Kreisräte ausgereicht werden, sind interne Dokumente der Verwaltung, deren Zweck allein in der Verwendung innerhalb des Kreisrats besteht. Sie dienen der Unterrichtung innerhalb des Gremiums und der Vorbereitung von Abstimmungen."

Zwar war vorgesehen, dass personenbezogene Daten dabei nicht offenbart werden dürfen. Auch kann bei einem sich daraus ergebenden erheblichen Aufwand von einer Veröffentlichung abgesehen werden. Die Behörde in der Vergangenheit erreichende Petitionen über Publikationen von amtlichen Mitteilungs- oder Verkündungsblättern nach § 4 Sächsisches E-Government-Gesetz (SächsEGovG) legen jedoch nahe, dass sich in vielen Fällen auch künftig hieran nicht gehalten werden wird. Dort hieß es bis 21. Juni 2019 in Absatz 3: „... In einer über öffentlich zugängliche Netze verbreiteten elektronischen Fassung der Publikation sind jedoch personenbezogene Daten unkenntlich zu machen, wenn der Zweck ihrer Veröffentlichung erledigt ist und eine fortdauernde Veröffentlichung das Recht der betroffenen Person auf informationelle Selbstbestimmung unangemessen beeinträchtigen würde. ..." Dies ergäbe sich nach der Gesetzesbegründung zur Änderung des SächsEGovG jetzt direkt aus der DSGVO. Im Ergebnis wurde jedoch oft keine entsprechende Prüfung vorgenommen.

Es steht zudem zu befürchten, dass Beratungsunterlagen durch mündlichen Vortrag ersetzt werden würden. Mit den Bedenken konnte mein Amtsvorgänger nicht durchdringen, der Gesetzentwurf wurde mit einem insoweit unveränderten Wortlaut in den Landtag eingebracht.

Dort wurde jedoch von den Koalitionsfraktionen Anfang des Jahres 2022 im Innenausschuss ein Änderungsantrag eingebracht, wonach das Live-Streaming von Ratssitzungen in einem neu eingefügten § 37 Abs. 3 ohne Einwilligung zulässig sein sollte; es war lediglich ein Widerspruchsrecht vorgesehen. Der Sächsische Datenschutzbeauftragte hatte jedoch bereits in seinem 13. Tätigkeitsbericht unter 5.5.1 zu Live-Übertragungen von Stadtrats- und Kreistagssitzungen

13. Tätigkeitsbericht:
↗ sdb.de/tb2202

ausgeführt, dass wegen der Berücksichtigung der einzelnen Rätinnen und Räte als Grundrechtsträgerinnen und Grundrechtsträger fraglich ist, ob zum Beispiel eine Veröffentlichung via Internet mit kommunaler Rechtssetzung, zum Beispiel mit einer Geschäftsordnung oder auch per Satzung, für alle Mitglieder der Vertretungskörperschaft pauschal und verbindlich vorgegeben werden kann. Dies auch vor dem Hintergrund, dass durch eine kommunale Satzung nicht gegen Bundesrecht verstoßen werden kann. § 22 des Kunsturheberrechtsgesetzes (KunstUrhG) fordert aber für eine entsprechende Übertragung eine Einwilligung; bei kommunalen Parlamenten wird es sich auch nicht um Personen der Zeitgeschichte handeln und § 23 Abs. 1 Nr. 1 KunstUrhG daher nicht einschlägig sein. Mit diesen Argumenten konnte ich überzeugen, sodass schließlich ein Einwilligungsvorbehalt aufgenommen wurde.

2.2.3 Besinnungsstunde führt zu Fragebogen

↗ SächsSchulG

Eltern wiesen mich darauf hin, dass die Schule ihrer Tochter im Klassenleiterunterricht in einer „Besinnungsstunde" vor den Weihnachtsferien einen Film gezeigt habe, indem das Töten von Tieren für den Fleischkonsum thematisiert und als Alternative vegane Nahrung vorgestellt wurde. Dies sei nicht von allen als besinnlich wahrgenommen worden; unter der Elternschaft der Klasse herrschte nach Darstellung der zur Stellungnahme aufgeforderten Schule vielmehr das blanke Entsetzen und Fassungslosigkeit vor.

Dies nahm der Klassenleiter zum Anlass, um von den Schülerinnen und Schülern in einem Fragebogen im neuen Jahr persönliche Angaben zu Essgewohnheiten, Einschlafstörungen, Angst und Ekelempfindungen der Kinder hinsichtlich dieser „Besinnungsstunde" abzufragen. Darüber informierte er nachträglich in einem Elternbrief, der wiederum einen Fragebogen enthielt und eine Rückantwort bzw. die Angabe von Gründen bei deren Fehlen vorsah.

Anzumerken ist hierzu, dass der Erziehungs- und Bildungsauftrag nach § 1 Abs. 3 Satz 2 Sächsisches Schulgesetz (SächsSchulG) als Ziel benennt, den Schülerinnen und Schülern insbesondere anknüpfend an die christliche Tradition im europäischen Kulturkreis Werte wie Ehrfurcht vor allem Lebendigen zu vermitteln. Fraglich ist angesichts der Reaktionen, ob dies gelungen ist. Datenschutzrechtlich konnte ich jedenfalls konstatieren, dass die ausgefüllten Fragebögen an die Schülerinnen und Schüler bzw. deren Eltern zurückgegeben wurden, da eine Rechtsgrundlage für deren Erhebung zumindest fraglich ist.

2.2.4 Neuausrichtung von Aufbewahrungsfristen für Gewerbeanzeigen

↗ § 4 SächsDSDG, § 14, § 146 GewO, Art. 6 Abs. 3 DSGVO

Das Gewerbeamt einer sächsischen Gemeinde wandte sich an mich mit der Anfrage, wie lange Gewerbeanzeigen nach der Anmeldung des Gewerbes aufzubewahren und vorzuhalten sind und ob die vormals vereinbarte Frist von fünf Jahren (vgl. 10. Tätigkeitsbericht 2002, 9.2.) noch zeitgemäß wäre und ob diese nicht auf zehn Jahre verlängert werden könnte und sollte. Eine explizite gesetzliche Regelung hierzu ist weder in der Gewerbeordnung (GewO) noch in der Gewerbeanzeigeverordnung zu finden.

Dass eine sofortige Löschung der Eintragung nach Gewerbeabmeldung nicht infrage kommt, steht außer Zweifel. Dem steht bereits die Vorschrift des § 146 Abs. 2 Nr. 1 GewO entgegen, wonach ordnungswidrig handelt, wer vorsätzlich oder fahrlässig entgegen § 14 Abs. 1 bis 3 GewO eine Anzeige nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erstattet. Denn würden nach der Anzeige der Gewerbeaufgabe sofort die in Rede stehenden Daten vernichtet, so wäre es der Behörde praktisch unmöglich nachzuprüfen, ob die angezeigte Gewerbeaufgabe tatsächlich erfolgt ist oder ob das Gewerbe ohne Anzeige weitergeführt wird. Dies kann keinesfalls sachgemäß sein.

Vor circa 20 Jahren wurde deswegen im Freistaat Sachsen noch eine Einigung dahingehend gefunden, dass die Aufbewahrungsfrist von fünf Jahren als angemessen und ausreichend empfunden wurde. Der gesellschaftliche Wandel, der sich auch insbesondere im Mittelstand widerspiegelt, erfordert indes durchaus ein Überdenken und eine Neubewertung – An- und Abmeldungen gehen viel leichter von der Hand als noch vor 20 oder 30 Jahren. Durch den technischen Fortschritt kommen immer mehr Start-ups auf den Markt, oder das Anfangskapital wird aufgrund des (derzeit noch) niedrigen Kreditzinses viel leichter finanziert.

Vor diesem Hintergrund war die Aufbewahrungsfrist zu überdenken. Betreibt der Gewerbetreibende sein Gewerbe nach Abmeldung rechtswidrig fort, drohen Untersagungsverfahren (§ 35 Abs. 1 bzw. § 15 Abs. 1 GewO) und Bußgelder in beträchtlicher Höhe, § 146 GewO. Auch sonst kann es bei der Beurteilung der gewerberechtlichen Zuverlässigkeit bei Erteilung und Untersagung des Gewerbes von Bedeutung sein, wie und wo sich ein Gewerbetreibender in den letzten Jahren betätigt hat.

Auch für eine Sachverhaltsermittlung durch sonstige Behörden (Strafverfolgung, Finanzamt, Berufsgenossenschaft, Sozialversicherungsträger etc.) kann die Vorhaltung dieser Daten relevant sein. Hinterzogene Steuern können beispielsweise noch innerhalb von zehn Jahren vom Finanzamt festgesetzt werden (§ 169 Abs. 2 Satz 2 Abgabenordnung). Auch die Sozialversicherer können vorenthaltene Beiträge innerhalb von 30 Jahren zurückfordern. Diese Form der Schwarzarbeit hat durchaus in den letzten Jahren zugenommen, weswegen dem auch angemessen zu begegnen ist. Eine Datenweitergabe an eine andere öffentliche Stelle für einen anderen als den ursprünglichen Zweck ist unter den Voraussetzungen des Art. 6 Abs. 3 Datenschutz-Grundverordnung (DSGVO) und § 4 Sächsisches Datenschutzdurchführungsgesetz (SächsDSDG) möglich.

Die Argumentation des Gewerbeamtes hat mich überzeugt. Deswegen erschien es auch aus meiner Sicht vertretbar und auch nachvollziehbar, einer Aufbewahrungsfrist von zehn Jahren zuzustimmen.

2.2.5 Übermittlung von Versammlungsveranstaltern an die Presse

↗ SächsVersG

Das Sächsisches Staatsministerium des Innern bat mich um meine Auffassung, ob Pressevertreterinnen bzw. -vertretern auf Nachfrage die vollständigen Namen von Versammlungsveranstalterinnen bzw. -veranstaltern zu nennen seien.
Ich habe zunächst auf die vorzunehmende Abwägung zwischen dem Informationsinteresse der Öffentlichkeit und dem entgegenstehenden privaten Interesse an der Geheimhaltung hingewiesen. Dabei teile ich die Auffassung des Verwaltungsgerichts Osnabrück vom 17.12.2021, AZ. 1 B 72/21, dass bei der vorzunehmenden Abwägung der entgegenstehenden Interessen zwischen dem Informationsinteresse der Presse und den privaten Interessen der Anmelderinnen bzw. Anmelder zu berücksichtigen ist, dass Demonstrationen von vornherein auf Publizität ausgelegt sind, weshalb die Anmelderinnen bzw. Anmelder zunächst in ihrer Sozialsphäre betroffen sind.
Nicht ausreichend für eine Auskunftsverweigerung ist demnach eine pauschale Befürchtung, dass „Personen, die beabsichtigen, eine Versammlung zu veranstalten, die Anzeige unterlassen, da sie nicht möchten, dass ihr Name und Wohnort einer breiten Öffentlichkeit einschließlich der politischen Gegner bekannt wird". Anders ist das beispielsweise bei Anhaltspunkten für schwerwiegende Beeinträchtigungen der Anmelderin bzw. des Anmelders (schon [mehrfach] Angriffen, Bedrohungen ausgesetzt); hier kann die Abwägung im Einzelfall zu einem anderen Ergebnis führen.

2.2.6 Datenschutzrechtliche Behandlung der Veröffentlichung von Bürgerbegehren im Amtsblatt

↗ § 4 Abs. 1 SächsEGovG, § 25 Abs. 2 und 4 SächsGemO, Art. 5 Abs. 1 c DSGVO

Im Berichtszeitraum wandten sich zwei Petenten an mich, die monierten, dass eine sächsische Gemeinde in ihrem Amtsblatt im Rahmen eines veröffentlichten Bürgerbegehrens rechtswidrig ihre Namen, Anschriften und sogar die Unterschriften veröffentlichte.

Die Petenten waren in einem Bürgerbegehren Vertrauenspersonen gemäß § 25 Abs. 2 Satz 1 Sächsische Gemeindeordnung (SächsGemO). Das Bürgerbegehren wurde durch einen Gemeinderatsbeschluss als unzulässig abgelehnt, was ortsüblich bekannt zu geben ist, § 25 Abs. 4 SächsGemO. Bekannt gegeben wurde der Sachverhalt im Amtsblatt, in der Druck- und in der Online-Version (Scan der Druckausgabe). Sowohl das Bürgerbegehren als auch der ablehnende Bescheid wurden in Volltext samt Namen, Adressdaten und der dazugehörigen (hektografierten) Unterschriften der Vertrauenspersonen abgedruckt. Hiergegen richtete sich dann die an mich gerichtete Beschwerde.

Dass die Gemeinde den Volltext des Bürgerbegehrens und den dazugehörigen Ablehnungsbescheid auch in Volltext abdruckt, ist zunächst nicht zu beanstanden und ist durch § 25 SächsGemO gesetzlich gedeckt. Nach der entsprechenden gemeindlichen Bekanntmachungssatzung ist der Abdruck im Amtsblatt klassischerweise die Form der ortsüblichen Bekanntmachung.

Da der ergangene Beschluss des Stadtrates den Inhalt des Bürgerbegehrens nicht in vollem Wortlaut wiedergab, war auch vertretbar, dessen Inhalt ebenfalls zu veröffentlichen. Schließlich hat die Gemeindeöffentlichkeit ein berechtigtes Interesse daran zu erfahren, aus welchen Gründen das Begehren abgelehnt wurde und ob das Vorbringen der Unterzeichnenden Berücksichtigung gefunden hat.

Auch die Veröffentlichung der Namen der Vertrauenspersonen war datenschutzkonform, § 25 Abs. 2 Satz 1 SächsGemO. Demnach muss das Bürgerbegehren eine Vertrauensperson und eine stellvertretende Verbandsperson bezeichnen, die jede für sich zur Entgegennahme von Mitteilungen und Entscheidungen der Gemeinde und zur Abgabe von Erklärungen ermächtigt ist. Angesichts des oben beleuchteten Vollständigkeitsgrundsatzes gebietet es sich, auch die Namen der Vertrauenspersonen zu benennen und auch zu veröffentlichen. Denn eine Vertrauensperson, die sich durch entsprechende Tätigkeit für ein Bürgerbegehren in die öffentliche kommunalpolitische Auseinandersetzung begibt, muss damit rechnen, dass jedenfalls ihre Namen in der vorgenannten – rechtlich fundamentierten – Weise bekannt werden, selbst wenn diese Quelle dank des Internets mittlerweile weltweit zugänglich ist.

Auch ist die Online-Veröffentlichung durch § 4 Abs. 1 Sächsisches E-Government-Gesetz (SächsEGovG) gedeckt. Diese Vorschrift sieht vor, dass Publikationen in amtlichen Mitteilungs- oder Verkündungsblättern zusätzlich oder ausschließlich durch eine elektronische Ausgabe erfüllt werden können, wenn diese über öffentlich zugängliche Netze angeboten wird. Ob der Scan des gedruckten Amtsblattes als eine elektronische Ausgabe in diesem Sinn zu werten ist, kann im Prinzip dahinstehen. Auch als ein sogenanntes wesensgleiches Minus wäre dieses ebenfalls von der Vorschrift gedeckt und ist deswegen auch als solches datenschutzkonform.

Datenschutzverstöße mussten der Gemeinde in dieser Sache aber trotzdem vorgeworfen werden: Sowohl die Veröffentlichung der Unterschriften als auch die der Adressen der Vertrauenspersonen waren nicht zulässig. Bei den Anschriften hätte es genügt, mit der Verkürzung der Anschrift auf den Ort selbst klarzustellen, dass es sich bei den Vertrauenspersonen um Bürger der entsprechenden Gemeinde gehandelt hat. Die konkrete Anschrift, also Straße und Hausnummer, waren hierfür jedoch nicht erforderlich, sodass hier das Gebot der Datenminimierung nach Art. 5 Abs. 1c Datenschutz-Grundverordnung (DSGVO) verletzt wurde.

Noch kritischer zu betrachten war die Wiedergabe der handschriftlichen Unterschriften der Vertrauenspersonen, insbesondere in der Online-Version. Diese Wiedergabe stellt von vornherein einen Verstoß gegen das Gebot der Datenminimierung dar. Denn sie war bereits nicht zur Unterrichtung des Gemeinderats im Vorfeld der von ihm zu treffenden Zulässigkeitsentscheidung erforderlich. Insoweit hätte es genügt, seitens der Gemeindeverwaltung den Vermerk „handschriftlich unterzeichnet" anzubringen. Die hektografierte Wiedergabe der Unterschriften in dem öffentlich zugänglichen – und zudem online eingestellten und somit weltweit abrufbaren – Amtsblatt war unter keinen Umständen erforderlich gewesen. Stattdessen aber stellt diese Wiedergabe im Zeichen der heutzutage immer weiter um sich greifenden Gefahren des Integritätsdiebstahls eine nicht unerhebliche Gefährdung des wirtschaftlich-persönlichen Rechtskreises der Vertrauenspersonen dar.

Was ist zu tun?
Die Kommunen haben insbesondere bei der online zugänglichen Veröffentlichung von personenbezogenen Daten stets die Rechtsgrundlagen und die Erforderlichkeit gründlich zu prüfen.

Die Gemeinde hat auf mein Eingreifen hin den Fehler erkannt und die rechtswidrig veröffentlichten Daten umgehend geschwärzt. Somit konnte das sich ergebene Risiko noch deutlich minimiert werden.

2.2.7 Weitergabe von Daten aus dem Kehrbuch des Bezirksschornsteinfegers

↗ § 3 Abs. 1 SächsDSDG, § 4 Abs. 2 Satz 4 BauGB, § 19 Abs. 5 Satz 2 Halbsatz 2. SchHfG

Im Berichtszeitraum erhielt ich die Anfrage eines Bezirksschornsteinfegers zu den geltenden datenschutzrechtlichen Bestimmungen, wie mit den im Rahmen seiner Tätigkeit erlangten personenbezogenen Daten seiner Kundinnen und Kunden umzugehen sei.

Im Rahmen der Erarbeitung eines städtebaulichen Energiekonzeptes wandte sich eine Gemeinde an den Schornsteinfeger und wollte zu einem bestimmten, räumlich abgegrenzten Untersuchungsgebiet wissen, über welche Art, welches Baujahr die Wärmeerzeuger der betreffenden Objekte verfügen, welche Energieträger eingesetzt werden und ob etwaig

Besonderheiten bestehen. Der anfragende Schornsteinfeger war sich unsicher, ob er diese Daten weitergeben darf und auch muss.

Nach eingehender Prüfung meinerseits und erfolgter Stellungnahme der betroffenen Gemeinde ergaben sich zwei Schlussfolgerungen:

Zum einen handelt es sich bei den abgefragten Informationen um personenbezogene Daten. Zumindest dann, wenn das betroffene Immobilienobjekt ein Einfamilienhaus ist (vorliegend fast ausschließlich), kann durch Namenszuordnung bestimmt werden, welche Familie welche Heizungsart nutzt. Vor dem Hintergrund von politischen und gesellschaftlichen Klimawandeldiskussionen ist nicht auszuschließen, dass dies hypothetisch zu Unmut führen könnte. Der Personenbezug dieser Daten ist somit in jedem Fall zu bejahen.

Zuvor hatte die Gemeinde noch gemäß § 137 Baugesetzbuch (BauGB) die Eigentümerinnen und Eigentümer der im Untersuchungsgebiet befindlichen Gebäude und Grundstücke über die Durchführung vorbereitender Untersuchungen informiert und um Mitwirkung gebeten. Die Angaben des Bezirksschornsteinfegers dienen der fachbezogenen Ergänzung dazu, da naturgemäß den meisten Eigentümerinnen und Eigentümern das konkrete Wissen hierzu fehlt.

Ob und in welcher Art und Weise Schornsteinfegerinnen und Schornsteinfeger nun diese personenbezogenen Daten verarbeiten und an Behörden übermitteln dürfen und müssen, richtet sich nach § 19 Abs. 5 Satz 2 Halbsatz 2. Schornsteinfegerhandwerksgesetz (SchfHwG). Dabei ist zu unterscheiden, in welcher Funktion die Schornsteinfegerinnen und Schornsteinfeger tätig werden. Sie bzw. er kann zum einen als private/r Gewerbetreibende/r ihre/seine Dienstleistungen anbieten, zum anderen wird sie/er als öffentlich bestellte/r Bezirksschornsteinfeger/in tätig und führt unter anderem das gesetzlich vorgeschriebene Kehrbuch oder nimmt die ebenfalls turnusmäßig vorgeschriebene Feuerstättenschau ab.

Im zweiten Fall wird die/der Schornsteinfeger/in als Beliehene/r der jeweiligen Gemeindeverwaltung tätig. Konsequenz dessen ist, dass die Vorschriften des Sächsischen Datenschutzdurchführungsgesetzes (SächsDSDG) für seine Tätigkeit Anwendung finden, § 2 Abs. 2 SächsDSDG: „Nehmen nichtöffentliche Stellen hoheitliche Aufgaben der öffentlichen Verwaltung wahr, sind sie insoweit öffentliche Stellen im Sinne dieses Gesetzes." Die Führung des Kehrbuches ist unter anderem eine derartige hoheitliche Aufgabe der/des bestellten Schornsteinfeger/in bzw. Schornsteinfegers, die/der bei diesen öffentlichen Aufgaben der Verwaltung als Beliehene/r tätig wird.

Nach §§ 141 in Verbindung mit § 139 Baugesetzbuch (BauGB) wird die Beteiligung und Mitwirkung öffentlicher Aufgabenträger im Rahmen vorbereitender Untersuchungen bei städtebaulichen Sanierungsmaßnahmen vorgeschrieben. Da hier Daten aus dem Kehrbuch des Bezirksschornsteinfegers relevant sind und er diese bei Erfüllung seiner öffentlichen Aufgaben erlangt hat, ergibt sich die Ermächtigung und auch die Pflicht zur Datenweitergabe für ihn aus § 4 Abs. 2 Satz 4 BauGB. Hieraus ergibt sich nämlich die konkrete Pflicht einer Behörde, vorliegende Informationen zu Zwecken des Städtebaus weiterzugeben.

Die Ermächtigungsgrundlage für die Datenübermittlung des Schornsteinfegers in seiner Funktion als öffentlich bestellter Schornsteinfeger bilden somit § 3 Abs. 1 SächsDSDG und § 4 Abs. 2 Satz 4 BauGB sowie § 19 Abs. 5 Satz 2 Halbsatz 2. SchfHwG.

Etwas anderes würde sich aber dann ergeben, wenn der oder die Schornsteinfeger/in Daten erheben würde zu Zwecken privater Dienstleistungen. Dann wäre sie/er insoweit – diese Differenzierung spielt hier eine tragende Rolle – kein/e Beliehene/r. Für die Datenweitergabe wäre dann keine (landesrechtliche) Ermächtigungsgrundlage gegeben, und diese wäre zumindest ohne vorliegende Einwilligung datenschutzrechtswidrig, § 19 Abs. 5 Satz 2 Halbsatz 2. SchfHwG.

2.2.8 Corona als Berufskrankheit, Umfang der Datenerhebung

↗ BKV, SGB I, SGB VII

Eine Petentin wandte sich an mich, da sie der Auffassung war, dass eine meiner Kontrolle unterliegende gesetzliche Unfallkasse von ihr in unzulässigem Umfang Daten fordere. Sie hatte die Anerkennung ihrer Erkrankung an Corona als Berufskrankheit beantragt und rügte, dass nach ihren privaten Kontakten zu an Corona erkrankten Personen gefragt werde.

Die gesetzliche Unfallkasse hat in ihrer Stellungnahme mitgeteilt, dass aufgrund des Antrags der Petentin ein Prüfverfahren zur Anerkennung ihrer Covid-19-Infektion als Berufskrankheit (BK) nach der Nr. 3101 der Anlage 1 zur Berufskrankheitenverordnung (BKV) erfolgt. Als Erzieherin und damit Mitarbeiterin im Bereich der Wohlfahrtspflege unterliegt sie dem relevanten Personenkreis, für den die Covid-19-Infektion als Berufskrankheit nach § 9 Siebtes Buch Sozialgesetzbuch (SGB VII) in Verbindung mit den Tatbestandsvoraussetzungen zur BK-Nr. 3101 BKV zu prüfen ist.

Die Deutsche Gesetzliche Unfallversicherung (DGUV) hat aufgrund bisheriger wissenschaftlicher Erkenntnisse zur Infektion und Ansteckung Handlungsempfehlungen erarbeitet, um eine möglichst einheitliche Prüfung der haftungsbegründenden Kausalität und eine einheitliche rechtliche Verfahrensweise sicherzustellen. Diese Handlungsempfehlungen bilden im Zusammenhang mit den Tatbestandsmerkmalen der BK 3101 nach BKV die Grundlagen der Ermittlungen der gesetzlichen Unfallkasse.

Der Nachweis der haftungsbegründenden Kausalität für eine Covid-19-Infektion als Berufskrankheit ist erbracht, wenn die berufliche Verursachung überwiegend wahrscheinlich ist. Zur Klärung dieses Nachweises hatte die Antragstellerin gemäß § 60 Sozialgesetzbuch Erstes Buch (SGB I) im Rahmen ihrer Mitwirkungspflichten die notwendigen Angaben zu erbringen.

Soweit sich im Rahmen der Ermittlungen herausstellt, dass ein intensiver beruflicher Kontakt zu einer infizierten Person aus dem Arbeitsumfeld (Indexperson) nachweisbar ist, ist der Kausalzusammenhang bei der BK-Nr. 3101 in der Regel gegeben, wenn die versicherte Person während des infrage kommenden Ansteckungszeitraums bei ihrer versicherten Tätigkeit

- einen intensiven Kontakt zu mindestens einer nachgewiesenen beruflichen Infektionsquelle (zum Beispiel Patientinnen und Patienten, Kolleginnen und Kollegen, Besucherinnen und Besucher, Untersuchungsmaterialien usw.) hatte,
- nach der Art des Kontaktes eine Infektionsübertragung dabei konkret möglich war und
- Umstände aus dem unversicherten Bereich oder eine ausgeprägte Ubiquität des Infektionserregers einem Schluss auf die Wahrscheinlichkeit des Zusammenhangs mit der versicherten Tätigkeit nicht entgegenstehen.

Für den letzten Punkt der Beurteilungskriterien ist die Frage nach privaten Kontakten zu Covid-19-Erkrankten in den letzten vier Wochen vor der eigenen Infektion relevant. Hier sind wenigstens die Initialen der Kontaktperson sowie der Diagnosezeitpunkt der Kontaktperson anzugeben. Diese Daten dienen ausschließlich der Bewertung und Beurteilung, ob neben der beruflichen Gefährdungsquelle gleichermaßen eine Infektion im außerberuflichen Bereich erfolgt sein könnte. Im Ergebnis ist diese Frage im Gesamtbild relevant für eine Entscheidung zur Anerkennung beziehungsweise Ablehnung der Berufskrankheit.
Den mir vorgelegten Handlungsempfehlungen der DGUV ist zu entnehmen, dass für die haftungsbegründende Kausalität zu prüfen ist, ob „Umstände aus dem unversicherten Bereich oder eine ausgeprägte Ubiquität des Infektionserregers einem Schluss auf die Wahrscheinlichkeit des Zusammenhangs mit der versicherten Tätigkeit nicht entgegenstehen". Dies ist erforderlich, um auszuschließen, dass sich die Petentin außerhalb der Arbeit angesteckt habe. Die Frage nach pri-

vaten Kontakten zu Covid-19-Erkrankten in den letzten vier Wochen vor der eigenen Infektion ist daher datenschutzrechtlich zulässig. Dabei beschränkt sich die gesetzliche Unfallkasse auf die Initialen der Kontaktperson sowie den Diagnosezeitpunkt der Kontaktperson. Deshalb sehe ich den Umfang der erhobenen Daten als erforderlich an.

2.2.9 Grundstücksbezogene Auskünfte aus der Kaufpreissammlung beim Gutachterausschuss

↗ § 91 SGB XII, § 67a SGB I, § 60 SGB I, § 10 SächsGAVO

Ein (ehemaliger) Sozialleistungsempfänger wandte sich an mich, nachdem er von seinem Sozialamt einen Rückforderungsbescheid erhalten hatte. Dem Schriftverkehr zwischen Sozialamt und Sozialhilfeempfänger war zu entnehmen, dass dem Petenten – bis zur Veräußerung in seinem Miteigentum stehender Grundstücke – darlehensweise Sozialhilfeleistungen auf Grundlage des § 91 Siebtes Buch Sozialgesetzbuch (SGB XII) gewährt worden waren, verbunden mit dem Hinweis, eine erfolgte Veräußerung dem Amt mitzuteilen. Eine entsprechende Mitteilung über die Veräußerung war indes trotz Aufforderung seitens des Petenten unterlassen worden; vielmehr hatte das Sozialamt erst durch den Gutachterausschuss des Landkreises von dem Verkauf und der Kaufpreishöhe erfahren.

Nach Prüfung der Sach- und Rechtslage unter Einholung einer Stellungnahme des Sozialamts konnte ich im Ergebnis einen datenschutzrechtlichen Verstoß hier nicht erkennen:

Nicht selbstgenutztes Wohneigentum ist sozialhilferechtlich zu berücksichtigendes Vermögen. Dessen konkreter Wert war hier zum Zeitpunkt der Leistungsbeantragung weder bekannt noch sachkundig festgestellt. Bevor eine Entscheidung getroffen werden kann, inwieweit Leistungen unter Berücksichtigung von Vermögen darlehensweise, gegebenenfalls unter entsprechender dinglicher Sicherung gewährt werden können, bedarf es in derartigen Fällen zunächst der Wertermittlung. Unter diesen Voraussetzungen ist die zur Aufgabenerfüllung

des Sozialamtes erforderliche Datenerhebung nach § 67a Abs. 1 SGB I erlaubt. Sie erfolgte hier dabei nicht durch die Behörde selbst, sondern im Rahmen eingeforderter Mitwirkung gemäß § 60 Abs. 1 SGB I. Der Petent war im Bewilligungsbescheid gebeten worden, die Erstellung eines entsprechenden Verkehrswertgutachtens zu beantragen. Hierfür wird nach Mitteilung des Sozialamts regelmäßig ein entsprechendes Schreiben zur Verfügung gestellt. Es enthält eine Angabe zur Zweckbindung sowie den Hinweis auf die Kostenfreiheit. Der unterschriebene Antrag wurde im vorliegenden Fall vom Petenten offensichtlich nicht an den Gutachterausschuss, sondern an das Sozialamt gesandt. Daher erfolgte die Versendung durch die Behörde. Eine selbstständige Datenabfrage und Datenerhebung beim Gutachterausschuss sei indes seitens der Sozialbehörde selbst zu keinem Zeitpunkt erfolgt.

Das betreffende Sozialamt war auf Grundlage des § 67a SGB X berechtigt, bei der zulässigen Überprüfung der Rückforderung der gezahlten Sozialleistung den konkreten Kaufpreis zu erfahren: Die Erhebung von Sozialdaten durch die in § 35 des Ersten Buches genannten Stellen ist zulässig, wenn ihre Kenntnis zur Erfüllung einer Aufgabe der erhebenden Stelle nach diesem Gesetzbuch erforderlich ist. Dass der Petent zum Zeitpunkt der Rückforderung nicht mehr im Leistungsbezug stand, ist unbeachtlich, das Sozialamt ist zur Überprüfung der gewährten Leistungen berechtigt, dies wurde dem Petenten auch bereits im Leistungsbescheid des Sozialamts dargelegt.

Im Hinblick auf § 10 der Sächsischen Gutachterausschussverordnung (SächsGAVO) ist eine grundstücksbezogene Auskunft zulässig. Denn auf schriftlichen Antrag sind grundstücksbezogene Auskünfte aus der Kaufpreissammlung zu erteilen, soweit die Empfängerin oder der Empfänger ein berechtigtes Interesse an der Kenntnis der Informationen glaubhaft macht, überwiegende schutzwürdige Interessen der oder des Betroffenen nicht entgegenstehen und eine sachgerechte Verwendung der Informationen gewährleistet erscheint. Vom Vorliegen eines berechtigten Interesses und der sachgerechten Verwendung der Informationen ist regel-

mäßig auszugehen, wenn die Auskunft von einer Behörde im Rahmen der Erfüllung ihrer Aufgaben für eine Wertermittlung beantragt wird.
Diese Voraussetzungen waren hier allesamt erfüllt.

2.2.10 Schwebender Rechtsstreit und Beitragsschulden – Welche Informationen dürfen Vereinsmitgliedern gegeben werden?

↗ § 26, § 27 Abs. 3 BGB, § 666 BGB, Art. 6 Abs. 2 in Verbindung mit Abs. 1 Buchst. c DSGVO, Art. 6 Abs. 1 Buchst. b, f DSGVO

Im Rahmen einer Mitgliederversammlung informierte der Vorsitzende eines Kleingartenvereins die anwesenden Vereinsmitglieder über den Inhalt eines Rechtsstreits mit einem der Anwesenden unter namentlicher Nennung des betroffenen Mitglieds. Dabei verlas er nach dessen Darstellung die Klagepunkte und gab weitere Details aus dem schwebenden Verfahren preis, gefolgt von einer öffentlichen Rüge des Fehlverhaltens. Später hätte dann die Schatzmeisterin noch die Namen der säumigen Zahlerinnen und Zahler, dies betraf unter anderem abermals dasselbe Mitglied, sowie deren Gartennummer genannt. Daraufhin sei es zu verbalen Anfeindungen gegenüber dem Vereinsmitglied gekommen. Diese sah sich zu Unrecht an den Pranger gestellt und wandte sich mit der Wiedergabe eines Erinnerungsprotokolls an meine Behörde.
Der Verein wähnte sich mir gegenüber im Recht und begründete die Informationsweitergabe zum schwebenden Rechtsstreit sowie zu den säumigen Gartenfreunden mit der Wahl eines neuen Vorstands. Dort antretende Mitglieder müssten eine Gewähr für rechtskonformes Verhalten bieten. Das Mitglied habe indes mehrfach unzulässige Baumaßnahmen im Pachtgarten vorgenommen, von denen eine offensichtlich auch Gegenstand des schwebenden Rechtsstreits war. Der Verein erkannte darin ein überragendes Informationsbedürfnis der anwesenden Vereinsmitglieder und sah sich gar selbst in der Darlegungspflicht, allein um einer Wahlanfechtung zu entgehen. Deshalb hätte auch nicht bis zum rechtskräfti-

gen Abschluss des Rechtsstreits abgewartet werden können. Neben einer persönlichen Haftung des Vorstands sei ferner die Gemeinnützigkeit des Vereins in Gefahr gewesen.

Die Namen der säumigen Beitragszahler/innen sowie des sich im Rechtsstreit befindlichen Vereinsmitglieds stellen personenbezogene Daten dar, vgl. Art. 4 Nr. 1 Datenschutz-Grundverordnung (DSGVO). Aber nicht erst der Name ist erforderlich, um eine Zuordnung zu einer natürlichen Person herzustellen, sondern auch andere Kennungen wie vorliegend eine Parzellennummer reichen hierzu aus. Die Preisgabe dieser personenbezogenen Daten gegenüber den übrigen Vereinsmitgliedern, auch wenn vereinsfremde Personen keinen Zutritt zur Versammlung hatten, ist eine Offenlegung im Sinne des Art. 4 Nr. 2 DSGVO. Denn Vereinsmitglieder gelten – mit Ausnahme der betroffenen Person selbst – aus Datenschutzsicht als Dritte (Art. 4 Nr. 10 DSGVO). Die im Bericht des Vorsitzenden getätigten Äußerungen sind dem Verein als juristischer Person zuzurechnen, § 26 Abs. 1 Bürgerliches Gesetzbuch (BGB). Demzufolge gilt auch der Verein als datenschutzrechtlicher Verantwortlicher (Art. 4 Nr. 7 DSGVO).

Zwar besteht in der Tat eine Rechenschaftspflicht des Vereins gegenüber den Mitgliedern (§ 27 Abs. 3 in Verbindung mit § 666 BGB). Diese beinhaltet jedoch keine Pflicht zur Preisgabe datenschutzrechtlich relevanter Informationen einzelner Mitglieder (Art. 6 Abs. 2 DSGVO). Der Verein konnte sich damit nicht auf den Erlaubnistatbestand des Art. 6 Abs. 1 Buchst. c DSGVO (Erforderlichkeit zur Erfüllung einer rechtlichen Verpflichtung) beziehen. Die preisgegebenen Daten standen auch nicht in unmittelbarem Zusammenhang mit der Durchführung des Mitgliedschaftsverhältnisses (Art. 6 Abs. 1 Buchst. b DSGVO). In der Folge war die rechtliche Beurteilung nur nach Art. 6 Abs. 1 Buchst. f DSGVO vorzunehmen. Besteht danach ein berechtigtes Interesse des Verantwortlichen oder eines Dritten und ist die Verarbeitung zur Interessenwahrung auch erforderlich, so dürfen zusätzlich die Interessen der betroffenen Person nicht schwerer wiegen. Zur Erfüllung der Rechenschaftspflicht des Vereins – wollte man darin ein berechtigtes Verarbeitungsinteresse sehen –

reichen allgemeine Hinweise auf einen offenen Rechtsstreit mit Darstellung der wesentlichen Streitpunkte aus, um dieser Genüge zu tun. Auch gegen Informationen zum Verfahrensstand sowie etwaiger Kostenrisiken habe ich nichts einzuwenden. Ausstehende Beitragszahlungen betreffen einzig das jeweilige individuelle Mitgliedschaftsverhältnis. Dementsprechend ist es ausreichend, wenn die Vereinsmitglieder Kenntnis über den Umstand ausstehender Zahlungen, die Anzahl der (vermeintlich) säumigen Beitragszahler/innen sowie die Höhe der ausstehenden Mitgliedsbeiträge erhalten. Ungeachtet dessen hat ein sich in einer laufenden gerichtlichen Auseinandersetzung mit dem Verein befindliches Mitglied in jedem Fall ein höheres Schutzinteresse als der Verein und auch die anwesenden Vereinsmitglieder. Es muss letzten Endes nicht hinnehmen, dass nicht abschließend entschiedene Sachverhalte in einer Versammlung offen kommuniziert werden. Voraussetzung für eine zulässige Weitergabe ist, dass die dargestellten Informationen belastbar sind. In Anbetracht des offenen Ausgangs eines schwebenden Rechtsstreits kommt eine uneingeschränkte Preisgabe von Detailinformationen jedoch einer Prangerwirkung gleich. Die Vereinsmitglieder, bei denen noch Beitragszahlungen ausstehen, müssen ihre namentliche Aufzählung aus den gleichen Gründen nicht schutzlos hinnehmen.

Eine datenschutzrechtliche Beurteilung erfolgt ausschließlich faktenbasiert, vollzieht sich nach objektiven Kriterien und nicht auf Basis von Wahrscheinlichkeiten oder subjektiven Wertungen. Letzten Endes kommt somit dem Gewicht und der Qualität der preisgegebenen Daten entscheidende Bedeutung zu.

Alles in allem lässt sich feststellen, dass eine Preisgabe von Sachverhalten, die ein einzelnes Mitglied betreffen, nicht per se ausgeschlossen und automatisch datenschutzwidrig ist. Indes müssen die das konkrete Vereinsmitglied betreffenden Informationen auf Tatsachen beruhen und belastbar sein. Begriffsimmanent kommt schwebenden, mithin noch nicht rechtskräftig abgeschlossenen (Gerichts-)Verfahren keine Tatsachenwirkung zu. Haftungsfragen oder auch die

Gefahr einer möglichen Wahlanfechtung ebenso wie des Verlusts der Gemeinnützigkeit gründen sich einzig auf vagen Befürchtungen und sind deshalb nicht geeignet, eine uneingeschränkte Preisgabe personenbezogener Daten zu rechtfertigen.

Was den konkreten Beschwerdefall angeht, ließ sich aufgrund sich widersprechender Parteiaussagen nicht zweifelsfrei ermitteln, welche Details zum laufenden Rechtsstreit der Vereinsvorsitzende tatsächlich in der Versammlung erwähnt hat. Ich konnte mich daher auf eine datenschutzrechtliche Belehrung des Vereins beschränken, um im Verein zumindest das Bewusstsein für einen sensiblen Umgang mit den Mitgliederdaten zu schärfen. Wegen der nicht bestrittenen namentlichen Erwähnung der säumigen Vereinsmitglieder stellte ich dem Verein gegenüber einen Datenschutzverstoß fest.

Was ist zu beachten?
Die namentliche Nennung säumiger Beitragszahlerinnen und -zahler ist nicht von der Rechenschaftspflicht eines Vereins gedeckt. Gleiches gilt für Detailinformationen aus einem schwebenden Rechtsstreit. Gegenüber Vereinsmitgliedern kommunizierte Sachverhalte, die ein einzelnes Mitglied betreffen, dürfen nicht strittig sein. Sie müssen abschließend festgestellt und damit belastbar sein.

2.2.11 Zulässigkeit von Verwaltungsermittlungen vor der Einleitung eines Disziplinarverfahrens

↗ § 17 SächsDG, § 111 Abs. 6 SächsBG, § 45 Abs. 2 BeamtStG, DSGVO

Mich erreichte die Beschwerde eines Polizeibeamten, der mitteilte, seine Dienststelle habe die Kinderärztin seines Kindes zur Stellungnahme und Informationsweitergabe über die Behandlung des Kindes aufgefordert. Die von mir um Stellungnahme gebetene Polizeidirektion (PD) bestätigte diese Darstellung und begründete ihr Vorgehen damit, dass es sich bei dem Schreiben an die Kinderärztin um eine zulässige Verwaltungsermittlung gehandelt habe. Dies sei zur Klärung und Prüfung, ob entsprechend § 17 Sächsisches Disziplinargesetz (SächsDG) zureichende tatsächliche Anhaltspunkte vorlägen, die den Verdacht eines Dienstvergehens des Petenten rechtfertigen würden, infolge dessen die PD ein Disziplinarverfahren einzuleiten habe, erforderlich gewesen, um die zunächst bloße Vermutung einer Dienstpflichtverletzung zu erhärten oder auszuräumen.

Dieser Einschätzung der PD konnte ich nicht folgen.

Verwaltungsermittlungen sind Maßnahmen des Dienstvorgesetzten vor Einleitung eines Disziplinarverfahrens, um allgemeine Verdächtigungen gegen seine Behörde oder gezielte Beschuldigungen gegen einzelne Beamte aufzuklären, die die Möglichkeit eines Dienstvergehens einschließen, aber personell oder sachlich noch nicht hinreichend konkretisiert sind. Zur grundsätzlichen Zulässigkeit, den Vorrausetzungen sowie Grenzen von Verwaltungsermittlungen hat mein Amtsvorgänger bereits im 12. Tätigkeitsbericht für den öffentlichen Bereich (2005) auf Seite 63ff. Stellung genommen. Im 13. Tätigkeitsbericht für den öffentlichen Bereich (2007) auf Seite 59ff. und dem 14. Tätigkeitsbericht für den öffentlichen Bereich (2009) auf Seite 37ff. ist er nochmals auf die Betroffenenrechte und auf die Thematik der Archivierung eingegangen.

Vorliegend wurde gegen den Petenten zwar (später) ein Disziplinarverfahren eingeleitet. Die an die Kinderärztin gerichtete schriftliche Bitte der PD um Auskunft bezüglich des Kindes des Petenten erfolgte aber zeitlich noch vor der Einleitung des Verfahrens. Konkret teilte die PD der Kinderärztin dabei mit, dass der Petent Beamter der PD ist, und übermittelte weitere dienstliche Informationen, bei denen es sich um personenbezogenen Daten im Sinne von Art. 4 Nr. 1 Datenschutz-Grundverordnung (DSGVO) handelte. Diese Übermittlung stellt eine Datenverarbeitung gemäß Art. 4 Nr. 2 DSGVO dar. Zudem bat die PD die Kinderärztin um Auskunft zu Gesundheitsdaten des Kindes im Sinne von Art. 9 DSGVO.

Auch im Beamtenverhältnis bedürfen Eingriffe in verfassungsmäßige Rechtspositionen des betroffenen Bediensteten – hier dessen Recht auf informationelle Selbstbestimmung – einer gesetzlichen Ermächtigung. Ermittlungshandlungen des Dienstvorgesetzten führen regelmäßig dazu, dass die Grundrechtssphäre des Beamten tangiert wird. Je konkreter die Ermittlungen auf einen bestimmten Beamten und einen eingegrenzten Lebenssachverhalt hinauslaufen, umso stärker beeinträchtigen sie den Rechtskreis des Beamten. Die Grundrechtsrelevanz der oben genannten Datenverarbeitung stand im vorliegenden Fall – insbesondere hinsichtlich

der Gesundheitsdaten des Kindes – außer Frage. Nach Art. 9 Abs. 1 DSGVO handelt es sich bei Gesundheitsdaten um besondere Kategorien personenbezogener Daten, deren Verarbeitung grundsätzlich untersagt ist. Nur in den von Art. 9 Abs. 2 DSGVO benannten Ausnahmen ist die Verarbeitung zulässig.

Eine gesetzliche Ermächtigungsgrundlage für diesen Eingriff fehlte.

§ 111 Abs. 6 Sächsisches Beamtengesetz (SächsBG) kommt insoweit nicht als Rechtsgrundlage in Betracht. Zwar ermächtigt die Vorschrift zur Erhebung und Verarbeitung personenbezogener Daten zur Vorbereitung personeller Maßnahmen; die Erforschung eines – disziplinarrechtlich relevanten – Sachverhalts durch gezielte Ermittlungsmaßnahmen, die auf Offenlegung bisher unbekannter, gleichwohl vermuteter Tatsachen abzielen, fällt allerdings nicht darunter. Bei der hier untersuchten Verwaltungsermittlung handelt es sich um einen gezielten Grundrechtseingriff, der einer gesetzlichen Ermächtigungsgrundlage bedarf. Der Gesetzgeber gesteht dem Dienstvorgesetzten Ermittlungs- und Beweiserhebungsbefugnisse (§ 24 SächsDG) nur im förmlich eingeleiteten Disziplinarverfahren zu; das gewährleistet den erforderlichen Grundrechtsschutz. Ein gegen den Beamten gerichtetes Disziplinarverfahren war aber zum Zeitpunkt der Anfrage der PD an die Kinderärztin gerade noch nicht förmlich eingeleitet. Zudem erklärt § 111 Abs. 6 SächsBG die Datenverarbeitung durch den Dienstvorgesetzten nur hinsichtlich personenbezogener Daten des Beamten selbst, nicht Dritter (wie hier des Kindes), für zulässig.

Lediglich im Einzelfall und ausnahmsweise können auch ohne gesetzliche Grundlage Verwaltungsermittlungen des Dienstvorgesetzten vor Einleitung des Disziplinarverfahrens zulässig sein, weil und soweit sie auf die beamtenrechtliche Fürsorge- und Schutzpflicht des Dienstherrn zurückgeführt werden können. Nach § 45 Satz 2 Beamtenstatusgesetz (BeamtStG) hat der Dienstherr die Beamten insbesondere bei ihrer amtlichen Tätigkeit und in ihrer Stellung zu schützen. Bestehen Vorwürfe Dritter hinsichtlich der Verletzung beamtenrechtlicher Dienst-

pflichten, ist der Dienstherr zur Aufklärung der Anschuldigung verpflichtet, sofern deren Berechtigung nicht feststeht (unter anderem Oberverwaltungsgericht Lüneburg vom 13.02.2007 – 5 ME 62.07). Bei der Durchführung von Verwaltungsermittlungen muss aber stets die Grenze zu § 17 Abs. 1 Satz 1 SächsDG eingehalten werden. Der Dienstvorgesetzte eines Beamten, gegen den der Verdacht eines Dienstvergehens durch Vorliegen zureichender tatsächlicher Anhaltspunkte gerechtfertigt ist, hat gemäß § 17 Abs. 1 SächsDG ein Disziplinarverfahren einzuleiten. Die Bestimmung des § 17 Abs. 1 Satz 1 SächsDG wird vom Verfolgungsgrundsatz beherrscht, demzufolge dem Dienstvorgesetzten die „Dienstpflicht" zur Einleitung eines Disziplinarverfahrens obliegt, wenn die Voraussetzungen – ein hinreichend konkreter Verdacht eines Dienstvergehens – hierfür vorliegen. Bloße Vermutungen reichen indes nicht aus. Sobald im Sinne von § 17 Abs. 1 SächsDG zureichende tatsächliche Anhaltspunkte gewonnen worden sind, die den Verdacht eines Dienstvergehens rechtfertigen, dürfen die notwendigen Ermittlungen, etwa die Einholung schriftlicher Auskünfte von Zeugen nach § 24 Abs. 1 Satz 2 Nr. 2 SächsDG, nur noch im Rahmen eines Disziplinarverfahrens durchgeführt werden (unter anderem BVerwG vom 27.12.2017 – 2 B 41/17). Die PD hatte zwar bereits mehrere Wochen vor Einleitung des Disziplinarverfahrens und noch vor dem Schreiben an die Kinderärztin in einem internen Vermerk festgestellt, dass der Petent eine Dienstpflichtverletzung begangen habe, und um die Einleitung eines Disziplinarverfahrens gebeten. Das Disziplinarverfahren gegen den Petenten wäre gemäß § 17 Abs. 1 SächsDG zu diesem Zeitpunkt einzuleiten gewesen, und der Petent hätte nach § 20 Abs. 1 SächsDG darüber unverzüglich unterrichtet werden müssen. Beides erfolgte zu diesem Zeitpunkt jedoch nicht.

Das Verfolgungsgebot in § 17 SächsDG entfaltete damit Sperrwirkung dahingehend, dass jegliche Verwaltungsermittlungen – hier die an die Kinderärztin gerichtete Bitte um Auskunft – nach Auftreten des hinreichend konkreten Verdachts eines Dienstvergehens und vor förmlicher Einleitung des Disziplinarverfahrens unzulässig waren.

Was ist zu beachten?
Das Verfolgungsgebot in § 17 SächsDG entfaltet Sperrwirkung dahingehend, dass jegliche Verwaltungsermittlungen nach Auftreten des hinreichend konkreten Verdachts eines Dienstvergehens von Rechts wegen ausgeschlossen sind.

Im Ergebnis der Prüfung der datenschutzrechtlichen Beschwerde habe ich die PD wegen des festgestellten Verstoßes gegen datenschutzrechtliche Vorschriften – konkret gegen die Pflicht, personenbezogene Daten rechtmäßig zu verarbeiten, Art. 5 Abs. 1 Buchst. a DSGVO sowie Art. 9 Abs. 1 DSGVO – gemäß Art. 58 Abs. 2 Buchst. b DSGVO verwarnt.
Was ist zu beachten?
Das Verfolgungsgebot in § 17 SächsDG entfaltet Sperrwirkung dahingehend, dass jegliche Verwaltungsermittlungen nach Auftreten des hinreichend konkreten Verdachts eines Dienstvergehens von Rechts wegen ausgeschlossen sind.

2.2.12 Kommunale Statistikerhebungen und das Sächsische Mietspiegel-Zuständigkeitsgesetz

↗ §§ 558ff. BGB, § 6 Abs. 3 und § 8 Abs. 1 Satz 1 SächsStatG, § 3ff. Mietspiegelverordnung, Art. 229 § 62 EGBGB, SächsMsZustG

Im Berichtszeitraum erreichte mich die Anfrage eines im Immobilienbereich Tätigen, der monierte, eine sächsische Stadt erhebe Daten zur Vorbereitung ihres nächsten Mietspiegels. Da aber hierfür (derzeit) eine Rechtsgrundlage für die Kommune fehle, sei diese Befragung unzulässig.
Ich habe mich dieser Auffassung so nicht anschließen können. Tatsächlich wurde im Juni 2021 vom Deutschen Bundestag das Gesetz zur Reform des Mietspiegelrechts (Mietspiegelreformgesetz) beschlossen (Beschlussempfehlung Bundestagsdrucksache 19/30933). Die bundesgesetzliche Neuregelung, die außer der jetzigen Fassung der §§ 558c und 558d Bürgerliches Gesetzbuch (BGB) auch bestimmte Verfahrensregelungen enthält (Änderung des Artikels 229 und Einfügung eines Artikels 238 in das Einführungsgesetz zum Bürgerlichen Gesetzbuche {EGBGB}) ist am 01.07.2022 in Kraft getreten. § 558 Abs. 4 Satz 2 BGB ordnet nunmehr an, dass für Gemeinden mit mehr als 50.000 Einwohnerinnen und Einwohnern Mietspiegel zu erstellen sind. Bisher war die Erstellung für die Kommunen unabhängig von der Größe eine freiwillige Aufgabe, für Gemeinden unterhalb dieser Grenze

bleibt dies auch dabei. Art. 229 § 62 EGBGB enthält hierzu Übergangsregelungen: Für Gemeinden, die nach der neuen Rechtslage erstmalig verpflichtet sind, einen Mietspiegel zu erstellen, ist dieser bis spätestens 01.01.2023 zu erstellen und zu veröffentlichen; erstellt die Gemeinde in Erfüllung dieser Verpflichtung einen qualifizierten Mietspiegel, so läuft diese Frist bis zum 01.01.2024.

Das Gesetz unterscheidet dabei zwischen qualifizierten Mietspiegeln, nämlich solchen, die nach anerkannten wissenschaftlichen Grundsätzen erstellt und von der nach Landesrecht zuständigen Behörde oder von Interessenvertretern der Vermieter und der Mieter anerkannt worden ist (§ 558d Abs. 1 Satz 1 BGB), und anderen Mietspiegeln, die diese Anforderungen nicht erfüllen, sogenannte einfache Mietspiegel. Welche Art von Mietspiegel eine Gemeinde unter oder über 50.000 Einwohnerinnen und Einwohnern aufstellt, regelt das Gesetz nicht, es obliegt der Entscheidung der Kommune, welche Art von Mietspiegel sie erstellen möchte. § 558c Abs. 5 BGB ermächtigt die Bundesregierung, eine Rechtsverordnung über den näheren Inhalt von Mietspiegeln und das Verfahren zu der Aufstellung und Anpassung einschließlich Dokumentationen und Veröffentlichung zu erlassen.

Von dieser Ermächtigung hat die Bundesregierung durch die Mietspiegelverordnung vom 28.10.2021 Gebrauch gemacht. In ihr werden sowohl qualifizierte als auch einfache Mietspiegel angesprochen:

Für die einfachen Mietspiegel bedarf es nach § 3 der Verordnung vorbehaltlich der in den §§ 4 und 5 geregelten Fragen der Dokumentation und der Veröffentlichung keines besonderen Verfahrens.

Für die qualifizierten Mietspiegel enthalten §§ 6ff. der Verordnung umfassende Regelungen. Die Besonderheit ist dabei, dass zur Erstellung eines qualifizierten Mietspiegels den Eigentümerinnen bzw. Eigentümern und Mieterinnen bzw. Mietern von Wohnraum eine gesetzliche Verpflichtung auferlegt wird, die notwendigen Auskünfte zu erteilen, insbesondere zu den dort geregelten Erhebungsmerkmalen und Hilfsmerkmalen, Art. 238 § 2 EGBGB. Diese Pflicht besteht auch bei

Gemeinden unter 50.000 Einwohnern (die ja nicht zur Erstellung von Mietspiegel verpflichtet sind), wenn sie sich denn zu einem solchen qualifizierten Mietspiegel entschließen.

In Sachsen fehlte es bis vor Kurzem an einer Regelung, die festlegte, wer „die nach Landesrecht zuständige Behörde" im Sinne des neugefassten BGB sein sollte. Diese Regelung wurde nunmehr mit dem Gesetz über die Zuständigkeiten zur Erstellung von Mietspiegeln (SächsMsZustG), das im Dezember 2022 den Landtag passierte, geschaffen (SächsGVBl. 2022, 766). Damit sind die Gemeinden entsprechend den Anforderungen nach Art. 83 Verfassung des Freistaates Sachsen (SächsVerf) nunmehr per Gesetz als die nach Landesrecht zuständigen Behörden (§ 558d Abs. 1 Satz 1 BGB) bestimmt.

Im Ergebnis war festzuhalten:

Kommunale Mietspiegel sind Kommunalstatistiken im Sinne des § 8 Abs. 1 Satz 1 Sächsisches Statistikgesetz (SächsStatG). Als solche bedürfen sie aufgrund § 8 Abs. 1 Satz 2, 1. Halbsatz dieses Gesetzes auch weiterhin einer Satzung.

Die Satzung der hier betroffenen Stadt, die die Grundlage für die infrage gestellte Datenerhebung bildete, enthielt keine Auskunftspflicht; vielmehr legte § 5 Abs. 3 der Satzung ausdrücklich eine freiwillige Auskunftserteilung fest.

Als einfacher Mietspiegel ist seit dem 01.07.2022 jeder Mietspiegel anzusehen, der nicht in vollem Umfang die neuen bundesgesetzlichen Anforderungen an den Inhalt eines qualifizierten Mietspiegels erfüllt, gleichviel, wie mehr oder weniger weitgehend er hinter diesem Katalog zurückbleibt. Aber auch wenn er diesen Katalog etwa umfassen sollte, ist es auch dann kein qualifizierter Mietspiegel, wenn seiner Datenerhebung keine Auskunftspflicht zugrunde liegt; denn diese ist nach den BGB-Vorschriften zwingende Grundlage von qualifizierten Mietspiegeln.

Da das neue Bundesgesetz für einfache Mietspiegel keine besonderen Anforderungen aufstellt, bestanden in dem hier monierten Fall keine Bedenken dagegen, dass derartige Befragungen, soweit sie auf der Grundlage einer Satzung in Gang gesetzt wurden, als freiwillige Maßnahme fortgeführt werden können. Es bedurfte daher nicht erst des oben ge-

nannten Sächsischen Zuständigkeitsgesetzes, da sich die Zuständigkeit der Gemeinde hierfür weiterhin aus den genannten Bestimmungen des Sächsischen Statistikgesetzes, konkret § 8 SächsStatG, ergibt. Allerdings – wie erwähnt – führt eine solche Befragung auf freiwilliger Grundlage lediglich zur Erstellung eines einfachen Mietspiegels.
Um zu einem qualifizierten Mietspiegel im Sinn des neuen Bundesrechts zu gelangen, war für die betroffene Stadt daher nur der folgende Weg offen:

- nach Inkrafttreten des zuständigkeitsbegründenden Landesgesetzes ihre bereits in Beschlussvorlage befindliche neue Satzung zu beschließen,
- erst dann mit der Erhebung zu beginnen,
- dabei die Erfüllung der gesetzlichen Auskunftspflichten der Betroffenen einzufordern und
- aus den Ergebnissen den Mietspiegel zu erstellen.

2.2.13 Rückgabe gekaufter Ware (Rückabwicklung von Kaufverträgen) nur bei Angabe der Kundendaten?

↗ Art. 6 Abs. 1 Satz1 Buchst. b und f DSGVO

Mehrere Kundinnen und Kunden des stationären Handels beschwerten sich darüber, dass bei der Rückgabe gekaufter Waren (das heißt Rückabwicklung von Kaufverträgen) die Händlerinnen bzw. Händler den Namen und die Adressdaten der Käuferinnen und Käufer notieren wollen, weil anderenfalls der Verkauf nicht rückabgewickelt werden könne. Konkret handelte es sich um die Rückgabe mangelhafter Schuhe und von noch im Original verpacktem Spielzeug, wohl aufgrund von Kaufreue, das heißt die Rückabwicklung erfolgte aufgrund der Kulanz des Verkäufers.
Meine Behörde teilte den Petentinnen und Petenten mit, dass dieses Verhalten keinen Datenschutzverstoß darstellt. Verkäuferinnen bzw. Verkäufer können bei der Rückabwicklung eines Kaufvertrages personenbezogene Daten wie Name und Adresse der Käuferin bzw. des Käufers verlangen und diese auch speichern. Dies gilt auch für Fälle, in denen die Käufe-

rin bzw. der Käufer die Ware bar gekauft hatte und die Verkäuferin bzw. der Verkäufer ursprünglich über keine weiteren Informationen zur Käuferin bzw. zum Käufer verfügte.

Abgesehen von den Kulanzfällen, bei denen die Rücknahme für die Verkäuferin bzw. den Verkäufer wie ein Ankauf von Waren zu betrachten ist, ist nicht ausgeschlossen, dass die Verkäuferin bzw. der Verkäufer nach einer Prüfung des von der Käuferin oder dem Käufer behaupteten Mangels diesen zurückweist und auf Vertragserfüllung besteht. Daraus könnte sich auch ein Rechtsstreit entwickeln. Die Verkäuferin bzw. der Verkäufer hat demzufolge ein berechtigtes Interesse gemäß Art 6 Abs. 1 Satz 1 Buchst. f Datenschutz-Grundverordnung (DSGVO), die persönlichen Daten der Vertragspartnerin bzw. des Vertragspartners wie Name und Anschrift zu speichern, um seine Ansprüche gegebenenfalls durchsetzen zu können oder auch schon vorher bei Rücksprachen zur Klärung der Angelegenheit zu kommunizieren.

Es ist auch denkbar, dass die Verkäuferin bzw. der Verkäufer die Ware nur in Kommission der Herstellerin bzw. des Herstellers vertreibt und diese bzw. dieser dann den Mangel nicht anerkennt. Dann gilt das Gleiche. Gegebenenfalls ist die Berechtigung auch aus Art. 6 Abs. 1 Satz 1 Buchst. b DSGVO, „zur Erfüllung eines Vertrages", zu entnehmen, da ein Kaufvertrag geschlossen worden und hier die Erfüllung bzw. die Rückabwicklung des Kaufvertrages zu klären ist.

Was ist zu beachten?
Das Verlangen der Verkäuferin bzw. des Verkäufers nach Namen und Anschriften der Käuferin bzw. des Käufers in Rückgabefällen ist nicht unbillig. Das gilt auch für ursprüngliche Barkäufe.

2.2.14 Unerwartete Telefonanrufe zur Werbung von Mitarbeitenden

↗ Art. 6 Abs. 1 Buchst. f DSGVO

In Zeiten des Personalmangels kam die Personalverwaltung einer Firma auf den Gedanken, in der Belegschaft nach persönlichen Daten ehemaliger befähigter Mitarbeiterinnen und Mitarbeiter zu fragen. Diese sollten dann kontaktiert werden, um sie zum Wiedereintritt in das Unternehmen zu bewegen. Die Anwerbung neuer Mitarbeitender ist grundsätzlich ein legitimer Zweck zur Datenerhebung. Fraglich ist nur, wie dieses Anliegen umgesetzt wird. Im vorliegenden Fall waren

tatsächlich die Kontaktdaten einer früheren Mitarbeiterin im Kollegenkreis noch bekannt. Eine Beschäftigte hatte noch Verbindung zu dieser früheren Mitarbeiterin und teilte dies den Personalverantwortlichen mit. Der Vertriebsleiter fragte diese Beschäftigte nach der Telefonnummer der früheren Kollegin, die sie ihm weitergab. Er nahm dann telefonisch Kontakt mit dieser ehemaligen Mitarbeiterin auf und fragte sie direkt, ob sie Interesse an einer erneuten Tätigkeit im Unternehmen hätte.

Die frühere Mitarbeiterin betrachtete diese Art der Kontaktaufnahme als störend und unangemessen und erhob Beschwerde wegen eines möglichen Datenschutzverstoßes, da ihr nicht verständlich war, weshalb die Firma noch über ihre persönlichen Kontaktdaten verfügte. Sie hatte bereits vor einigen Jahren das Unternehmen verlassen.

Nach den Grundsätzen des Datenschutzes ist es jedenfalls nicht zulässig, ehemalige Beschäftigte unaufgefordert, das heißt ohne deren Einwilligung, anzurufen, um sie als Mitarbeitende zu werben.

Als Erlaubnistatbestand wäre allein ein berechtigtes Interesse gemäß Art. 6 Abs. 1 Buchst. f Datenschutz-Grundverordnung (DSGVO) in Betracht gekommen. Jedoch ist die Erhebung von Daten durch aktives Nachfragen nach und das Speichern von Telefonnummern sowie direkte Anrufe bei ehemaligen Mitarbeitenden dafür nicht erforderlich, das heißt, es gibt weniger schwer in Rechte der Betroffenen eingreifende Mittel. Dazu zählen zum Beispiel die üblicherweise in diesen Fällen verwendeten Stellenausschreibungen in diversen Medien. Ein milderes Mittel wäre es auch gewesen, wenn der Vertriebsleiter die Beschäftigte zuvor gefragt hätte, ob die frühere Mitarbeiterin der Weitergabe ihrer Telefonnummer an ihn zustimmt und ob sie etwas dagegen habe, wegen eines Stellenangebots angerufen zu werden. Direkte Telefonanrufe zur Werbung von Mitarbeiterinnen und Mitarbeitern sind daher – ohne vorherige Einwilligung der Person – unzulässig, vergleichbar dem Rechtsgedanken bei Direktwerbung bzw. unerwarteten Telefonanrufen gemäß § 7 Abs. 2 Nr. 1 des Gesetzes gegen den unlauteren Wettbewerb (UWG).

Was ist zu beachten?

Telefonische Kontaktdaten zur Anwerbung von Arbeitskräften haben ordnungsgemäß erhoben zu sein. Vor telefonischer Kontaktaufnahme ist die Empfangsbereitschaft betroffener Personen zur Ansprache zu klären. In Zweifelsfällen sollte auf eine Zustimmung zur Kontaktaufnahme nicht verzichtet werden.

2.2.15 Dienstliche Kommunikation eines Gerichtsvollziehers über WhatsApp

↗ Art. 32, 44ff. DSGVO

Ein Petent, Schuldner in einem Zwangsvollstreckungsverfahren, informierte mich, dass ein Gerichtsvollzieher in seinen dienstlichen Schreiben die Möglichkeit benennt, Zahlungsnachweise per WhatsApp zu erbringen.
Die dienstliche Nutzung von WhatsApp ist aus Gründen des Datenschutzes unzulässig. Dies gilt sowohl für die dienstliche Kommunikation der am Zwangsvollstreckungsverfahren beteiligten Bediensteten untereinander als auch für die Kommunikation mit der Bürgerin bzw. dem Bürger (Schuldnerin und Schuldner, Gläubigerin und Gläubiger).
Die Verarbeitung personenbezogener Daten in dem hier interessierenden Zusammenhang unterliegt den Anforderungen der Datenschutz-Grundverordnung (DSGVO). Ganz zentral ist dabei die Sicherheit der Verarbeitung nach Art. 32 Abs. 1 DSGVO. Im Zusammenhang mit der Nutzung von WhatsApp kommt es zu einer Übermittlung von Daten in ein Drittland (USA), sodass Art. 44ff. DSGVO zu beachten sind.
Die insofern bestehenden Vorgaben der DSGVO werden bei der Nutzung von WhatsApp verfehlt, da mit der Installation und Nutzung der App folgende Konsequenzen verknüpft sind:

- Übertragung von personenbezogenen Daten an andere Unternehmen des Meta-Konzerns
- Übertragung der Kontakte aus dem Adressbuch des betroffenen Telefons
- Übertragung der personenbezogenen Daten in die USA
- Zugriff auf Metadaten
- Nutzung der personenbezogenen Daten durch WhatsApp

Staatliche Stellen dürfen – selbstverständlich – nicht die auf ihren Smartphones hinterlegten Kontakte Dritter an ein Unternehmen in einem Drittland (mit nicht ausreichendem Datenschutzniveau) weiterleiten. Ebenso wenig sollte bzw. darf die staatliche Stelle einen solchen Kommunikationsweg für Bürgerinnen und Bürger anbieten und so auch die

Übermittlung und Nutzung von deren Daten und von denen Dritter, die als Kontakte gespeichert sind, verursachen oder zumindest fördern.
Die Unzulässigkeit des Einsatzes ergibt sich damit direkt aus der DSGVO, die unsichere und intransparente Datenverarbeitungen verbietet und Übermittlungen in Drittstaaten nur unter engsten Voraussetzungen erlaubt.
Aufgrund der sehr klaren Rechtslage habe ich den verantwortlichen Gerichtsvollzieher aufgefordert, die Nutzung von WhatsApp unverzüglich und mit sofortiger Wirkung einzustellen und die verwendeten Dokumente, in denen auf die Möglichkeit der Nutzung hingewiesen wird, zu überarbeiten. Sollte es sich bei der im Briefkopf angegebenen Mobilnummer um ein Diensthandy handeln, ist das Nutzerkonto bei WhatsApp unverzüglich zu löschen. Zudem habe ich den Vorgang zum Anlass genommen, das zuständige Amtsgericht als Aufsichtsbehörde über das datenschutzwidrige Vorgehen entsprechend zu informieren und aufgefordert, alle Gerichtsvollzieherinnen und Gerichtsvollzieher im Zuständigkeitsbereich entsprechend zu belehren. Ebenso habe ich mich an das Sächsische Staatsministerium der Justiz und für Demokratie, Europa und Gleichstellung gewandt und gebeten, in seinem Geschäftsbereich dafür zu sorgen, dass die Gerichtsvollzieherinnen und Gerichtsvollzieher auf diese Rechtslage hingewiesen werden.

Was ist zu beachten?
Die dienstliche Nutzung von WhatsApp durch Gerichtsvollzieherinnen und Gerichtsvollziehern ist aus Gründen des Datenschutzes unzulässig. Gleiches gilt für die Verwendung des Messengerdienstes durch andere staatliche Stellen.

2.2.16 Gästebewertungen im Internet – wann darf ein Hotel den Gast persönlich ansprechen?

↗ Art. 6 Abs. 1 DSGVO, Art. 58 Abs. 2 DSGVO

Wer möchte nicht vor der Buchung einer Unterkunft sichergehen, dass er die richtige Wahl getroffen hat? Hierzu greift man auf die Gästebewertungen zurück, um sich an den Erfahrungen und Einschätzungen der früheren Gäste zu orientieren. Bei der Recherche in einem Internetportal wurde eine Nutzerin darauf aufmerksam, dass dort zwei Beherbergungsbetriebe unter Verwendung des Nachnamens der Gäste

auf deren Bewertungen antworteten und dies, obwohl die Gäste selbst nur mit ihrem Vornamen oder einem Pseudonym erschienen. Auf den daraufhin erfolgten Hinweis konnte ich bei meiner Nachforschung auch tatsächlich mehrere direkte Gästeansprachen finden.

Der Nachname einer natürlichen Person gehört zu den vom Datenschutzrecht geschützten personenbezogenen Daten (Art. 4 Nr. 1 Datenschutz-Grundverordnung {DSGVO}). Dieser war auf den frei zugänglichen Bewertungsseiten für alle einsehbar. Für eine derartige Verarbeitung (Art. 4 Nr. 2 DSGVO) konnten mir die betreffenden Hotels keine Einwilligung nachweisen (Art. 6 Abs. 1 Buchst. a DSGVO). Eine Berechtigung ließ sich auch nicht aus dem Beherbergungsvertrag herleiten (Art. 6 Abs. 1 Buchst. b DSGVO). Schließlich fehlte es auch an einem legitimen Verarbeitungsinteresse. Damit schied gleichfalls die einzig noch denkbare Rechtfertigung des Art. 6 Abs. 1 Buchst. f DSGVO (Wahrung berechtigter Interessen) aus.

Nachdem ich die beiden Hotels mit meiner rechtlichen Wertung konfrontiert hatte, änderten diese sogleich alle von mir monierten Bewertungen, sodass sich darin die Nachnamen der Gäste nicht mehr fanden. Eines der beiden Hotels legte seiner Stellungnahme ergänzende Bildschirmausdrucke bei, die die Gästebewertungen aus Hotelsicht wiedergaben. Der Portalanbieter führt die im Buchungsprozess verwendete Buchungsnummer auf, über die eine eindeutige Zuordnung zu den Gästen möglich ist. Außerdem sind je Gast die Bewertungen nach den einzelnen Kategorien aufgeschlüsselt. Damit wurde klar, dass die Hotels mit den dortigen Angaben auf den bewertenden Gast schließen konnten und so zu dem vollständigen Gästenamen gelangten. Den Hotels war im Übrigen offensichtlich entgangen, dass der Betreiber des Bewertungsportals in seinen Richtlinien ausdrücklich klarstellt, dass die Erwähnung des Nachnamens des Gastes zu unterbleiben hat.

Die im Verhältnis zur Gesamtzahl der Kommentare der beiden Hotels geringe Anzahl der beanstandeten Bewertungen legte den Schluss nahe, dass die mir bekannten Fälle letztlich auf einzelne Beschäftigte zurückgingen. Denn in allen anderen

Was ist zu beachten?
Bei der Beantwortung von Gästebewertungen, ob auf Portalseiten oder dem eigenen Internetauftritt eines Hotels oder einer Pension, empfiehlt sich die Verwendung neutraler Formulierungen. Oder aber der Betreiber hält sich an die vom Gast verwendeten Angaben, also Vor- oder Nachname oder ein Pseudonym. Nur wenn der Gast selbst mit seinem Nachnamen auftritt, darf er auch mit diesem direkt angesprochen werden.

Fällen verwendeten die Hotels die von den Gästen gewählten Vornamen bzw. Pseudonyme oder griffen auf neutrale Formulierungen („Sehr geehrter Gast") zurück. Anhand des Umfangs der betroffenen Bewertungen kam ich in einem Fall jedoch nicht umhin, gegenüber dem verantwortlichen Hotelbetreiber eine Verwarnung nach Art. 58 Abs. 2 Buchst. b DSGVO auszusprechen. Im anderen Fall beließ ich es bei einem Hinweis (Art. 57 Abs. 1 Buchst. d DSGVO).
Ungeachtet dessen nahmen die Hotelverantwortlichen meine Hinweise als Anstoß für eine Schulung der zuständigen Beschäftigten. Weiter sicherten sie mir zu, künftig auf eine namentliche Anrede zu verzichten.

2.2.17 Dauerhafte Speicherung von Daten im Online-Club

↗ Art. 6 Abs. 1 Satz 1 Buchst. f DSGVO

Ein Beschwerdeführer teilte mir mit, dass seine E-Mail-Adresse weiterhin bei einem Sozialen Netzwerk, einem Online-Club, gespeichert wird, dessen Mitglied er war. Sein Zugang zum Club war von dem betreibenden Unternehmen gesperrt worden. Der Beschwerdeführer wollte mit seiner Beschwerde erreichen, dass der Club seine E-Mail-Adresse nicht weiter speichern dürfe, da er kein Mitglied mehr sei.
Zur Stellungnahme aufgefordert, teilte der Club-Betreiber mit, dass das Profil des Beschwerdeführers gelöscht worden sei, weil dieser gegen interne Regeln mehrfach und gravierend verstoßen habe. Deswegen sei gegen ihn ein virtuelles Hausverbot verhängt worden. Um dieses durchzusetzen, blieben die E-Mail-Adressen gesperrter (ehemaliger) Mitglieder nur in einer internen Blacklist gespeichert, um den weiteren Zugang zu verhindern; ein Einloggen sei für diese ehemaligen Mitglieder folglich nicht mehr möglich. Insofern war eine Abwägung zu treffen. Einerseits berief sich das ehemalige Mitglied als ausgeschlossener Nutzer auf seine widerrufene Einwilligung zur Speicherung seiner Daten und forderte auch die Löschung seiner E-Mail-Adresse. Der Anbieter wiederum berief sich zumindest auf das berechtigte

Interesse gemäß Art. 6 Abs. 1 Buchst. f Datenschutz-Grundverordnung (DSGVO), zur Durchsetzung des Hausverbots die E-Mail-Adresse des ehemaligen Mitglieds weiterhin in einer internen Blacklist speichern zu müssen.

Die genauen Gründe für die vom Anbieter vorgenommene Sperrung bzw. das virtuelle Hausverbot wurden weder vom Beschwerdeführer noch vom Verantwortlichen dargelegt. Gegebenenfalls wären diese Aspekte auch abwägungsrelevant gewesen. Aufgrund der vorliegenden Informationen war von einer kostenpflichtigen Mitgliedschaft auszugehen. Für diesen Fall ist ergänzend darauf hinzuweisen, dass einer physischen Löschung bestimmter Datenarten gesetzliche Aufbewahrungsfristen (insbesondere § 257 des Handelsgesetzbuches {HGB} und §§ 140ff. der Abgabenordnung {AO}) mit bis zu 10 Jahren entgegenstehen. Diese 10-Jahres-Frist umfasst vorliegend vor allem Buchungsbelege sowie Rechnungen. Die Aufbewahrungsfrist bei Handelsbriefen – also die geschäftliche Kommunikation – beträgt 6 Jahre (§ 257 Abs. 4 HGB).

Nach den vorliegenden Informationen konnte meine Behörde – auch in der Abwägung der verschiedenen Interessen und betroffenen Rechte – keinen Datenschutzverstoß erkennen.

Dafür ist ausschlaggebend, dass das Vorgehen des Anbieters, ein virtuelles Hausverbot bei (unterstellten) groben Verstößen gegen die vertraglichen Nutzungsbedingungen auszusprechen, grundsätzlich legitim ist (vgl. hierzu BGH V ZR 115/11, Urteil vom 09.03.2012 zum Hausverbot eines Hotelbetreibers, insbesondere Rdnr. 8, 13). In den Nutzungsbedingungen ist auch das Recht des Betreibers geregelt, insbesondere bei Verstößen gegen die Nutzungsbedingungen, den Zugang des Nutzers zeitweilig oder dauerhaft zu sperren.

Dieses virtuelle Hausverbot – durch Verweigern des Einloggens – lässt sich nachvollziehbar nur dann umsetzen, wenn bestimmte Informationen der oder des früheren Mitglieds zum Beispiel in einer Blacklist gespeichert bleiben. Anderenfalls wäre die Identität des Mitglieds für den Anbieter nicht mehr erkennbar und ein Nutzungsverbot nicht durchsetzbar.

Weiterhin sprach dafür, dass der Anbieter auf der Internet-

seite des Clubs in seiner Datenschutzerklärung unter „Registrierter Nutzer" ausführt: „Sensible Daten wie das genaue Geburtsdatum oder die E-Mail-Adresse sind generell nicht öffentlich einsehbar und werden ausschließlich für die interne Verwendung erhoben und gespeichert."
Es war auch davon auszugehen, dass die Information, welches Mitglied mit seiner E-Mail-Adresse (wegen Verstößen gegen die Hausordnung) gesperrt ist, nicht nach außen gelangt. Damit werden auch das Interesse und die Rechte des Mitglieds auf Anonymität gewahrt.
Nach den Datenschutzinformationen des Anbieters bleiben die Daten, die zur Durchsetzung des Hausverbots notwendig vorgehalten werden müssen, wie die E-Mail-Adresse, bis zu einer eventuellen Aufhebung der Sperre gespeichert, das heißt gegebenenfalls auch dauerhaft. Da ein dauerhaftes (virtuelles) Hausverbot bei groben und/oder mehrfachen Verstößen gegen die Nutzungsbedingungen ausgesprochen wird, ist auch insoweit die Verhältnismäßigkeit für eine unter Umständen dauerhafte Speicherung von Daten gegeben. Auch hat der Bundesgerichtshof (BGH) in seiner Rechtsprechung grundsätzlich keine zeitliche Begrenzung eines Hausverbots ausgesprochen, vgl. oben genanntes BGH-Urteil.

Was ist zu beachten?
Privat geführte Clubs können zur Sanktionierung von Regelverstößen gegenüber Mitgliedern (virtuelle) Hausverbote verhängen und zu deren Durchsetzung personenbezogene Daten der (ehemaligen) Mitglieder, die zur Identifizierung notwendig sind, gegebenenfalls auch dauerhaft speichern.

2.2.18 Datenerhebung in Sozialen Netzwerken durch Steuerbehörden

↗ § 3 SächsDSDG, Art. 6 Abs. 1 Satz 1 Buchst. e DSGVO, BMG

Eine Petentin wandte sich wegen eines Steuerstrafverfahrens an mich, in dem eine Steuerbehörde Daten aus ihrer Facebook-Seite erhoben hatte.
Der Sachverhalt stellte sich wie folgt dar. Die Petentin hatte den Namen ihres früheren Lebensgefährten an ihrem Briefkasten „für gemeinsame Anschaffungen" angebracht, obwohl dieser nicht (bzw. nicht mehr) bei ihr wohnte. Als die Beziehung endete, vergaß sie nach ihrer Darstellung, den Namen vom Briefkasten abzunehmen. Im Januar 2020 fand die Steuerbehörde den Namen somit noch vor. Aus den erhobenen Meldedaten ergab sich zudem, dass sie bis zum 1. Janu-

ar 2018 bei ihrem früheren Lebensgefährten gewohnt hatte (und entsprechend unter dortiger Anschrift gemeldet war).
Die Steuerbehörde hat daraufhin zur Überprüfung des Vorliegens der Voraussetzungen für eine Zweitwohnungssteuer Daten von der Facebook-Seite der Petentin erhoben und diese aufgefordert, Auskunft über ihren ehemaligen Lebensgefährten zu erteilen. Als die Auskunft ausblieb, wurde schließlich ein Zwangsgeld festgesetzt – woraufhin sich die Petentin an mich wandte.
Im Ergebnis konnte ich keinen Datenschutzverstoß feststellen. Die Datenerhebung war gemäß Art. 6 Abs. 1 Satz 1 Buchst. e Datenschutz-Grundverordnung (DSGVO) zulässig. Danach ist die Datenverarbeitung rechtmäßig, wenn diese für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Das richtet sich gemäß Art. 6 Abs. 3 Satz 1 Buchst. b DSGVO nach dem Recht der Mitgliedstaaten, dem der Verantwortliche unterliegt.
Rechtsgrundlage für die Verarbeitung der Daten war vorliegend § 3 Sächsisches Datenschutzdurchführungsgesetz (SächsDSDG). Gemäß § 3 Abs. 1 SächsDSDG ist die Verarbeitung personenbezogener Daten durch öffentliche Stellen zulässig, wenn sie zur Erfüllung der in der Zuständigkeit des Verantwortlichen liegenden Aufgabe oder in Ausübung öffentlicher Gewalt, die dem Verantwortlichen übertragen wurde, erforderlich ist.
Steuerpflichtig war gemäß der einschlägigen Zweitwohnsteuersatzung die bzw. der Inhaber/in der Wohnung, deren bzw. dessen melderechtlichen Verhältnisse die Beurteilung der Wohnung als Zweitwohnung bewirken. Als Inhaber/in einer Zweitwohnung gilt die Person, der die Verfügungsbefugnis über die Wohnung als Eigentümer/in oder Mieter/in oder als sonstige dauernutzungsberechtigte Person (auch unentgeltlich) zusteht.
Die melderechtlichen Verhältnisse ergaben sich nicht korrekt bzw. nicht eindeutig aus dem Melderegister, sodass weitere Nachforschungen notwendig waren. Zur Ermittlung der mel-

derechtlichen Verhältnisse, also wer in eine Wohnung gemäß § 17 Abs. 1 Bundesmeldegesetz (BMG) eingezogen war, war die Hinzuziehung der Daten aus der öffentlich zugänglichen Facebook-Seite der Petentin durch die Steuerbehörde notwendig.

2.2.19 Tesla: Dashcam und Wächtermodus

↗ Art. 4, 6, 13 DSGVO

Zunehmend gehen auch bei mir Anfragen und Beschwerden zu Tesla-Fahrzeugen mit ihren zahlreichen Kameras ein. In besonderem Maße betrifft das den sogenannten Wächtermodus (Videoüberwachung der Umgebung des geparkten Fahrzeugs), dessen Aktivierung für betroffene Personen durch einen Blick ins Fahrzeuginnere regelmäßig erkennbar (aufgeklapptes Display mit entsprechender Anzeige) ist.
Soweit im Rahmen der Beschwerden oder Anfragen eventuelle Datenflüsse vom Fahrzeug zum Hersteller thematisiert werden, ist grundsätzlich festzustellen, dass die datenschutzrechtliche Kontrollzuständigkeit dafür bei der niederländischen Datenschutzaufsichtsbehörde liegt, denn Tesla hat seine europäische Hauptniederlassung in Amsterdam. Innerdeutsch werden diesbezügliche Vorgänge durch die Berliner Beauftragte für Datenschutz und Informationsfreiheit als die für den deutschen Tesla-Hauptsitz zuständige Aufsichtsbehörde koordiniert.
Anders sieht es hingegen bei der Nutzung der Dashcam-Funktionalität bzw. bei der Kameraüberwachung im Rahmen des Wächtermodus aus. In beiden Fällen werden nur dann Videoaufzeichnungen erstellt, wenn der/die Fahrzeugnutzer/in ein entsprechend formatiertes Speichermedium (USB-Stick) ins Fahrzeug eingesteckt hat. Derjenige bzw. diejenige Fahrzeugnutzer/in, der/die anschließend die Dashcam oder den Wächtermodus dauerhaft oder im Einzelfall aktiviert hat, ist dann in der Regel Verantwortliche/r im Sinne des Art. 4 Nr. 7 Datenschutz-Grundverordnung (DSGVO). Denn in diesem Fall entscheidet diese/r Fahrzeugnutzer/in über die damit verbundenen Videoaufzeichnungen. Daraus ergibt sich

wiederum die Kontrollzuständigkeit der für den jeweiligen Wohn- oder Geschäftssitz zuständigen Datenschutzaufsichtsbehörde – für in Sachsen ansässige Fahrzeugnutzer/innen also meine Behörde. Im Fall einer Ordnungswidrigkeitenanzeige kann die Verfolgung aber auch durch die Verwaltungsbehörde am Begehungs- oder Entdeckungsort erfolgen.
Zur Frage der Zulässigkeit des Einsatzes von – regelmäßig zu Beweissicherungszwecken betriebenen – Dashcams habe ich in meinen Tätigkeitsberichten schon mehrfach Ausführungen gemacht. Maßgebliche Rechtsgrundlage ist an dieser Stelle Art. 6 Abs. 1 Buchst. f DSGVO, wonach die Verarbeitung, mithin der Betrieb einer Dashcam, vor allem die Speicherung von Videoaufnahmen, nur dann zulässig ist, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.
Diese Voraussetzungen sind bei der permanenten und damit anlassfreien Fertigung von Videoaufzeichnungen im öffentlichen Straßenverkehr allenfalls dann gegeben, wenn insgesamt immer nur wenige Minuten Videomaterial gespeichert werden. Die Aufnahmen müssen also stets unmittelbar überschrieben werden; eine dauerhafte Speicherung darf nur erfolgen, wenn hierfür ein konkreter Aufzeichnungsanlass besteht (z. B. Auslösen eines Crash-Sensors). Für die Dokumentation eines Unfallhergangs oder eines sonstigen Vorgangs ist es regelmäßig ausreichend, einen Zeitraum von circa 30 Sekunden bis eine Minute vor und circa 30 Sekunden bis eine Minute nach dem Unfallereignis zu speichern. Für darüber hinausgehende Videoaufzeichnungen fehlt es schon an der Erforderlichkeit der Verarbeitung personenbezogener Daten zur Zweckerreichung. Speicherzyklen in Dashcams sollten daher einen Zeitraum von etwa drei Minuten nicht überschreiten. Diesbezüglich hat der Bundesgerichtshof (BGH) in seinem Urteil vom 15.05.2018 (VI ZR 233/17, juris) einerseits entschieden, dass Dashcam-Aufnahmen unter ge-

wissen Voraussetzungen als Beweismittel bei Unfall-Prozessen verwertbar sind, andererseits aber auch klar festgestellt, dass jedenfalls eine permanente anlasslose Aufzeichnung des gesamten Geschehens auf und entlang der Fahrstrecke zur Wahrnehmung von Beweissicherungsinteressen nicht erforderlich ist, denn es sei technisch möglich, eine kurze, anlassbezogene Aufzeichnung des unmittelbaren Unfallgeschehens, beispielsweise durch ein dauerndes Überschreiben der Aufzeichnungen in kurzen Abständen und Auslösen der dauerhaften Speicherung erst bei Kollision oder starker Verzögerung des Fahrzeuges (vgl. BGH, Pressemitteilung 88/2018).

Unbeschadet der schon festgestellten fehlenden Erforderlichkeit von wenige Minuten überschreitenden Videoaufzeichnungen, überwiegen auch die schutzwürdigen Interessen der unbeteiligten, sich verkehrsgerecht verhaltenden Passanten/innen und Fahrzeugführer/innen, nicht anlasslos und heimlich auf öffentlichem Grund überwacht zu werden, das Aufzeichnungsinteresse des Fahrzeugführers bzw. der Fahrzeugführerin jedenfalls dann, wenn der beschriebene Zeitrahmen überschritten wird. Mit der heimlichen Videoüberwachung wird in schwerwiegender Weise in das Recht auf informationelle Selbstbestimmung der anderen Verkehrsteilnehmer eingegriffen. Die anderen Verkehrsteilnehmer/innen sind auf die Nutzung von Gehweg und Straße angewiesen und werden – ohne hierfür einen Anlass oder Grund gegeben zu haben – vom bzw. von der Fahrzeugführer/in unter Generalverdacht gestellt und mittels Videokamera überwacht.

In den Tesla-Fahrzeugen wird – bei eingelegtem Speichermedium – permanent die gesamte Fahrt in der „Dashcam"-Funktion aufgezeichnet und erst wieder nach einer Stunde überschrieben. Bei einem besonderen auslösenden Ereignis oder nach manueller Intervention des Fahrers bzw. der Fahrerin werden die letzten 10 Minuten dauerhaft gespeichert. Diese Zeiträume können nicht als kurzzeitig bezeichnet werden.

Für den Wächtermodus gelten grundsätzlich die gleichen rechtlichen Erwägungen. Im Wächtermodus wird nach meiner

Kenntnis – bei eingelegtem Speichermedium – gleichfalls permanent ein Ringspeicher von 60 Minuten beschrieben; eine dauerhafte Speicherung von Bildaufnahmen erfolgt bereits dann, wenn jemand lediglich zu nahe an einem Tesla-Fahrzeug vorbeigeht. Die Länge dieser dauerhaft gespeicherten Videosequenzen beträgt auch hier 10 Minuten. Das 360-Grad-Aufnahmefeld reicht je nach betrachteter Tesla-Kamera 50 bis 250 Meter. Tatsächlich sind die diesbezüglichen Fahrzeugkameras dann nicht anders zu betrachten als stationäre Kameras mit entsprechender Bewegungserkennung. Solche Kameras sind im öffentlichen Verkehrsraum aber regelmäßig unzulässig. Es sollte unstrittig sein, dass es – allein schon bei der vorsorglichen Ringspeicherung, aber auch bei der bloßen Wahrnehmung einer Bewegung in dem das Fahrzeug umgebenden öffentlichen Verkehrsraum – zunächst einmal schon an einem konkreten Anlass und damit einem berechtigten Aufzeichnungsinteresse fehlt, darüber hinaus geht die im Übrigen durchzuführende Interessenabwägung klar zugunsten der betroffenen Personen (gefilmte Passanten/innen und Fahrzeugführer/innen) aus. Etwas Anderes kann nur gelten, wenn das Fahrzeug auf dem eigenen Grundstück oder in nicht für Dritte zugänglichen Bereichen abgestellt wird.

Vor diesem Hintergrund kann Tesla-Fahrern/innen nur geraten werden, die vorstehend benannten Kamerafunktionen grundsätzlich nicht zu aktivieren bzw. deaktiviert zu lassen. Dies kann durch ein Nichtnutzen bzw. ein Entfernen des USB-Sticks, der für die Aktivierung sowohl der Dashcam als auch des Wächtermodus benötigt wird, erfolgen.

Nicht unerwähnt bleiben soll, dass natürlich auch bei Fahrzeugkameras die Informationspflichten des Art. 13 DSGVO zu erfüllen sind. Der bzw. die jeweilige Fahrzeugnutzer/in muss die betroffenen Personen auf die kameragestützte Verarbeitung ihrer personenbezogenen Daten transparent hinweisen. Während dies beim stehenden Fahrzeug noch realisierbar zu sein scheint und bedingen würde, dass der/die Fahrzeugnutzer/in unter anderem seine/ihre Kontaktdaten deutlich sichtbar im Fahrzeug hinterlassen müsste, weist dies bei fahrenden Fahrzeugen in praktischer Hinsicht natürlich eine Rei-

Was ist zu tun?

Um nicht der Gefahr eines Ordnungswidrigkeitenverfahrens ausgesetzt zu werden, sollten Tesla-Fahrer/innen aktuell auf die Nutzung der fahrzeuginternen Dashcam und des Wächtermodus verzichten.

he von Schwierigkeiten auf. Gleichwohl stellt sich bei Tesla-Fahrzeugen zunächst einmal die Frage, wie überhaupt ein rechtskonformer Kamerabetrieb erreicht werden kann.

2.2.20 Die Videokamera in der Gartenparzelle – Was kann der Kleingartenverein dagegen unternehmen?

↗ Nr. 7.4 und 7.6 Rahmenkleingartenordnung des Landesverbandes Sachsen der Kleingärtner e. V.

Der Vorsitzende eines Kleingartens wandte sich an mich, da er vonseiten mehrerer Mitglieder aufgefordert wurde, gegen eine Videoüberwachung in der Kleingartensparte vorzugehen.

Was war geschehen? Die Mitglieder eines Kleingartenvereins entdeckten eines Tages mehrere Kameras in einem Kleingarten. Sie wähnten sich dadurch auf dem Weg zu ihrer Gartenparzelle überwacht. Die erspähten Videokameras befanden sich am Gartenhaus und waren sowohl auf den Anlagenhauptweg als auch auf Nachbarparzellen gerichtet. Verständlicherweise wollten das die anderen Kleingartennutzerinnen und -nutzer nicht hinnehmen und bedrängten daher den Vereinsvorsitzenden, gegen die Garteninhaberin vorzugehen. In einem hilflosen Versuch wandte sich der Vorsitzende mit einer E-Mail an die Kamerabetreiberin und lud diese darin vor einer geplanten Gartenbegehung zu einem Gespräch ein. Nach seinem Bekunden habe er ihr auch (mündliche) Sanktionen angedroht. Dem für die Kleingartenanlage zuständigen Regionalverband wurde der Vorgang gleichfalls zur Kenntnis gegeben. Dieser wandte sich ebenso an das Vereinsmitglied mit der Bitte, die Mängel abzustellen. Allerdings konnte die Parzelleninhaberin offensichtlich von keiner Stelle zu einem Einlenken bewogen werden. So sah der Vorsitzende für sich letztlich keine andere Möglichkeit, als sich hilfesuchend an meine Behörde zu wenden.

Nach den mir vom Vorsitzenden vorgelegten Bildern der Videokameras am Gartenhaus wirkten diese in der Tat bedrohlich und ließen eine über die Gartenumzäunung hinaus-

gehende Überwachung befürchten. Jedoch sah ich in diesem Fall in Ausübung meines Ermessenspielraums von einem eigenen Tätigwerden ab.

Stattdessen wies ich den Verein darauf hin, dass er von den in der Rahmenkleingartenordnung des Landesverbandes Sachsen der Kleingärtner e.V. zur Verfügung stehenden Möglichkeiten Gebrauch machen soll. Die Rahmenkleingartenordnung enthält detaillierte Bestimmungen in Form von Ge- und Verboten zur Nutzung der einzelnen Kleingärten sowie der Gemeinschaftsflächen. Sie gilt für alle im Landesverband organisierten Verbände (Kreis-, Territorial-, Regional- und Stadtverbände) und deren Kleingartenvereine. Außerdem wird sie automatisch Bestandteil jedes (Unter-) Pachtvertrags, den das einzelne Vereinsmitglied mit dem Kleingartenverein (Hauptpächter) abschließt.

Der Betrieb „elektronischer Überwachungseinrichtungen" und somit auch von Videokameras ist nach der Rahmenkleingartenordnung nur dann erlaubt, wenn sich der Aufnahmebereich innerhalb der Parzellengrenze bewegt (Nr. 7.4 der Rahmenkleingartenordnung). Eine darüber hinausgehende Überwachung stellt eine vertragliche Leistungsstörung dar. Die anderen (Unter-)Pächterinnen und Pächter werden hierdurch in ihrem Persönlichkeitsrecht beeinträchtigt. Zudem wirken sich Videokameras negativ auf das nachbarliche Verhältnis innerhalb der Kleingartenanlage aus.

Es lag also in der Sphäre des zuständigen Verbandes und Kleingartenvereins, von der verantwortlichen Kamerabetreiberin Auskunft über den Umfang der Videoüberwachung zu verlangen. Bei einem festgestellten Verstoß kann gegen die Garteninhaberin zunächst eine Abmahnung und bei fortgesetzten Verstößen auch eine Kündigung des Pachtvertrags ausgesprochen werden (Nr. 7.6 Rahmenkleingartenordnung). Hierauf wies ich den Vereinsvorsitzenden hin und bat ihn, mit diesen Mitteln auf die Kamerabetreiberin einzuwirken. Denn angesichts der massiven Beschwerden aus dem Kreis der Gartennutzer lag dem Kleingartenverein sehr daran, eine schnelle Lösung zu finden. Gerade vor dem Hintergrund der sich offenkundigen Weigerungshaltung der Kamerabetrei-

berin wäre mit einer langen Verfahrensdauer bei einem behördlichen Aufsichtsverfahren zu rechnen gewesen.
Nicht nur bei diesem Hinweis wurde ich, wie so oft in der täglichen Praxis beim Umgang mit Hinweisen und Beschwerden, mit einer zum Teil unrealistischen Erwartungshaltung konfrontiert. Zudem scheint es manchen Akteuren leichter zu fallen, auf mich zu verweisen, statt selbst tätig zu werden. Die datenschutzrechtlichen Vorschriften erlauben es mir grundsätzlich, die Außerbetriebnahme einer rechtswidrig betriebenen Kamera zu bewirken und diese auch mit den Mitteln des Verwaltungszwangs durchzusetzen. Schneller und effektiver lässt sich dieses Ergebnis jedoch im Wege des Zivilrechts mit der Rahmenkleingartenverordnung erreichen. Je nach konkreter Ausgestaltung des Einzelfalls können auch die Zivilgerichte die Demontage einer Videokamera anordnen oder sprechen den Betroffenen gar Schadensersatzansprüche zu.

Was ist zu tun?
Videokameras in Kleingärten sind nur zulässig, wenn die Kamerabetreiberin bzw. der Kamerabetreiber damit ihre/seine eigene Gartenparzelle überwacht. Geht der Erfassungsbereich über die Parzellengrenze hinaus, können Kleingartenvereine und -verbände eine Abmahnung aussprechen. Bei fortgesetzten Regelverstößen kommt auch eine Kündigung des Pachtvertrags in Betracht.

2.2.21 Videoüberwachung in Spielhallen

↗ § 7 DGUV Vorschrift 25, DGUV Regel 115-004, § 15 SGB VII, Art. 5 Abs. 1 Buchst. c und e DSGVO, Art. 6 Abs. 1 Buchst. c, Art. 6 Abs. 2 DSGVO

In der letzten Zeit mehren sich Hinweise und Beschwerden im Zusammenhang mit einer Videoüberwachung von Spielhallen. In einem Fall sah ein ehemaliger Spielhallenmitarbeiter seine Persönlichkeitsrechte dadurch verletzt, dass der Betreiber mutmaßlich länger zurückreichende Videoaufzeichnungen gegen ihn verwendete. In dem Arbeitsvertrag, den er mir vorlegte, fand sich ein ausdrücklicher Hinweis auf den dortigen Betrieb einer Videoüberwachungsanlage. Darin wurde ihm auch strengstens untersagt, während der Arbeitszeiten an den Automaten zu spielen.
Nach seiner Darstellung habe ihm die Teamleiterin eine WhatsApp-Nachricht gesendet und darin auf mehrere Tage zurückliegende Videoaufzeichnungen verwiesen, die sie gesichtet habe. Er wandte sich als Erstes schriftlich an den Arbeitgeber und trug dort seine datenschutzrechtlichen Bedenken vor. In den für Zwecke der Mitarbeiterüberwachung

genutzten Aufzeichnungen sah er eine zweckwidrige Verwendung. Er bemängelte weiter das Fehlen seiner Einwilligung in die Videoüberwachung am Arbeitsplatz. Nachdem er offensichtlich keine zufriedenstellende Antwort erhielt und er nach wie vor davon ausging, dass es länger als 72 Stunden zurückliegende Aufzeichnungen geben muss, wandte er sich schließlich mit einer Datenschutzbeschwerde an mich.

Eine Videoüberwachung in Spielhallen ist nicht per se datenschutzrechtswidrig. Vielmehr sind Betreibende von Spielhallen durch Vorgaben der Unfallversicherungsträger sogar verpflichtet, einzelne Spielhallenbereiche zu überwachen und das Videomaterial zu speichern. Entsprechende Vorgaben wegen des Überfallschutzes beim Umgang mit Bargeld, Wertsachen und sonstigen Zahlungsmitteln finden sich in der DGUV-Vorschrift 25 („Unfallverhütungsvorschrift Überfallprävention" vom 1. April 2021) der Deutschen Gesetzlichen Unfallversicherung. Dieses Regelwerk richtet sich sowohl an Kredit- und Finanzdienstleistungsunternehmen als auch an Spielstätten (§ 1 Abs. 1 DGUV Vorschrift 25).

Spielhallenbetreibende haben die Pflicht, bei der Annahme und Ausgabe von Bargeld in öffentlich zugänglichen Bereichen sichtbare Kameras anzubringen (§ 7 Abs. 1 DGUV Vorschrift 25). Damit soll erreicht werden, dass Überfälle nachhaltig zurückgehen. Verstärkt werden soll dies durch zusätzlich angebrachte Hinweisschilder im Eingangsbereich. Anders als DGUV-Regeln und -Informationen haben DGUV-Vorschriften verbindlichen Charakter. Demzufolge besteht eine gesetzliche Notwendigkeit zur Videoüberwachung, sodass diese vom Rechtsgrund der „Erforderlichkeit zur Erfüllung einer Rechtspflicht" gedeckt ist (Art. 6 Abs. 1 Buchst. c und Abs. 2 Datenschutz-Grundverordnung {DSGVO} in Verbindung mit § 15 Siebtes Sozialgesetzbuch {SGB VII} in Verbindung mit § 7 DGUV-Vorschrift 25). Auf eine (zusätzliche) Einwilligung der betroffenen Mitarbeiterinnen und Mitarbeiter oder Gäste kommt es damit im Ergebnis nicht an.

Die Unfallverhütungsvorschriften bedeuten jedoch keinen Freibrief für Spielhallenbetreibende. Vielmehr stellen die Unfallversicherungsträger unter Nummer 2.5 der DGUV-Regel

115-004 unmissverständlich klar, dass die Videoüberwachung auf das notwendige Minimum zu beschränken ist und nur der Aktionsraum einer Täterin bzw. eines Täters überwacht werden darf. Im Besonderen zählen hierzu die Ein- und Ausgänge sowie die Bereiche mit Geldübergabe (Grundsatz der Datenminimierung, Art. 5 Abs. 1 Buchst. c DSGVO). Nicht benötigte Aufnahmen sind außerdem unverzüglich zu löschen (§ 7 Abs. 2 DGUV-Regel 25, Grundsatz der Speicherbegrenzung, Art. 5 Abs. 1 Buchst. e DSGVO). Außerdem treffen die Betreiberin bzw. den Betreiber sämtliche weiteren datenschutzrechtlichen Verantwortlichenpflichten (namentlich die Hinweispflicht nach Art. 13 DSGVO).

Doch zurück zur konkreten Datenschutzbeschwerde. Nachdem sich der Chatverlauf durchaus im Sinne des nunmehr arbeitslosen Mitarbeiters interpretieren ließ, wandte ich mich mit einem schriftlichen Auskunftsersuchen an den Spielhallenbetreiber. Erwartungsgemäß stritt dieser die zweckwidrige Verwendung zur Überwachung der Mitarbeiterinnen und Mitarbeiter und letzten Endes auch den vermuteten Zugriff auf die Videoaufzeichnungen für diese Zwecke ab. Außerdem wies er mir glaubhaft nach, dass er die Aufzeichnungen nach 72 Stunden löscht. Schließlich konnte ich keinen Anhaltspunkt für eine unzulässige Videoüberwachung der Spielhallenräumlichkeiten, insbesondere des (ehemaligen) Mitarbeiters, finden.

Jedoch gab sich der Petent mit meiner abschlägigen Mitteilung nicht zufrieden, sondern reichte eine Klage vor dem Verwaltungsgericht ein mit dem Ziel, seiner „Beschwerde stattzugeben". Als er vom Gericht zur Zahlung eines Vorschusses auf die Gerichtskosten aufgefordert wurde, wurde ihm erstmals bewusst, dass ein Gerichtsverfahren – im Gegensatz zu einer Beschwerdeeinreichung bei meiner Behörde – nicht kostenfrei ist. Er nahm daraufhin die Klage umgehend zurück. Im Übrigen wäre dieser inhaltlich auch wenig Erfolg beschieden gewesen, da ich als Aufsichtsbehörde sowohl hinsichtlich des „Ob" eines Tätigwerdens als auch der zu wählenden Maßnahmen einen Ermessensspielraum habe (siehe Urteil des Verwaltungsgerichts Ansbach

vom 7. Dezember 2020, Az. AN 14 K 18.02503). Da mir eine schriftliche Stellungnahme des verantwortlichen Spielhalleninhabers vorlag, die in Widerspruch zu den Darstellungen des vormaligen Mitarbeiters stand, sah ich keine Möglichkeit zur weiteren Sachaufklärung, zumal die in Rede stehenden Aufzeichnungen zwischenzeitlich längst gelöscht waren.
Offensichtlich wurde dem Beschwerdeführer im Verlauf der konfrontativen Auseinandersetzung mit dem Arbeitgeber bewusst, dass eine arbeitgeberseitige Kündigung wegen mutmaßlicher Pflichtenverstöße unmittelbar bevorstand. Denn schließlich hatte er diesem gegenüber sogar schriftlich eingestanden, dass er der Versuchung nicht widerstehen konnte, selbst an den Automaten zu spielen. Was den Beschwerdeführer jedoch tatsächlich dazu veranlasst hatte, den befristeten Arbeitsvertrag kurz vor Beschwerdeeinreichung zu kündigen, bleibt letztlich sein Geheimnis.

Was ist zu beachten?
In Spielhallen und -stätten ist der Einsatz von Videokameras in einzelnen Bereichen von dem Unfallversicherungsträger vorgegeben. Aus Gründen des Überfallschutzes dürfen die Ein- und Ausgänge sowie die Bereiche mit Geldübergabe überwacht werden. Ansonsten gelten die allgemeinen datenschutzrechtlichen Vorschriften. Am Eingang sind die Besucher auf die Videoüberwachung hinzuweisen (Art. 13 DSGVO).

2.2.22 Videoüberwachung auf Privatwegen

↗ § 1018 BGB, Art. 6 Abs. 1 DSGVO

Über eine Kommune erreichte mich eine anonyme Beschwerde wegen einer Videoüberwachung in unmittelbarer Nähe zu einer Ortsdurchgangsstraße. Auf einem angrenzenden Wohngrundstück hatte der Grundstückseigentümer am dortigen Wohnhaus in Ausrichtung der Ortsdurchfahrt eine Domekamera angebracht. Von dort zweigte im rechten Winkel ein Privatweg ab. Dieser führte am Wohngrundstück des Kamerabetreibers vorbei bis zum dahinterliegenden Grundstück des Nachbarn. Beide Nachbarn hatten erst wenige Monate zuvor die Erschließungsstraße von der Gemeinde erworben.
Der Kamerabetreiber gab mir in knapper Form zu verstehen, dass er von einem legalen Kamerabetrieb ausgeht und legte mir zur Rechtfertigung zwei Bildschirmausdrucke vor. Die Kamera war tagsüber auf die Hofeinfahrt sowie den Privatweg gedreht. Außerdem waren auch die Randbereiche des gegenüber gelegenen Mietwohngrundstücks des Verantwortlichen zu sehen und marginal der öffentliche Verkehrsbereich am Beginn der Privatstraße. Nachts drehte die

Kamera parallel zum Wohnhaus mit Ausrichtung auf den Hauseingangsbereich des Wohnhauses.

Nachdem meine wiederholten Versuche zur weiteren Sachverhaltsklärung, auch unter zwischenzeitlicher Beteiligung eines Rechtsanwalts, keinen Erfolg hatten, verpflichtete ich den Verantwortlichen schließlich zum Schutz der von der Videoüberwachung betroffenen Personen mittels eines förmlichen Bescheids unter Androhung eines Zwangsgeldes zur Herstellung rechtmäßiger Zustände. Meine Anordnung habe ich in Anbetracht der Massivität des Grundrechtseingriffs mit einer Anordnung der sofortigen Vollziehung versehen, um zu verhindern, dass der Verantwortliche im Fall einer Klageerhebung die Kamera auf unbestimmte Zeit weiterbetreiben kann.

Gegen diese förmliche Anordnung setzte sich der Verantwortliche mit einem Antrag auf Aussetzung der Vollziehung sowie einer Klage beim zuständigen Verwaltungsgericht zur Wehr. Nach seinem Bekunden habe er zwei Tage vor Erlass meiner Anordnung die Kameraausrichtung so verändert, dass sie nur noch auf seine Grundstückseinfahrt zeigt. Das Gericht hatte sich in der Sache darüber hinaus mit mehreren strittigen Wertungen und Rechtsfragen im Hinblick auf die zur Rechtsverteidigung angeführten Argumente des Kamerabetreibers zu befassen.

Zunächst galt es zu klären, welche Bedeutung der geänderten Kameraausrichtung zukam. Denn davon hatte ich zum Erlasszeitpunkt keine Kenntnis, sodass ich meine Entscheidung nur auf die mir bis dahin bekannten tatsächlichen Verhältnisse stützen konnte. Das Verwaltungsgericht stimmte mit mir darin überein, dass ich einzig und somit rechtsfehlerfrei meiner Entscheidung nur die mir bekannten Sachverhalte zugrunde legen konnte. Die Verantwortung für die neue Sachlage sah es einzig in der Sphäre des verantwortlichen Kamerabetreibers. Dieser hätte mich vor Anordnungserlass über die geänderte Kameraausrichtung informieren müssen.

Weiter ging es um die Frage, ob die Datenschutzvorschriften überhaupt Anwendung finden oder die Videoüberwachung auch jenseits der Grenze des Wohngrundstücks von

der „Haushaltsausnahme" (Haushaltsprivileg) gedeckt war (Art. 2 Abs. 2 Buchst. c Datenschutz-Grundverordnung – DSGVO). Der Verordnungsgeber nimmt darin private und familiäre Tätigkeiten vom Anwendungsbereich der Datenschutzvorschriften aus. Nach der Wertung des Gerichts ist diese Vorschrift jedoch eng auszulegen. Sie nimmt lediglich den persönlichen Bereich, wie Vorgänge des Privat- und Familienlebens von Einzelpersonen, von der Geltung des Datenschutzrechts aus. Mit der Videoüberwachung des öffentlichen Straßenverkehrs oder des privaten Raums Dritter verlässt eine Kamerabetreiberin bzw. ein Kamerabetreiber jedoch diesen Rahmen. Da der überwachte Bereich auch die öffentliche und private Straße sowie das angrenzende Grundstück betraf, war folglich die Grenze der Ausnahmevorschrift überschritten.

Der Verantwortliche versuchte auch, die Zulässigkeit der Videoüberwachung durch Vorlage einer Einwilligung des Miteigentümers der Privatstraße zu begründen. Für einen Rückgriff auf den Einwilligungstatbestand (Art. 6 Abs. 1 Unterabs. 1 Buchst. a DSGVO) bedarf es der Einwilligung aller betroffenen Personen. Allein aus dem unbestimmten Personenkreis der Nutzer der Privatstraße war diese Vorgabe aus praktischen Gründen schlicht nicht umsetzbar. Die Einwilligung des Nachbars konnte nur dessen mögliche Erfassung legitimieren. Bereits die Beobachtung der Familienangehörigen des Nachbarn sowie Dritter war jedoch schon nicht mehr von der Einwilligung gedeckt.

Bei einer Überwachung außerhalb der eigenen Grundstücksgrenze befindlicher Bereiche reduziert sich die Zulässigkeitsprüfung auf die Vorschrift Art. 6 Abs. 1 Unterabs. 1 Buchst. f DSGVO (Wahrung berechtigter Interessen). Bei einer im Privateigentum stehenden Straße konnte sich der Verantwortliche auf den Eigentumsschutz (Art. 14 Grundgesetz) berufen. Jedoch hätte es einer konkreten Gefährdungslage für das zu schützende Rechtsgut (Eigentum) bedurft, welches eine unterschiedslose Erfassung aller Straßenbenutzerinnen und -benutzer notwendig macht. Die in allgemeiner Form gehaltenen (subjektiven) Befürchtungen des Kamerabetreibers reich-

ten hierfür nicht aus. Weiter ging das Verwaltungsgericht davon aus, dass mit Schädigungsabsicht handelnde Personen im Regelfall im Schutz der Dunkelheit und zudem maskiert vorgehen. In jedem Fall wäre es bei der Interessenabwägung, insbesondere anhand der Schwere und des Gewichts eines mit der Videoüberwachung verbundenen Grundrechtseingriffs, zu einem Überwiegen des Betroffeneninteresses gegenüber dem Überwachungsinteresse gekommen.

Die vom Kamerabetreiber am Beginn der Privatstraße angebrachten Pflastersteine zum Zweck der optischen Abgrenzung konnten das Verwaltungsgericht auch nicht überzeugen, ebenso wenig wie das teils private Miteigentum an der Privatstraße. Vielmehr war für den Richter maßgeblich, dass die Privatstraße ungehindert und ohne Überwindung einer physischen Grenze betreten werden kann. Ferner sind optische Hinweise auf die Videoüberwachung und ein Betretungsverbot nicht geeignet, das Aufsuchen der Anliegergrundstücke von Personen ohne familiäre oder verwandtschaftliche Berührungspunkte (wie Post oder Lieferanteninnen und Lieferanten) zu verhindern. Überdies kann eine Beschilderung auch Kinder oder andere des Lesens Unkundige nicht vom Betreten des überwachten Bereichs abhalten. In der Konsequenz konnten auch die diesbezüglichen Bemühungen des Kamerabetreibers keinen legalen Kamerabetrieb begründen. Damit lassen sich aus der Gerichtsentscheidung folgende Erkenntnisse ziehen:

- Die „Haushaltsausnahme" des Art. 2 Abs. 2 Buchst. c DSGVO ist eng auszulegen. Davon erfasst werden nur solche Vorgänge des Privat- und Familienlebens von Einzelpersonen, die objektiv betrachtet ausschließlich persönlicher oder familiärer Art sind. Wird auch öffentlicher Straßenraum (auch eine Privatstraße) oder der private Raum Dritter überwacht, wird der persönliche Bereich der „Haushaltsausnahme" verlassen.

- Für die Einhaltung und Durchsetzung der Datenschutzvorschriften bei Videoüberwachungen kommt es nicht primär darauf an, in wessen Eigentum der überwachte Bereich steht. Entscheidend ist, ob der überwachte Bereich räumlich ausschließlich dem Bereich der privaten Lebensführung (siehe Art. 2 Abs. 2 Buchst. c DSGVO) zuzuordnen ist. Dies ist dann nicht der Fall, wenn dieser ohne Überwindung erkennbarer physischer Barrieren aufgesucht werden kann. Hinweisschilder können ein Betreten von Personen ohne familiäre oder verwandtschaftliche Berührungspunkte, insbesondere von Kindern, nicht verhindern.
- Eine Videoüberwachung lässt sich nur dann auf die Einwilligungslösung (Art. 6 Abs. 1 Unterabs. 1 Buchst. a DSGVO) stützen, wenn von allen betroffenen Personen eine wirksame Einwilligung vorliegt.

In der Konsequenz veranlasste die aus Sicht der Datenschutzaufsichtsbehörden positive Gerichtsentscheidung den Antragsteller schließlich doch dazu, seinen gerichtlichen Antrag ebenso wie die dort erhobene Klage zurückzunehmen, sodass die behördliche Anordnung letzten Endes Bestandskraft erlangte.

Die richterliche Wertung lässt sich auch auf eine Videoüberwachung von über private Grundstücksbereiche führenden Zuwegungen übertragen. Denkbar ist ein derartiger Fall bei Hinterlieger- oder Hammergrundstücken. Damit wird das hintere von zwei hintereinanderliegenden Grundstücken bezeichnet, welches im ungünstigsten Fall ausschließlich über das vordere Grundstück erreichbar ist. Sicherstellen lässt sich dies mit Eintragung eines Wegerechts im Grundbuch in Form eines Geh- und Fahrtrechts (beispielsweise als Grunddienstbarkeit, § 1018 Bürgerliches Gesetzbuch – BGB). Möchte nun die Eigentümerin bzw. der Eigentümer des vorderen Grundstücks ihre/seine privaten Grundstücksbereiche überwachen, so hat sie bzw. er den vom Geh- und Wegerecht umfassten Zuwegungsbereich von der Videoüberwachung auszunehmen.

Was ist zu tun?

Kamerabetreiberinnen und -betreiber können eine Videoüberwachung außerhalb der eigenen Grundstücksgrenze nicht mit der „Haushaltsausnahme" rechtfertigen, auch wenn es sich dabei um einen Privatweg handelt. Privatwege dienen dem öffentlichen Straßenverkehr, wenn es keine erkennbaren physischen Barrieren (Zaun) gibt, die zu überwinden wären.

2.2.23 Identifikationspflicht beim Immobilienkauf

↗ § 11 GwG, Art. 6 Abs. 2 in Verbindung mit Abs. 1 Buchst. c DSGVO

Ein Kaufinteressent wurde in einem Immobilienportal auf eine interessante Immobilie aufmerksam. Sodann richtete er eine schriftliche Anfrage an den Immobilienmakler, der das Objekt inserierte. Schnell war ein Besichtigungstermin vereinbart, allerdings forderte das Maklerunternehmen zuvor eine beiderseitige Kopie des Personalausweises von dem potenziellen Kaufbewerber. Zur Begründung fügte der Makler seiner E-Mail-Nachricht eine Erklärung zum Geldwäschegesetz und auch einen Zeitungsbericht bei, der die Pflicht zur Identitätsprüfung zum Gegenstand hatte. Es gelang ihm augenscheinlich nicht, den Kaufinteressenten damit zu überzeugen, sodass sich dieser schließlich mit einer Beschwerde an meine Behörde wandte. Darin machte er Bedenken gegen das Vorlageverlangen geltend und sah zudem die Gefahr einer unzulässigen Verwendung seiner einmal an den Makler herausgegebenen Ausweisdaten.

Maßgeblich für die rechtliche Beurteilung sind in diesem Fall die Vorschriften des Geldwäschegesetzes (GwG). Dessen Zweck besteht darin, Geldwäsche und Terrorismusfinanzierung zu verhindern (§ 11a Abs. 1 GwG). Es richtet sich an Verpflichtete, wozu nicht nur klassische Kreditinstitute oder Finanzdienstleister zählen, sondern auch Immobilienmaklerinnen und -makler (§ 2 Abs. 1 Nr. 14 in Verbindung mit § 1 Abs. 11 GwG).

Bei einer Transaktion, wie dem Verkauf eine Wohnimmobilie, ist die Maklerin bzw. der Makler verpflichtet, vor deren Durchführung seine Vertragspartner zu identifizieren (§ 11 Abs. 1 GwG). Im Umkehrschluss haben die Vertragspartner diesem die Informationen und Unterlagen zur Verfügung zu stellen, die dieser zur Identifizierung benötigt (§ 11 Abs. 6 Satz 1 GwG). Um die Identifikationspflicht auszulösen, bedarf es allerdings eines ernsthaften Interesses (§ 11 Abs. 2 GwG), wovon zum Zeitpunkt der Objektbesichtigung noch nicht auszugehen ist. Deren Zweck liegt ja gerade darin, dass

sich die Kaufinteressentin oder der Kaufinteressent vor Ort Klarheit darüber verschafft, ob das ihr bzw. ihm bis dahin nur aus dem Exposé bekannte Objekt auch in der Realität ihren/seinen Vorstellungen entspricht. Danach entscheidet sich, ob die Kaufanwärterin bzw. der Kaufanwärter auch nach Inaugenscheinnahme des Objekts am Kaufinteresse festhält. Von einem ernsthaften Interesse im Sinne des Geldwäschegesetzes ist erst dann auszugehen, wenn die bzw. der voraussichtliche Käufer/in einen Kaufvertrag erhalten, sie bzw. er mit der Maklerin bzw. dem Makler oder der Verkäuferin bzw. dem Verkäufer einen Vorvertrag oder eine Reservierungsvereinbarung abgeschlossen oder der Maklerin bzw. dem Makler eine Reservierungsgebühr gezahlt hat. Erst dann muss die Maklerin bzw. der Makler die beteiligten Parteien, also Verkäuferin bzw. Verkäufer und Käuferin bzw. Verkäufer, identifizieren. Die Identifikationspflicht kann nur dann entfallen, wenn sich eine Vertragspartnerin bzw. ein Vertragspartner zuvor schon einmal bei der- oder demselben Geschäftspartner/in identifiziert hat und hierüber Aufzeichnungen vorhanden sind (§ 11 Abs. 3 Satz 1 GwG).

Zur Identifikation hat sich die bzw. der Verpflichtete von beiden Vertragsparteien einen gültigen amtlichen Ausweis (Pass, Personalausweis oder Pass/Ausweisersatz) zeigen zu lassen (§ 12 Abs. 1 Satz 1 Nr. 1 GwG).

Das Geldwäschegesetz regelt auch im Einzelnen, welche Daten von natürlichen Personen zum Zweck der Identifikation zu erheben sind (§ 11 Abs. 4 Nr. 1 GwG). Demnach fallen hierunter neben Vor- und Nachname auch Geburtsdatum und -ort, die Staatsangehörigkeit sowie die Wohnanschrift. Ebenso wie die Art, die Nummer und die den Ausweis ausstellende Behörde sind alle erhobenen Daten aufzuzeichnen (§ 8 Abs. 1, Abs. 2 Satz 1 GwG). Von dem Ausweisdokument muss die bzw. der Verpflichtete zudem eine vollständige Kopie anfertigen oder dieses vollständig optisch digital erfassen (§ 8 Abs. 2 Satz 2 GwG). Die erhobenen Angaben und eingeholten Informationen sind dann für einen Zeitraum von mindestens fünf Jahren aufbewahren (§ 8 Abs. 4 Satz 1 GwG).

Was ist zu tun?

- Immobilienmaklerinnen und -makler haben beim Kauf einer Immobilie die Identität von Käuferinnen bzw. Käufern und Verkäuferin bzw. Verkäufern festzustellen. Diese Identifikationspflicht besteht aber erst bei einem ernsthaften Interesse. Hierfür reicht eine bloße Objektbesichtigung nicht aus. Sie haben sich dann von jeder Partei ein gültiges Ausweisdokument vorlegen zu lassen. Hiervon ist eine vollständige Kopie anzufertigen, oder es muss optisch digital erfasst und gespeichert werden.

Das Geldwäschegesetz enthält damit eine Vielzahl die Verpflichteten treffenden Rechtspflichten und legt im Einzelnen fest, welche personenbezogenen Daten in welcher Art und Weise zu verarbeiten sind. Die datenschutzrechtliche Zulässigkeit resultiert damit aus der oder dem Verpflichteten jeweils auferlegten gesetzlichen Pflichten (Art. 6 Abs. 1 Unterabs. 1 Buchst. c, Abs. 2 DSGVO).
Was die Anfrage des potenziellen Immobilienkäufers angeht, so waren dessen Zweifel unterm Strich berechtigt. Ich konnte ihm hierzu noch ergänzende rechtliche Erläuterungen geben und die maßgeblichen Rechtsvorschriften benennen.

2.2.24 Übergang des Verwaltervertrags vom bisherigen Hausverwalter (Einzelunternehmen) auf eine Kapitalgesellschaft (GmbH)

↗ § 152, § 171 UmwG; § 26 WEG; Art. 6 Abs. 1 Buchst. b DSGVO

Die Vielfalt der von meiner Behörde zu beachtenden und anzuwendenden Rechtsvorschriften spiegelt sich in einem weiteren Fall aus dem Bereich der Wohnungswirtschaft wider. Die Eigentümerversammlung eines größeren Immobilienobjekts beschloss sechs Wochen vor Ablauf des Verwaltervertrags – dabei handelt es sich um einen Einzelkaufmann – dessen Verlängerung für weitere fünf Jahre. Hierzu veranlasste der Beirat einen kurzen Nachtrag zum bestehenden Verwaltervertrag.
Als im darauffolgenden Jahr die turnusgemäße Eigentümerversammlung anstand, wunderte sich ein Wohnungseigentümer nicht schlecht darüber, dass das Einladungsschreiben den Briefkopf einer ihm unbekannten GmbH trug. Wie sich bei deren näherer Betrachtung herausstellte, tauchte der Einzelunternehmer darauf nunmehr als (neuer) Geschäftsführer jener GmbH auf. Ein Blick auf die Tagesordnung offenbarte, dass darin auch die Erarbeitung und Bestätigung eines angepassten Verwaltervertrags vorgesehen war, begründet mit dem ab 1. Januar 2021 neu geltenden Wohnungseigentumsgesetz (WEG). Dies reichte dem Eigentümer als Beleg dafür, dass der Geschäftsführer selbst die Rechtmäßigkeit

der „heimlichen" Installation der GmbH als neuen Hausverwalter infrage stellte. Die daraufhin vorgenommene Recherche im öffentlich zugänglichen Handelsregister nährte die Zweifel des Wohnungseigentümers, fand er dabei doch heraus, dass basierend auf einem Gesellschafterbeschluss die Übernahme des einzelkaufmännischen Unternehmens als Gesamtheit sowie eine GmbH-Umfirmierung stattfanden. Zum Zeitpunkt der Beschlussfassung und auch der Unterzeichnung des Vertragsnachtrags gab es jedoch noch keinen Eintrag im Handelsregister.

Aus Sorge um seine personenbezogenen Eigentümerdaten stellte er sich die Frage nach deren Verbleib. Der ohne Beteiligung der Wohnungseigentümergemeinschaft vollzogene Übergang der Verwaltertätigkeit warf aus seiner Sicht auch Haftungsfragen auf. Schließlich bemängelte er die fehlende Zustimmung zum Verbleib dieser Daten bei der GmbH, sodass sich seine Beschwerde auf die unberechtigte Weitergabe seiner Eigentümerdaten von dem Einzelunternehmen an die Kapitalgesellschaft (GmbH) konzentrierte. In diesem Kontext rügte er auch eine fehlende Information über den Datenübergang.

Im Vorgriff einer datenschutzrechtlichen Beurteilung war zunächst zu klären, wie sich der Unternehmensübergang darstellte. Hierzu bedurfte es eines Blicks in das Umwandlungsgesetz (UmwG). Der Rechtsbegriff der Umwandlung meint die gesellschaftliche Neuordnung von Unternehmen. Diese kann sich auf verschiedene Arten vollziehen, also in Form einer Verschmelzung oder Spaltung. Bei der Übernahme des einzelkaufmännischen Verwalterunternehmens in die neu gegründete GmbH handelte es sich rechtlich gesehen um eine Ausgliederung als Unterform der Spaltung (§ 152 Satz 1 UmwG). Danach kann das von einem im Handelsregister eingetragenen Einzelkaufmann betriebene Unternehmen zur Aufnahme durch eine Personen-, Kapitalgesellschaft oder eine eingetragene Genossenschaft oder Neugründung einer Kapitalgesellschaft ausgegliedert werden. Entscheidender Zeitpunkt für den Unternehmensübergang, bei dem auch das von der Ausgliederung umfasste Vermögen sowie

die Verbindlichkeiten im Wege der partiellen Gesamtrechtsnachfolge übergehen (§ 171 Satz 1 in Verbindung mit § 131 Abs. 1 Nr. 1 UmwG), ist die Eintragung im Handelsregister. Die vom Einzelkaufmann geführte Firma erlischt nach § 155 Satz 1 UmwG vollständig. Die Löschung wird nach § 155 Satz 2 in Verbindung mit § 171 UmwG mit der Eintragung ins Handelsregister des übertragenden Rechtsträgers (Einzelunternehmen) wirksam.

Die sich daran anschließende Frage war, welche Auswirkungen die Umwandlung aus der Sicht des Wohnungseigentumsgesetzes auf das Bestehen bzw. die Verlängerung des Verwaltervertrags hatte. Der Zufall wollte es, dass sich zur selben Zeit auch der Bundesgerichtshof mit dieser Fragestellung beschäftigte (Urteil vom 2. Juli 2021, Az. V ZHR 201/20). Aus Sicht des Gerichts ist ein entscheidender Punkt, ob es den Wohnungseigentümerinnen und -eigentümern mit der Bestellung einer natürlichen Person zur Verwalterin bzw. zum Verwalter in besonderem Maße auf die höchstpersönliche Wahrnehmung der Verwalteraufgaben durch diese natürliche Person ankommt. Dabei geht der Bundesgerichtshof indes nicht davon aus, dass die Bestellung einer natürlichen Person zur Verwalterin bzw. zum Verwalter (wie zum Beispiel bei einer Einzelkauffrau bzw. einem Einzelkaufmann) dem Verwalteramt und -vertrag einen höchstpersönlichen Charakter verleiht. Heranzuziehen sind dabei nicht die Vorschriften des Bürgerlichen Gesetzbuchs (§§ 671, 613 Abs. 1 BGB) oder die des Wohnungseigentumsgesetzes (§ 26 Abs. 1 WEG), sondern vielmehr die Vorschriften des Umwandlungsgesetzes als vorrangige Sonderreglungen.

Nach seiner Ansicht bietet eine fachkundige Verwalterin bzw. ein fachkundiger Verwalter auch dann eine Gewähr für die ordnungsmäßige Aufgabenerfüllung, wenn sie bzw. er Mitarbeiterinnen bzw. Mitarbeiter beschäftigt, denen sie bzw. er die Verwaltung überträgt. Dies kann sie bzw. er sowohl als Einzelunternehmerin bzw. Einzelunternehmer als auch als Gesellschafterin bzw. Gesellschafter und Geschäftsführerin bzw. Geschäftsführer mit maßgeblichem Einfluss auf die Gesellschaft. Die Sachkunde und Leistungsfähigkeit der Person

der Verwalterin bzw. des Verwalters geht also auch mit der Tätigkeit als GmbH-Geschäftsführer nicht verloren.

Die Wohnungseigentümerinnen und -eigentümer sind bei einer Unternehmungsumwandlung auch nicht schutzlos gestellt. Verlieren sie das Vertrauen in die Person der Verwalterin bzw. des Verwalters (zum Beispiel nach einem Geschäftsführerwechsel), steht ihnen ein Abberufungs- und außerordentliches Kündigungsrecht zu. Nach der ab 1. Dezember 2020 geltenden Rechtslage ist eine Verwalterabberufung jederzeit möglich (§ 26 Abs. 3 Satz 1 WEG).

Es lässt sich also feststellen, dass ein Verwaltervertrag nicht automatisch bei einer Unternehmensausgliederung endet. Wollte man davon ausgehen, müsste die neue Verwalterin bzw. der neue Verwalter für jede Wohnungseigentümergemeinschaft der bisher verwalteten Objekte eine Eigentümerversammlung einberufen, um darüber die Zustimmung zur Übertragung oder Verwalterbestellung der (neuen) Kapitalgesellschaft sowie den Abschluss eines neuen Verwaltervertrags zu erreichen. Hiergegen spricht nach dem entscheidenden Gericht, dass eine Ausgliederung gerade auf die Fortgeltung des Verwaltervertrags abzielt und diese gerade im Sinne der Wohnungseigentümerinnen und -eigentümer ist. Im anderen Fall bestünde ein verwalterloser Zustand oder die natürliche Person der bzw. des vormals eingetragenen Einzelkauffrau/kaufmanns wäre zur Erfüllung der Verwalteraufgaben rechtlich nicht (mehr) imstande.

Der Beschränkung des Haftungsumfangs bei einer GmbH kommt dabei auch keine Bedeutung zu, da eine Einzelkauffrau bzw. ein Einzelkaufmann für die Dauer von fünf Jahren der Nachhaftung für übergegangene Verbindlichkeiten unterliegt (§§ 156, 157 UmwG). Damit haben die Wohnungseigentümerinnen und -eigentümer ausreichend Zeit zur Bestellung einer anderen Verwalterin bzw. eines anderen Verwalters, sollten sie die Haftungsbeschränkung nicht hinnehmen wollen.

Der Bundesgerichtshof verneint auch die Pflicht zur Einholung von Alternativangeboten. Er sieht diese nur dann als verpflichtend, wenn es zu relevanten Veränderungen der Amtsführung

der Verwalterin bzw. des Verwalters (zum Beispiel Qualitätsdefiziten) gekommen ist oder andere Verwaltungen dieselben Leistungen spürbar kostengünstiger erbringen. Auch die faktische Fortführung der Verwaltertätigkeit durch das neu gegründete Unternehmen erfordert keine Alternativangebote, können die Wohnungseigentümerinnen und -eigentümer doch insbesondere dadurch beurteilen, ob der neue Rechtsträger die Anforderungen an eine ordnungsgemäße Verwaltung erfüllt und sie mit diesem zurechtkommen.

In dem Aufsichtsverfahren bei meiner Behörde stellte sich noch die Frage, ob die neu gegründete GmbH überhaupt zur Eigentümerversammlung einladen konnte oder ob sie als unberechtigte Dritte anzusehen war. Auch damit setzte sich der Bundesgerichtshof auseinander und meinte hierzu, dass der einladenden Person nur dann eine Bedeutung zukommt, wenn sich der Beschlussmangel auf das Abstimmungsergebnis ausgewirkt hat. Hierfür gab es nach dem Beschwerdesachverhalt keine Anhaltspunkte, erteilten die Wohnungseigentümerinnen und -eigentümer doch der (rückwirkenden) Bestellung der GmbH auch formal mit Beschlussfassung in der Eigentümerversammlung – mit einer Nein-Stimme (mutmaßlich von dem Beschwerdeführer) – ihre Zustimmung.

Im Ergebnis wurde der mit dem Einzelunternehmen geschlossene Verwaltervertrag mit der GmbH als juristischer Person fortgesetzt. Aus datenschutzrechtlicher Sicht ist die (weitere) Verarbeitung der personenbezogenen Eigentümerdaten damit durch die Erforderlichkeit zur Vertragserfüllung legitimiert (Art. 6 Abs. 1 Buchst. b DSGVO), sodass es auf eine Einwilligung der betroffenen Eigentümerinnen und -eigentümer nicht ankam.

Eine rechtsgrundlose und unzulässige Datenweitergabe war damit nicht gegeben. Dementsprechend konnte auch kein Verstoß gegen die Informationspflichten des Art. 13 DSGVO vorliegen. Denn diese Vorschrift bezieht sich nur auf Informationen zum Zeitpunkt der Datenerhebung. Sie findet also auf einen Betriebsübergang oder eine Firmenübernahme und die dabei erfolgende Datenüberleitung gerade keine Anwendung. Gleichwohl wäre es im konkreten Beschwerdefall rat-

Was ist zu tun?

Ändert sich bei einer Wohnungseigentümergemeinschaft der laufende Verwaltervertrag, weil die Hausverwalterin bzw. der Hausverwalter sich von einem Einzelunternehmen zu einer GmbH wandelt, endet der Vertrag dadurch nicht automatisch. Die neue Verwalterin bzw. der neue Verwalter setzt den bestehenden Vertrag fort, ohne Auswirkungen auf die datenschutzrechtliche Zulässigkeit der Datenverarbeitung. Es ist allerdings zu empfehlen, die betroffenen Eigentümerinnen und Eigentümer von der Änderung zu informieren, auch wenn datenschutzrechtlich hierzu keine Pflicht besteht.

sam gewesen, wenn die Änderung der Hausverwaltung den davon betroffenen Wohnungseigentümerinnen und -eigentümern zeitnah kommuniziert worden wäre.

2.2.25 Mitglieder von Wohnungseigentümergemeinschaften dürfen die Höhe der Nach- oder Überzahlung der anderen Mitglieder über die Jahresabrechnung erfahren

↗ §§ 18, 26, 28 WEG, Art. 6 Abs. 1 DSGVO

Immer wieder erreichen mich Beschwerden von Mitgliedern von Wohnungseigentümergemeinschaften. Diese zielen zumeist gegen Hausverwaltungen, denen man einen unsachgemäßen Umgang mit den Eigentümerdaten unterstellt. Wie sich nicht selten bei meiner Untersuchung herausstellt, bestehen oftmals schon langjährige Meinungsverschiedenheiten mit einzelnen Eigentümerinnen und Eigentümern.

Die Ausübung einer Verwaltertätigkeit bedingt den fortwährenden Umgang mit personenbezogenen Eigentümerdaten der verwalteten Objekte. Zu denken sei hier etwa an die Einladung, Durchführung und Protokollierung von Eigentümerversammlungen, aber auch die Aufstellung eines Wirtschaftsplans und über die jährliche Abrechnung hierüber in Form der Jahresabrechnung. Letztere nahm ein Eigentümer zum Anlass und wandte sich deswegen mit einer Eingabe an meine Behörde. Der monierten Jahresabrechnung lag eine Anlage bei, in der die Abrechnungsergebnisse (als Summenbeträge) aller Wohneinheiten aufgeführt waren. Diese erlaubte jedem Mitglied der Wohnungseigentümergemeinschaft die Kenntnis darüber, bei welchem der anderen Eigentümerinnen und Eigentümer eine Nach- oder Überzahlung anfiel und wie hoch diese in Summe war.

Nach dem Wohnungseigentumsrecht liegt die Verwaltung des gemeinschaftlichen Eigentums zunächst bei der Gemeinschaft der Wohnungseigentümerinnen und -eigentümer (§ 18 Abs. 1 Wohnungseigentumsgesetz – WEG). Diese können mit einfacher Mehrheit eine Verwalterin oder einen Verwalter

bestellen (§ 26 Abs. 1 WEG), die bzw. der auch zur Erstellung einer jährlichen Abrechnung über den Wirtschaftsplan nach Ablauf eines Kalenderjahres verpflichtet ist (§ 28 Abs. 2 Satz 2 WEG). Diese Jahresabrechnung – auch als Hausgeld- oder WEG-Abrechnung bekannt – veranschaulicht die Einnahmen und Ausgaben der Wohnungseigentümergemeinschaft im Zeitraum eines Kalenderjahres durch Einzelabrechnungen und eine Gesamtrechnung. Auf die Kosten der Gemeinschaft (das sogenannte Hausgeld) zahlen die einzelnen Eigentümerinnen und Eigentümer monatliche Vorschüsse. Am Ende eines Kalenderjahres werden die Vorschüsse den Ausgaben gegenübergestellt und entsprechende Nachzahlungs- und Guthabenbeträge je Eigentümer ermittelt.

Die Jahresabrechnung ist damit wesentlich für die Beschlussfassung über die Einforderung von Nachschüssen oder die Anpassung von Vorschüssen (§ 28 Abs. 2 Satz 1 WEG). Eine gesetzliche Pflicht zur Offenlegung des Summenergebnisses je Wohneinheit gegenüber allen Eigentümerinnen und Eigentümern enthält die Vorschrift des § 28 Abs. 2 WEG indes nicht. Damit fehlt es auch an der Erforderlichkeit zur Erfüllung einer rechtlichen Verpflichtung (Art. 6 Abs. 1 Buchst. c Datenschutz-Grundverordnung – DSGVO).

Der zwischen der Eigentümergemeinschaft und der Hausverwaltung abgeschlossene Verwaltervertrag regelt, dass Letztere eine ordnungsgemäße Abrechnung erstellen muss. Eine Jahresabrechnung ist dann ordnungsgemäß, wenn sie

- aus sich heraus schlüssig ist und
- einer Plausibilitätskontrolle standhält.

Zwar bewertet der Bundesgerichtshof eine Abrechnung bereits dann als schlüssig, wenn darin der Anfangs- und Endbestand der Gemeinschaftskonten sowie die nach Kostenart aufgegliederten Einnahmen und Ausgaben enthalten sind (Bundesgerichtshof, Urteil vom 25. September 2020, Az. V ZR 80/19). Eine Jahresabrechnung ist nach Ansicht des Gerichts dann plausibel, wenn sich mittels Addition bzw. Subtraktion (Anfangsbestand plus Einnahmen minus Ausgaben) der Endbestand ermitteln lässt. Ungeachtet dessen halte ich es für

eine ordnungsgemäße Vertragserfüllung aus Verwaltersicht nicht nur geboten, sondern auch für erforderlich, in die Abrechnung gleichfalls die summierten Abrechnungsbeträge je Wohneinheit aufzunehmen (Art. 6 Abs. 1 Buchst. b DSGVO). Schließlich gibt es auch ein berechtigtes Informationsinteresse der Mitglieder der Wohnungseigentümergemeinschaft an den Summenbeträgen der anderen Mitglieder. So fanden sich im konkreten Beschwerdefall in der dortigen Jahresabrechnung an mehreren Stellen die in einer Anlage aufgeführten Summenbeträge. Ohne deren Beifügung wären die Mitglieder schlicht nicht imstande gewesen, die Herkunft mehrerer in der mehrseitigen Rechnungslegung aufgeführten Beträge ohne Zuhilfenahme der betreffenden Einzelabrechnungen herzuleiten. Einer Eigentümerin oder einem Eigentümer muss es aber ohne Probleme möglich sein, die Jahresrechnung gerade ohne vorherige Einsichtnahme in sämtliche Einzelabrechnungen zu prüfen. Somit konnte sich die Verwaltung auch auf die Wahrung berechtigter Interessen berufen (Art. 6 Abs. 1 Buchst. f DSGVO).

Dessen ungeachtet stellt sich ohnehin die Frage, welche Rückschlüsse sich anhand des geringen Informationsgehalts eines kumulierten Summenwerts auf das individuelle Verbrauchsverhalten der einzelnen Eigentümerinnen bzw. Eigentümer oder deren Mieterinnen bzw. Mieter ziehen lassen.

Was ist zu tun?
Die Hausverwaltung verstößt nicht gegen datenschutzrechtliche Vorschriften, wenn sie einer Jahresabrechnung eine Zusammenstellung mit dem Betrag der Nach/Überzahlung für jedes einzelne Mitglied einer Wohnungseigentümergemeinschaft beifügt. Daraus lassen sich keine Rückschlüsse auf das jeweilige Mitglied, insbesondere dessen individuelles Verbrauchsverhalten, ziehen.

2.3 Einwilligungsfragen

2.3.1 Einwilligungserklärung bei Bestehen einer gesetzlichen Grundlage für die Datenerhebung

↗ Art. 5 Abs. 1 Buchst. a DSGVO

Zwei Körperschaften des öffentlichen Rechts im Gesundheits- bzw. Sozialwesen verwendeten – unabhängig voneinander – Formulare mit denen die Antragstellerin bzw. der Antragsteller in die Datenerhebung oder in die Datenübermittlung einwilligen kann. Diese Formulare wurden auch genutzt, wenn eine gesetzliche Verarbeitungsbefugnis für die zu erhebenden oder anzufordernden Daten im Raum stand. Die For-

mulare für die Einwilligungen sahen nicht vor, dass diese für eine/n konkret zu benennende Ärztin bzw. Arzt, beziehungsweise eine konkrete Einrichtung erteilt wird. Dies wurde mir jeweils durch Beschwerden von Betroffenen bekannt.

Die Petenten rügten, dass sich die Körperschaft Daten von einer Gesundheitseinrichtung verschafft habe, obwohl die vom Petenten erteilte Einwilligungserklärung diese Einrichtungen nicht betraf. Aus Sicht der Petenten war die Datenerhebung deshalb rechtswidrig.

In den Stellungnahmen zu den Petitionen beriefen sich beide Körperschaften des öffentlichen Rechts jeweils darauf, dass eine gesetzliche Grundlage für die Datenerhebung bzw. Datenübermittlung vorlag und diese daher rechtmäßig war.

Meine Prüfung hat ergeben, dass bei allen Beschwerden jeweils eine gesetzliche Verarbeitungsbefugnis vorlag.

Den Körperschaften des öffentlichen Rechts habe ich mitgeteilt, dass aus meiner Sicht eine Einwilligung als Rechtsgrundlage regelmäßig ausscheidet, wenn eine gesetzliche Verarbeitungsbefugnis im Raum steht (vgl. Kühling/Buchner Kommentar zur DSGVO und BDSG. Art. 6 Rdnr. 24). Die Vorgehensweise stellt nach meiner Einschätzung einen Verstoß gegen Treu und Glauben im Sinn von Art. 5 Abs. 1 Buchst. a DSGVO dar, wenn der betroffenen Person einerseits signalisiert wird, dass es für die Datenverarbeitung auf deren Einwilligung ankäme, andererseits aber doch jederzeit auf die Alternative der gesetzlichen Verarbeitungsbefugnis zurückgegriffen werden kann.

Entweder wird eine Datenerhebung oder Datenübermittlung auf eine gesetzliche Grundlage gestützt, oder sie erfolgt auf der Grundlage einer Einwilligungserklärung. Eine „Kombination" beider Rechtsgrundlagen halte ich nicht für zulässig.

Wird eine Einwilligungserklärung verwendet, so ist die Einwilligung jeweils für die konkrete Einrichtung bzw. die konkrete Ärztin bzw. den konkreten Arzt abzufordern. Die Erklärung ist von der oder dem Betroffenen so auszufüllen, dass sie bzw. er konkret aufführt, für welche Ärztin oder welchen Arzt, Einrichtung/Krankenhaus diese jeweils erteilt wird. Dazu kann das Formular verwendet werden, das auch auf

Musterformular zur Entbindung von der Schweigepflicht:
↗ sdb.de/tb2203

meiner Internetseite eingestellt ist. Eine „pauschale" Einwilligung abzufordern ist nach meiner Einschätzung nicht zulässig, da diese inhaltlich unbestimmt ist.
Die beiden Körperschaften wurden daher von mir aufgefordert, die Einwilligungserklärungen künftig nur noch zu verwenden, wenn keine gesetzliche Verarbeitungsbefugnis besteht. Einwilligungen, soweit im Einzelfall unbedingt nötig, sind nur für die konkrete Einrichtung bzw. die konkrete Ärztin oder den konkreten Arzt von den betroffenen Personen abzufordern.
Eine Körperschaft hat mir bereits mitgeteilt, dass sie ihre Verfahrensweise entsprechend ändern wird. Von der zweiten Körperschaft liegt mir zwischenzeitlich eine Stellungnahme vor. Es sind weitere Abstimmungen erforderlich.
Was ist zu beachten? Eine Datenerhebung kann sich entweder auf eine gesetzliche Grundlage oder auf eine Einwilligungserklärung stützen.

2.3.2 Aufzeichnung von Telefongesprächen

↗ DSGVO

Ein immer wiederkehrendes Thema in der Beschwerdebearbeitung ist die Aufzeichnung von Telefongesprächen bei Handel und Dienstleistung. Fast schon regelmäßig geht es dabei um die Qualitätssicherung der geführten Telefonate, und oftmals wird den anrufenden Personen dann keine Alternative zu einer Gesprächsaufzeichnung geboten, das heißt, es erfolgt ein bloßer Hinweis zu Beginn des Telefonats, ohne dass eine Möglichkeit des Abwählens der Gesprächsaufzeichnung besteht. Wollen oder müssen die anrufenden Personen das Telefonat führen, etwa, weil es auf eine zeitnahe Sachverhaltsklärung ankommt, müssen sie dann hinnehmen, dass das Telefonat aufgezeichnet wird.
Festzustellen ist zunächst, dass eine solche Gesprächsaufzeichnung keinesfalls auf Art. 6 Abs. 1 Buchst. f Datenschutz-Grundverordnung (DSGVO) gestützt werden kann. Dagegen spricht zum einen, dass eine Gesprächsaufzeichnung schon nicht erforderlich ist, denn die Qualitätssicherung des Telefonats kann auch durch andere Möglichkeiten erreicht wer-

den kann, zum Beispiel durch eine freiwillige Beantwortung von Fragen mit „Ja" und „Nein" im Anschluss an das Gespräch. Darüber hinaus stehen aber auch gewichtige Interessen der anrufenden Personen einer Aufzeichnung entgegen, denn hier geht es um die Gewährleistung der Vertraulichkeit des nichtöffentlich gesprochenen Wortes.

DSK-Beschluss zur Aufzeichnung von Telefongesprächen:
↗ sdb.de/tb2204

Die Datenschutzkonferenz hat dazu schon 2018 einen Beschluss gefasst. Danach ist die Aufzeichnung von Telefongesprächen in aller Regel nur mit Einwilligung der anrufenden Person zulässig. Eine datenschutzrechtlich wirksame Einwilligung im Sinne von Art. 4 Nr. 11 DSGVO setzt voraus, dass die anrufende Person vor Beginn der beabsichtigten Aufzeichnung gefragt wird, ob sie mit der Aufzeichnung einverstanden ist und, falls sie einverstanden ist, gebeten wird, ihr Einverständnis beispielsweise durch Aussprechen eines „Ja" oder durch eine aktive bestätigende Handlung (etwa durch das Betätigen einer Telefontaste) eindeutig zum Ausdruck zu bringen. Die bloße Einräumung einer Widerspruchsmöglichkeit und das anschließende Fortsetzen des Telefonats stellen keine datenschutzrechtlich wirksame Einwilligung im Sinne der Datenschutz-Grundverordnung dar. Da der Verantwortliche nachweisen können muss, dass die betroffene Person eine wirksame Einwilligung erteilt hat (Art. 7 Abs. 1 DSGVO), muss er auch nachweisen können, dass die Einwilligung „in informierter Weise" abgegeben worden ist (vgl. Art. 4 Nr. 11 DSGVO).

Leitlinien 05/2020 des EDSA zur Einwilligung gemäß Verordnung 2016/679:
↗ sdb.de/tb2205

Die Datenschutzaufsichtsbehörden halten auch weiterhin an diesem Beschluss fest und schließen insbesondere eine konkludente Einwilligung (Weitertelefonieren ohne bestätigende Handlung) als Rechtsgrundlage für die Gesprächsaufzeichnung aus. So spricht auch der Erwägungsgrund 32 zur Datenschutz-Grundverordnung von einer „eindeutig bestätigenden Handlung". Diese muss der Verantwortliche auch nachweisen können (Art. 5 Abs. 2 DSGVO). Diese Auffassung wird weiterhin gestützt durch die Leitlinien 05/2020 des Europäischen Datenschutzausschusses (EDSA) zur Einwilligung gemäß Verordnung 2016/679, Version 1.1, angenommen am 4. Mai 2020.

Darin wird unter den Randnummern 75 bis 77 und 95 ausgeführt, dass ein bloßes Weiternutzen nicht als Einwilligung ausreicht, sondern es sich vielmehr um eine eindeutig bestätigende Handlung handeln muss. Demnach muss eine Einwilligung stets durch eine aktive Handlung oder Erklärung erteilt werden. Es muss offensichtlich sein, dass die betroffene Person in diese bestimmte Verarbeitung eingewilligt hat.
Eine Widerspruchslösung, die – wie mir schon vorgetragen wurde – darin besteht, dass man die Telefonaufzeichnung zwar abwählen kann, aber gerade dies eine aktive Handlung, zum Beispiel das laute Sagen eines „Nein", erfordert, wird diesen Vorgaben nicht gerecht. Nicht die Ablehnung ist durch eine aktive Handlung zu erklären, sondern die Einwilligung. Dies widerspräche auch den Vorgaben des Art. 25 DSGVO – Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen, zudem gingen dann undeutliches Sprechen, fehlerhafte Antwortinterpretationen, Überhören oder Nichtverstehen der entsprechenden Ansage regelmäßig zulasten der anrufenden Person.
Selbst wenn man im Übrigen – verlässliche Rechtsprechung hierzu liegt noch nicht vor – konkludente Einwilligungen als zulässig anerkennen würde, wäre die Freiwilligkeit der Einwilligung infrage zu stellen. Die Freiwilligkeit wäre nur gewährleistet, wenn eine adäquate Alternative vorhanden wäre. Diese ist jedoch dann zu verneinen, wenn am Anfang des Telefonats auf den schriftlichen Weg oder eine E-Mail verwiesen wird. Beide Optionen stellen im Vergleich zu einem Telefonat deutlich langsamere Kommunikationswege dar und sind damit keine angemessene Alternative.

Was ist zu tun?
Vor der Aufzeichnung von Telefongesprächen ist regelmäßig die Einwilligung der anrufenden Person einzuholen; ein bloßer Hinweis auf die Aufzeichnung genügt insoweit nicht.

2.3.3 Personalausweiskopien bei der Anmietung von Lagerraum

↗ § 20 PAuswG, DSGVO

„Selfstorage" als eine moderne Art des Einlagerns von Gegenständen beliebiger Art ist eine wachsende Branche und wird inzwischen in vielen deutschen Städten angeboten. Man kann für beliebige Zeiträume Lagerräume beliebiger Größe anmieten

und dort Dinge, für die man selbst vorübergehend keine eigenen Lagermöglichkeiten hat, sicher und überwacht einlagern.

Von einem potenziellen Kunden bin ich auf die offensichtliche Praxis eines solchen Selfstorage-Anbieters, im Rahmen der Vertragsanbahnung von seiner Kundschaft alternativlos und somit als Bedingung für einen Vertragsabschluss eine ungeschwärzte Personalausweiskopie zu verlangen und anschließend für die Dauer des Mietvertrages aufzubewahren, angesprochen worden.

Rechtsgrundlage für die Verarbeitung personenbezogener Daten im Rahmen eines Vertragsverhältnisses ist zunächst einmal Art. 6 Abs. 1 Buchst. b Datenschutz-Grundverordnung (DSGVO). Danach muss die Verarbeitung für die Erfüllung des Vertrages oder zur Durchführung vorvertraglicher Maßnahmen erforderlich sein. Unstreitig sein dürfte die Feststellung, dass solche Personalausweisdaten wie Personalausweisnummer, Augenfarbe, Körpergröße, Ausstellungsdatum, Meldebehörde, Gültigkeitsablauf und Zugangsnummer keine Bedeutung für den Vertragsabschluss und dessen Durchführung haben und somit nach dieser Vorschrift nicht verarbeitet werden dürfen. Darüber hinaus und dessen ungeachtet ist die Anfertigung von Personalausweiskopien immer dann nicht notwendig, wenn sich die Vertragsparteien beim Vertragsabschluss persönlich gegenüberstehen und eine Identifizierung des Vertragspartners durch bloße Einsichtnahme in den Personalausweis (§ 20 Abs. 1 Personalausweisgesetz {PAuswG}) möglich ist. Das betreffende Selfstorage-Unternehmen bietet seiner Kundschaft einen Vertragsabschluss nicht nur online, sondern auch in seinen Filialen an – insoweit wäre die Verfahrensweise zumindest in diesen Fällen möglich und daher auch so vorzusehen.

Unabhängig davon eröffnet § 20 Abs. 2 PAuswG auch die Möglichkeit der Anfertigung von Personalausweiskopien. Dabei darf der Ausweis nur von der Ausweisinhaberin bzw. vom Ausweisinhaber oder von anderen Personen mit Zustimmung der Inhaberin bzw. des Inhabers in der Weise abgelichtet werden, dass die Ablichtung eindeutig und dauerhaft als Kopie erkennbar ist. Werden durch Ablichtung personenbezogene Daten aus dem Personalausweis erhoben oder

verarbeitet, so darf die datenerhebende oder -verarbeitende Stelle dies nur mit Einwilligung der Ausweisinhaberin bzw. des Ausweisinhabers tun.

Die Anfertigung von Personalausweiskopien erfordert demnach zunächst einmal die Einwilligung der Vertragspartnerinnen und -partner. Die Einwilligung muss freiwillig erteilt werden (Art. 7 Abs. 4 DSGVO), jederzeit widerrufbar (Art. 7 Abs. 3 DSGVO) sowie nachweisbar (Art. 5 Abs. 2 DSGVO) sein und darf insbesondere wegen des Kopplungsverbotes (Art. 7 Abs. 4 DSGVO) nicht als zwingende Voraussetzung für den Vertragsabschluss benannt werden. Darüber hinaus ergibt sich aus dem Erforderlichkeitsgebot des bereits benannten Art. 6 Abs. 1 Buchst. b DSGVO einerseits wie auch dem Gebot der Datenminimierung (Art. 5 Abs. 1 Buchst. c DSGVO) andererseits die Forderung, dass der Kundschaft bezüglich der bereits genannten Datenarten die Möglichkeit einer Teilschwärzung der Ausweiskopie eingeräumt wird.

Nachdem ich dem Selfstorage-Unternehmen den Sachverhalt vorgehalten hatte, hat mir dieses unmittelbar zugesichert, das Verfahren so umzustellen, dass das Gebot der Datenminimierung entsprechend gewahrt bleibt, das heißt, eine Verarbeitung für den Vertragszweck nicht erforderlicher Daten zukünftig unterbleibt und insbesondere auch Schwärzungen möglich sind. Die Umsetzung der datenschutzrechtlichen Vorgaben werde ich nach pflichtgemäßem Ermessen weiter begleiten. Der Beschwerdeführer hatte sich – abgeschreckt durch diese Forderung – inzwischen bereits eine Alternative gesucht und dem Unternehmen erst gar keine Ausweiskopie übergeben. Dies kann als Beispiel gelten, dass datenschutzwidriges Verhalten durchaus auch Kunden kosten und damit Umsatzeinbußen bewirken kann.

Was ist zu tun?
Die Abforderung von Personalausweiskopien sollte stets kritisch hinterfragt werden; Schwärzungen von für einen Vertragsabschluss nicht erforderlichen Daten sind grundsätzlich zulässig. Bei direktem Kundenkontakt reicht zur Identifizierung regelmäßig eine Einsichtnahme in den Personalausweis.

2.3.4 Spendenaufruf einer Hochschule an ehemalige Absolventen

↗ Art. 18 DSGVO

Die ehemalige Studentin einer sächsischen Hochschule hatte sich an mich gewandt, nachdem sie von einer Fakultät ihrer

damaligen Hochschule eine Mail, einen Spendenaufruf betreffend, erhalten hatte. Die Petentin hatte sich auch bereits direkt an die Hochschule gewandt.
Alle Absolventinnen und Absolventen der Hochschule erhalten nach Auskunft der Hochschule dort ein Einwilligungsformular zur Erfassung in der Alumnidatenbank. In dem damaligen Erfassungsformular, welches nach Auskunft der Hochschule auch die Petentin ausgefüllt hatte, waren die Verarbeitungszwecke: „die Zuordnung und Kontaktaufnahme, Berichterstattung und ggf. Marketingmaßnahmen sowie für statistische Zwecke durch die Hochschule" genannt, wobei die Hochschule unter Marketingmaßnahmen zum Beispiel auch Spendenaufrufe mit umfasst sah. Seitens der Hochschule war der Petentin unter Hinweis auf Art. 18 Datenschutz-Grundverordnung (DSGVO) sodann angeboten worden, in der von der Hochschule geführten Datenbank zu vermerken, dass in ihrem Fall keine Kontaktaufnahme zu Marketingzwecken zukünftig erfolgen dürfe.
Dies war nach erteilter Zustimmung der Petentin sodann auch erfolgt, das Petitum der Petentin konnte insoweit also abgeschlossen werden.
Da ich allerdings davon ausging, dass dieses Angebot auch anderen Absolventinnen und Absolventen der Hochschule zur Verfügung gestellt werden sollte, habe ich die Eingabe zum Anlass genommen und die Hochschule aufgefordert, das betreffende Einwilligungsformular transparenter zu überarbeiten, insbesondere entsprechende Auswahlmöglichkeiten zur Nutzung der E-Mail-Adressen zuzulassen.
Die im Rahmen der Alumnidatenbank verwendeten Formulare wurden hierauf diesbezüglich überarbeitet.

2.3.5 Schulische Zirkusprojekte

↗ § 22 KunstUrhG, Art. 7 DSGVO, VwV Schulformulare,

Seit einigen Jahren bieten sächsische Schulen Zirkusprojektwochen an. Wie ich jetzt erfahren musste, werden bei diesen jedoch mitunter die Belange des Datenschutzes vernachlässigt.

So informierten mich Eltern, dass sie von ihrem Kind ein Bestellformular für eine DVD von der Aufführung erhielten. So erfuhren sie erstmals von der Aufnahme der Aufführung mit Videokamera. Geplant waren offensichtlich die Vervielfältigung und Verteilung an die Eltern der beteiligten Kinder. Vorherige Informationen zur Videoaufzeichnung hatten sie nicht erhalten. Im Gegenteil: Bei Schuleintritt hatten sie in einem Formular Film/Videoaufnahmen widersprochen. Eine Einwilligung seitens des Projektzirkus wurde nicht erfragt, da sie nicht als erforderlich angesehen wurde.
Auch wenn die Petenten sich schließlich mit dem Zirkus so verständigten, dass ihr Kind maskiert auftritt, habe ich die Petition zum Anlass genommen, mich dazu an das Landesamt für Schule und Bildung (LaSuB) zu wenden. Ich bat um Information der sächsischen Schulen, dass derartige Veröffentlichungen nach § 22 Kunsturhebergesetz (KunstUrhG) nur mit Einwilligung zulässig sind.
Nr. II.5 VwV Schuldatenschutz weist auf Folgendes hin:

> „(1) Hat der Schüler das vierzehnte Lebensjahr noch nicht vollendet, ist die Einwilligung der Personensorgeberechtigten des Schülers notwendig.
> (2) Hat der Schüler das vierzehnte Lebensjahr vollendet, kann er die Einwilligung selbst erteilen, sofern er die nötige Einsichtsfähigkeit hierfür besitzt. Die Einsichtsfähigkeit setzt voraus, dass der Schüler die Risiken und Folgen der Verarbeitung der ihn betreffenden personenbezogenen Daten vorhersehen und sachgerecht einschätzen kann. Verfügt der minderjährige Schüler nicht über diese Einsichtsfähigkeit, bedarf es der Einwilligung der Personensorgeberechtigten. In Zweifelsfällen ist die Einwilligung sowohl des minderjährigen Schülers als auch der Personensorgeberechtigten notwendig."

Das LaSuB hat meine Anregung aufgenommen und diese rechtlichen Hinweise mit Handlungsempfehlungen unter dem Betreff „Einwilligung in Foto-, Film- und Videoaufnahmen bei Veranstaltungen und Projekten, zum Beispiel Zirkusprojekt, an

Schulen" im Schulportal für alle sächsischen Schulen veröffentlicht.

2.3.6 Abo-Modelle im Online-Bereich

↗ DSGVO, TTDSG

Seit einigen Jahren bieten große Medienhäuser für eine Nutzung der publizistischen Online-Angebote sogenannte Pur-Abonnements oder ähnlich genannte Möglichkeiten an. Verbraucherinnen und Verbraucher werden vor die Wahl gestellt, entweder ein Abonnement zur werbefreien Nutzung der Website abzuschließen oder es wird eine Zustimmung in eine weitreichende Nachverfolgung des Nutzungsverhaltens und das Teilen der Daten mit einer unüberschaubaren Anzahl von Werbepartnerinnen und -partnern gefordert. Bei genauer Betrachtung der Modelle fällt auf, dass ein solches Pur- oder Weberfrei-Abo mitnichten alle Inhalte der Website umfasst, es gibt dann meist noch ein zusätzliches Abonnement für die Premium-Artikel. Das Werbefrei-Abo ermöglicht in vielen Fällen also lediglich eine Nutzung der Website, wie es auch mit einem handelsüblichen Werbeblocker und Zustimmung möglich ist. Auch wenn sich die Verlage bedeckt halten, ist der wirtschaftliche Hintergrund klar weniger auf den Abschluss von möglichst vielen Werbefrei-Abos gerichtet als vielmehr auf eine möglichst hohe Zustimmungsrate für das Online-Tracking. Eine damit verbundene Weitergabe an eine bis zu dreistellige Anzahl an Verantwortliche, die mit den Daten website-übergreifende persönliche Profile für Online-Werbung erstellen und handeln, dürfte als datenschutzrechtliches Problem offenkundig sein. Auch wenn sich viele Verbraucherinnen und Verbraucher an das Vorhandensein von Online-Werbung gewöhnt haben, würden die meisten über die Masse und die Tiefe an erhobenen Daten, die das Verhalten im Netz minutiös und zielgenau erfassen, verknüpfen und mit statistischen Daten anreichern, erstaunt sein. Bereits hier wird deutlich, dass die Freiwilligkeit einer Einwilligung auf sehr tönernen Füßen steht und sich die Frage stellt, ob diese als generelle und vom Ansatz her schran-

kenlose Legitimation überhaupt tauglich ist. Vor allem auch deshalb, weil diese Einwilligungen täglich auch von zahlreichen Minderjährigen abgegeben werden. Auch Minderjährige nutzen Medien, und das Datenschutzrecht sieht einen besonderen Schutz für diese Zielgruppe vor, der in der Praxis schlicht nicht vorhanden ist.

Die im Jahr 2021 im Rahmen der Umsetzung der sogenannten Digitale-Inhalte-Richtlinie eingeführten Änderungen im Bürgerlichen Gesetzbuch (BGB), welche ein Bezahlen mit Daten in den §§ 327ff. in Form von Verbraucherverträgen prinzipiell vorsieht, hat vielfach für Diskussionen gesorgt, da – ungeachtet der rechtlichen Möglichkeit – die Vorgaben der DSGVO parallel bestehen und zusätzlich Verbraucherschutzrecht zu beachten ist.

Tätigkeitsbericht 2020:
↗ sdb.de/tb2020

Die deutschen Aufsichtsbehörden haben sich im Rahmen der laufenden Medienprüfung (siehe Tätigkeitsbericht 2020, 7. Gemeinsame Überprüfung von Medienunternehmen durch Datenschutzaufsichtsbehörden, Seite 164) mit der Thematik befasst und die nachfolgend dargestellte Auffassung entwickelt. Eine Beschlussfassung kam bislang noch nicht zustande.

1. Grundsätzlich ist denkbar, die Nachverfolgung von Nutzerverhalten (Tracking) auf eine Einwilligung zu stützen, wenn alternativ ein trackingfreies Bezahlmodell angeboten wird. Die Leistung, die Nutzer/innen bei einem Bezahlmodell erhalten, muss jedoch erstens eine gleichwertige Alternative zu der Leistung darstellen, die Nutzer/innen durch eine Einwilligung erlangen. Zweitens muss die Einwilligung alle Wirksamkeitsvoraussetzungen gemäß Art. 4 Nr. 11 DSGVO erfüllen.
2. Ob die Bezahlmöglichkeit – also zum Beispiel ein Monats-Abo – als eine gleichwertige Alternative zur Einwilligung in das Tracking zu betrachten ist, hängt davon ab, ob den Nutzer/innen gegen ein marktübliches Entgelt ein gleichwertiger Zugang zu derselben Leistung eröffnet wird. Ein gleichwertiger Zugang liegt in der Regel vor, wenn die Angebote zumindest dem Grunde nach die

gleiche Leistung umfassen. Eine absolute Identität der verschiedenen Angebote ist hierbei nicht erforderlich. Hinsichtlich der Kosten des Alternativangebots ist eine vom Dienst und Nutzerverhalten losgelöste Betrachtung nicht möglich. Die datenschutzrechtliche Überprüfung ist insoweit darauf beschränkt, ob die Preisgestaltung des Anbieters offensichtlich unverhältnismäßig und deshalb keine echte Alternative ist.

3. Nehmen Nutzer/innen das Angebot im Rahmen eines „trackingfreien" Abonnements wahr und erteilen keine zusätzliche Einwilligung, dürfen gemäß § 25 Abs. 1 Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) nur Speicher- und Auslesevorgänge erfolgen, die für den von den Nutzer/innen ausdrücklich gewünschten Telemediendienst unbedingt erforderlich sind. Nachfolgende Verarbeitungen personenbezogener Daten müssen auf die gesetzlichen Erlaubnistatbestände gemäß Art. 6 Abs. 1 Buchst. b, c und f DSGVO gestützt werden können. Diesbezüglich gelten die allgemeinen Ausführungen in der Orientierungshilfe der DSK für Anbieter/innen von Telemedien.
4. Die Wirksamkeit von Einwilligungen von Nichtabonnentinnen und -abonnenten ist bei den sogenannten „Pur"-Abo-Modellen sicherzustellen. Soweit mehrere Verarbeitungszwecke vorliegen, die wesentlich voneinander abweichen, müssen die Anforderungen der Granularität der Einwilligung umgesetzt werden. Dies bedeutet, dass die Nutzer/innen die Möglichkeit haben müssen, die einzelnen Zwecke, zu denen eine Einwilligung eingeholt werden soll, selbst und aktiv auswählen zu können (Opt-In). Nur wenn Zwecke in einem sehr engen Zusammenhang stehen, kann eine Bündelung von Zwecken in Betracht kommen. In allen Fällen, in denen gemessen an diesen Maßstäben nicht alle in Rede stehenden Verarbeitungszwecke unter dieselbe Einwilligung gebündelt werden können, sind die Anforderungen an eine wirksame Einwilligung durch Nichtabonnentinnen und -abonnenten

Was ist zu tun?
Verantwortliche für Websites müssen diese auf datenschutzrechtliche Aspekte prüfen. Insbesondere die Einbindung von Drittinhalten sowie das Verwenden von Cookies müssen auf den Prüfstand und dürfen nur mit tragfähigen Rechtsgrundlagen verwendet werden.

nicht gewahrt, sofern dem oder Nutzer/in lediglich ein pauschales Akzeptieren aller Verarbeitungszwecke ermöglicht wird.

5. Darüber hinaus müssen die Einwilligungen den sonstigen Anforderungen der DSGVO gerecht werden, insbesondere auch jenen an Transparenz, Verständlichkeit und Information der Betroffenen aus Art. 4 Nr. 11 und Art. 7 Abs. 2 DSGVO (vgl. hierzu die Orientierungshilfe Telemedien 2021, Version 1.1).

OH Telemedien 2021 (Version 1.1):
↗ sdb.de/tb2206

2.4 Sensible Daten, besondere Kategorien personenbezogener Daten

2.4.1 Übermittlung von Gesundheitsdaten an Inkassounternehmen

↗ Art. 4 Nr. 15 DSGVO, Art. 9 Abs. 2 Buchst. f DSGVO, Art. 9 Abs. 2 Buchst. h DSGVO

Mich erreichte die Anfrage, ob Gesundheitsdaten an Inkassounternehmen übermittelt werden dürfen. Hintergrund war, dass ein Patient eine ärztliche Behandlung nicht bzw. nicht fristgemäß bezahlt hatte. Zur Durchsetzung seiner Ansprüche auf Zahlung des ärztlichen Honorars hatte der Arzt ein Inkassounternehmen mit der Geltendmachung seiner Ansprüche gegenüber dem Patienten beauftragt. Der Patient wurde von dem Inkassounternehmen zur Zahlung des ärztlichen Honorars aufgefordert. Der Patient hatte sich deshalb an meine Behörde gewandt und gefragt, ob der Arzt berechtigt war, seine Daten an das Inkassounternehmen zu übermitteln, da dieses keinem Berufsgeheimnis bzw. keinen Geheimhaltungspflichten unterliegen würde.

Die Verarbeitung von personenbezogenen Daten bedarf grundsätzlich einer Rechtsgrundlage, vgl. Art. 5 Abs. 1 Buchst. a Datenschutz-Grundverordnung (DSGVO). Die Verarbeitung von Gesundheitsdaten im Sinne des Art. 4 Nr. 15 DSGVO ist grundsätzlich untersagt, soweit nicht ein Ausnah-

metatbestand nach Art. 9 Abs. 2 DSGVO gegeben ist. Mit der Verarbeitung von Gesundheitsdaten sind – im Verhältnis zu personenbezogenen Daten nach Art. 4 Nr. 1 DSGVO – weitere Voraussetzungen an eine rechtmäßige Datenverarbeitung verbunden.

Gesundheitsdaten im Sinne der DSGVO sind personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen; Art. 4 Nr. 15 DSGVO. Unerheblich ist, ob es sich um den früheren, gegenwärtigen oder künftigen körperlichen oder geistigen Gesundheitszustand der betroffenen Person handelt, vgl. Erwägungsgrund 35 der DSGVO. Auch Informationen, die sich mittelbar auf den Gesundheitszustand einer Person beziehen, können grundsätzlich unter den Begriff der Gesundheitsdaten im Sinne des Art. 4 Nr. 15 DSGVO fallen, wie zum Beispiel die Information über den Besuch bei einer Ärztin oder einem Arzt. Im vorliegenden Fall blieb unklar, welche konkreten Daten an das Inkassounternehmen übermittelt wurden, sodass eine Aussage, ob die Beurteilung der Rechtmäßigkeit der Datenverarbeitung nach Art. 9 Abs. 2 DSGVO oder Art. 6 DSGVO vorzunehmen ist, nicht getroffen werden konnte.

Dem Anfragenden habe ich daher nur mitteilen können, dass Art. 9 Abs. 2 Buchst. f DSGVO Rechtsgrundlage für die Datenverarbeitung sein könnte, soweit es sich um Gesundheitsdaten handeln sollte. Danach ist die Verarbeitung von Gesundheitsdaten ausnahmsweise zulässig, wenn dies zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder bei Handlungen der Gerichte im Rahmen ihrer justiziellen Tätigkeit erforderlich ist. Dazu zählt auch die außergerichtliche Geltendmachung von Ansprüchen; vgl. Erwägungsgrund 52 Satz 3 der DSGVO. Es gilt jedoch zu beachten, dass es sich bei der Geltendmachung von außergerichtlichen Ansprüchen um streitige Ansprüche handeln muss. In derartigen Fällen ist demzufolge eine datenschutzrechtliche Einwilligung nach Art. 9 Abs. 2 Buchst. a DSGVO nicht erforderlich.

Was ist zu tun?

Bei der Übermittlung von Gesundheitsdaten an Dritte ist Verantwortlichen, die Patientendaten zu verarbeiten haben, Sorgfalt anzuraten. Im Zweifel ist sogar eine Einwilligung für eine Datenweitergabe einzuholen, es sei denn, streitige Rechtsansprüche sollen durchgesetzt werden.

Ich habe darauf hingewiesen, dass für Art. 9 Abs. 2 Buchst. f DSGVO die Vorschrift des Art. 9 Abs. 3 DSGVO, wonach die Verarbeitung nur von Personen, die einer Geheimnispflicht unterliegen, durchgeführt werden darf, nicht greift. Ein Erfordernis mit der außergerichtlichen Geltendmachung von Zahlungsansprüchen nur Personen zu beauftragen, die einem Berufsgeheimnis oder einer Geheimhaltungspflicht unterliegen, ergibt sich für den Erlaubnistatbestand des Art. 9 Abs. 2 Buchst. f DSGVO gerade nicht.
Inwieweit eine vorherige Forderungsabtretung an das Inkassounternehmen ggf. eine andere datenschutzrechtliche Beurteilung zur Folge hätte, konnte in Ermangelung einer Konkretisierung des Sachverhalts durch die betroffene Person meinerseits nicht beurteilt werden.

2.4.2 Masernschutzgesetz: Einwilligung zur Übermittlung einer Kopie des Nachweises an das Gesundheitsamt

↗ DSGVO, IfSG

Nach dem Masernschutzgesetz besteht für Kinder, die in Gemeinschaftseinrichtungen, wie zum Beispiel Kindertagesstätten oder Schulen, betreut werden, und die dort Beschäftigten die Pflicht, gegenüber der Leitung der Einrichtung den Nachweis ihres ausreichenden Impfschutzes gegen Masern zu erbringen. Dies ergibt sich aus § 20 Abs. 8 bis 14 Infektionsschutzgesetz (IfSG).

Tätigkeitsbericht 2020:
↗ sdb.de/tb2020

Tätigkeitsbericht 2021:
↗ sdb.de/tb2021

Im Tätigkeitsbericht 2020 (2.2.9, Seite 589) hatte sich mein Amtsvorgänger bereits zum Masernschutzgesetz geäußert, in meinem Tätigkeitsbericht 2021 (2.4.4, Seite 92) griff ich das Thema aus Anlass zahlreicher Anfragen erneut auf. Die Anfragen betrafen das Anfertigen von Kopien der vorgelegten Nachweise, um diese bei der Einrichtung zu den Akten zu nehmen. Da § 20 Abs. 9 IfSG lediglich die Vorlage des Nachweises fordert, dürfen der Impfausweis oder auch ein ärztliches Zeugnis/Attest aus datenschutzrechtlichen Gründen nicht kopiert werden.

Eine mir im Berichtsraum vorliegende Anfrage betraf die Vorgehensweise der Leitung einer kommunalen Einrichtung bei der Übermittlung von personenbezogenen Daten an das zuständige Gesundheitsamt.

Wenn der Nachweis nicht vorgelegt wird oder wenn Zweifel an der Echtheit oder inhaltlichen Richtigkeit des vorgelegten Nachweises bestehen, hat die Leitung der jeweiligen Einrichtung unverzüglich dem zuständigen Gesundheitsamt nach § 20 Abs. 9 Satz 2 IfSG personenbezogene Angaben zu übermitteln. Es handelt sich dabei um die in § 2 Nr. 16 IfSG genannten personenbezogenen Angaben (Name und Vorname, Geschlecht, Geburtsdatum, Anschrift der Hauptwohnung oder des gewöhnlichen Aufenthaltsortes der betroffenen Person und, falls abweichend, Anschrift des derzeitigen Aufenthaltsortes der betroffenen Person sowie, soweit vorliegend, Telefonnummer und E-Mail-Adresse). Die weiteren Fälle, in denen dem Gesundheitsamt personenbezogene Angaben zu übermitteln sind, werden in § 20 Abs. 9a, 10 und 11 IfSG geregelt.

Die Übermittlung einer Kopie des vorgelegten Nachweises an das zuständige Gesundheitsamt ist damit nach § 20 Abs. 9 Satz 2 IfSG nicht zulässig. Dies gilt auch, wenn ein Fall des § 20 Abs. 9a, 10 oder 11 IfSG vorliegt.

Im Zuge der Prüfung der Anfrage hatte mir der Träger der kommunalen Kindertagesstätte mitgeteilt, dass er bei einer Meldung an das Gesundheitsamt des Landkreises bzw. der Kreisfreien Stadt gemäß § 20 Abs. 9 Satz 2 IfSG neben den personenbezogenen Angaben nach § 2 Nr. 16 IfSG gegebenenfalls auch eine Kopie des Nachweises an das Gesundheitsamt weiterleitet, wenn die Eltern dem zugestimmt haben. Meine Nachfrage ergab, dass sich der Träger dazu eine schriftliche Einwilligung zur Weiterleitung einer Kopie des von den Eltern vorgelegten Nachweises an das Gesundheitsamt erteilen lässt.

Es muss hier eine ausdrückliche Einwilligung der beiden Erziehungsberechtigten gemäß Art. 6 Abs. 1 Buchst. a und Art. 9 Abs. 2 Buchst. a DSGVO vorliegen, da es sich um personenbezogene Daten gemäß Art. 4 Nr. 1 DSGVO und um Gesund-

heitsdaten im Sinne des Art. 9 Abs. 1 DSGVO handelt. Dabei ist zu beachten, dass die Einwilligung nach Art. 7 DSGVO freiwillig zu erteilen ist. Dies ist zum Beispiel der Fall, wenn die Eltern dem Träger der Einrichtung eine Kopie des Nachweises überlassen, damit dieser den Nachweis an das Gesundheitsamt weiterleitet. Die Einwilligung ist schriftlich zu erteilen, damit der Träger nachweisen kann, dass eine wirksame Einwilligung vorliegt.

Da der Träger das Erfordernis der Einwilligung nach Art. 7 DSGVO beachtet, ist seine Vorgehensweise datenschutzrechtlich zulässig.

Zusammenfassend stelle ich fest: Nur wenn der Leitung der Einrichtung eine ausdrückliche Einwilligung des Betroffenen vorliegt, ist das Übersenden einer Kopie des Nachweises an das Gesundheitsamt datenschutzrechtlich zulässig.

Was ist zu tun?

Die Übermittlung einer Kopie des Nachweises an das Gesundheitsamt ist nur mit der ausdrücklichen Einwilligung des Betroffenen zulässig.

3 Betroffenenrechte

3.1 Spezifische Pflichten des Verantwortlichen

3.1.1 Öffentliche Zustellung und Veröffentlichung von Bescheiden in Volltext im elektronischen Amtsblatt

↗ § 10 VwZG in Verbindung mit § 4 Abs. 1 SächsVwVfZG, Art. 7 Abs. 1 DSGVO

Im Berichtszeitraum wandte sich ein Petent an mich, der monierte, dass eine sächsische Gemeinde im Rahmen einer öffentlichen Zustellung die an den Petenten zuzustellenden Bescheide nicht nur bekannt gegeben hat, sondern auch in ihrem vollen Wortlaut im gemeindlichen elektronischen Amtsblatt veröffentlichte.

Nach § 10 Abs. 1 Verwaltungszustellungsgesetz (VwZG) in Verbindung mit § 4 Abs. 1 Verwaltungsverfahrensgesetz für den Freistaat Sachsen (SächsVwVfZG) kann eine Zustellung von Verwaltungsakten durch öffentliche Bekanntmachung erfolgen, wenn der Aufenthaltsort des Empfängers unbekannt ist und eine Zustellung an einen Vertreter oder Zustellungsbevollmächtigten nicht möglich ist.

In dem vorliegenden Fall waren – nach Darstellung der Gemeinde – sämtliche Empfangseinrichtungen des Adressaten abmontiert und eine Ersatzzustellung an Bevollmächtigte nicht möglich. So konnten mehrere Bescheide zu Kosten- und Zwangsgeldfestsetzung nicht zugestellt werden. Eine recht- und ordnungsgemäße Zustellung ist indes gesetzliche Voraussetzung für die Vollstreckung von Verwaltungsakten.

So hatte man sich des Instruments der öffentlichen Zustellung durch Bekanntmachung bedient. Nach § 10 Abs. 2 Satz 1 VwZG in Verbindung mit § 4 Abs. 1 SächsVwVfZG erfolgt dies durch Bekanntmachung einer Benachrichtigung an der Stelle, die von der Behörde hierfür allgemein bestimmt ist, oder durch Veröffentlichung einer Benachrichtigung im Bundesanzeiger (bzw. Gemeindlichen Amtsblatt).

Die hier betroffene Gemeinde hat festgelegt, dass amtliche Veröffentlichungen ausschließlich in einer über die gemeindliche Homepage abrufbaren elektronischen Version des Amtsblattes (mit Suchmaske) abrufbar sein sollen. Gemeinden können die Art und Weise der amtlichen Mitteilungen und Verkündungen im Rahmen der Selbstverwaltung über sogenannte Bekanntmachungsverordnungen weitgehend selbst bestimmen. Soweit ist dies datenschutzrechtlich nicht zu beanstanden.

Allerdings sind im Rahmen der öffentlichen Zustellung seit der Reform des Verwaltungsvollstreckungsrechtes 2010 in jedem Fall nur noch eine Bekanntmachung über das Vorliegen eines Bescheides zu veröffentlichen. Nach § 10 Abs. 2 Satz 2 VwZG in Verbindung mit § 4 Abs. 1 SächsVwVfZG muss die Benachrichtigung die Behörde, für die zugestellt wird, den Namen und die letzte bekannte Anschrift des Zustellungsadressaten, das Datum und das Aktenzeichen des Dokuments sowie die Stelle, wo das Dokument eingesehen werden kann, enthalten.

Auch schon vor der Reform war im Übrigen die damalige Vorschrift eine Soll-Vorschrift, die es der Verwaltung erlaubte, nur in einem begründeten Ausnahmefall und nur nach gründlicher Abwägung die Bescheide in Volltext zu veröffentlichen. Ein solcher lag in diesem Fall nicht vor und wurde von der Gemeinde auch nicht beansprucht. Ich habe die Gemeinde aufgefordert, die entsprechenden Einträge und Veröffentlichungen im elektronischen Amtsblatt zu löschen. Die gesetzliche Pflicht zur Löschung von – wie vorliegend – rechtsgrundlos veröffentlichten Daten findet sich unmittelbar in Art. 17 Abs. 1 Datenschutz-Grundverordnung (DSGVO), die auf Bundes- und Landesebene direkte Anwendung findet. Dem steht auch nicht das Sächsische E-Government-Gesetz (SächsEGovG)

entgegen. Löschungspflichten wurden durch eine Novelle 2019 in diesem Gesetz nur deswegen gestrichen, weil diese lediglich Wiederholungen der in der DSGVO normierten Pflichten darstellten.
Die Löschung der Bekanntmachung einer öffentlichen Zustellung im elektronischen Amtsblatt ist nach Zweckerreichung zu veranlassen. Nach § 10 Abs. 2 VwZG tritt die Fiktion der Zustellung zwei Wochen nach Veröffentlichung ein, sodass zu diesem Zeitpunkt auch der Zweck erreicht wird. Zur Praktikabilität kann auf die Zweiwochenfrist ein Karenzaufschlag von zwei bis maximal vier weiteren Wochen hinzukommen, um den gemeindlichen Verwaltungsaufwand zu bündeln. So können beispielsweise einmal im Monat die abgelaufenen öffentlichen Zustellungen aus dem elektronischen Amtsblatt gelöscht werden. Nach meinem Dafürhalten ist dies datenschutzrechtlich vertretbar und berücksichtigt den Ausgleich zwischen datenschutzrechtlichen Löschungspflichten und angemessenem Verwaltungsaufwand.

3.2 Auskunftsrecht

3.2.1 Anforderung einer beglaubigten Ablichtung eines Ausweisdokuments bei Auskunftsersuchen

↗ § 59 BDSG

Im Berichtszeitraum erreichte mich die Eingabe eines Petenten, der vortrug, dass eine Staatsanwaltschaft, die er um Auskunft über seine Daten nach § 491 Abs. 2 Strafprozessordnung (StPO) in Verbindung mit § 57 Bundesdatenschutzgesetz (BDSG) gebeten habe, eine beglaubigte Ablichtung seines Personalausweises oder anderen Ausweisdokumentes angefordert hatte, um sicherzustellen, dass Auskünfte nicht an eine unberechtigte Person erteilt würden. Die von mir um Stellungnahme gebetene Staatsanwaltschaft bestätigte diese Darstellung und verwies auf eine Rundverfügung des Generalstaatsanwalts des Freistaates Sachsen vom Januar 2020, die unter anderem die Anforderung eines Legitimationsnachweises bei Auskunftserteilung bestimmte:

„Die besondere Sensibilität der in den Staatsanwaltschaften verarbeiteten Daten erfordert einen ausreichenden Legitimationsnachweis des Antragstellers. Ausweislich der Gesetzesbegründung zu § 59 Abs. 5 BDSG steht diese Vorschrift dem nicht entgegen. In der Regel setzt daher die Erteilung von Auskünften einen schriftlichen Antrag und die Vorlage einer beglaubigten Ablichtung eines amtlichen Personaldokuments durch den Antragsteller voraus."

Jede Verarbeitung personenbezogener Daten muss auf rechtmäßige Weise, nach dem Grundsatz von Treu und Glauben und in einer für die betroffenen natürlichen Personen nachvollziehbaren Weise erfolgen. Die Daten dürfen nur für bestimmte, durch Rechtsvorschriften geregelte Zwecke verarbeitet werden. Die Anforderung einer beglaubigten Ablichtung eines amtlichen Ausweisdokuments stellt zweifelsfrei eine Verarbeitung personenbezogener Daten dar und bedarf einer Rechtsgrundlage. Die hier einschlägige gesetzliche Ermächtigungsgrundlage für die Anforderung eines Identitätsnachweises ist § 59 Abs. 4 BDSG, wonach der Verantwortliche die Möglichkeit erhält, bei begründeten Zweifeln an der Identität des Antragstellers zusätzliche Informationen anzufordern, die zur Bestätigung der Identität der betroffenen Person erforderlich sind. Ohne besonderen Anlass für Zweifel darf die auskunftspflichtige Behörde damit allerdings keinen Identitätsnachweis von einem Antragsteller verlangen. In der – hier nicht zur Anwendung kommenden – Datenschutz-Grundverordnung ist dies entsprechend in Art. 12 Abs. 6 geregelt.

Die in der oben genannten Rundverfügung der Generalstaatsanwaltschaft angesprochene gesetzgeberische Intention, dass § 59 Abs. 4 BDSG die bisherige Praxis, „den Nachweis der Identität auch weiterhin als Grundvoraussetzung für die Antragstellung anzusehen", nicht ändern soll, ist nicht mit dem Gesetzeswortlaut vereinbar. § 59 Abs. 4 BDSG ermöglicht keine routinemäßige Identitätsprüfung.

So entschied jüngst das Verwaltungsgericht Berlin, dass der Beklagte (Amtsgericht Tiergarten) vom Antragsteller keinen

Identitätsnachweis einfordern dürfe, da die Anschrift des Antragstellers dem Gericht schon seit Längerem bekannt war. Außerdem fehle jeder Anhaltspunkt dafür, dass ein Dritter Interesse an der begehrten Auskunft haben könnte und deshalb unter Benutzung einer falschen Identität die Auskunft erschleichen könnte. Schließlich sei zu beachten, dass der Beklagte durch eine förmliche Zustellung seines Auskunftsschreibens dessen Fehlleitung unterbinden könne (Verwaltungsgericht Berlin, Urteil vom 31.08.2020 – 1 K 90.19).

Verbleiben begründete Zweifel an der Identität des Antragstellers, muss der Verantwortliche bei der Festlegung der Art und Weise der Identitätsfeststellung verhältnismäßig vorgehen. Das Auskunftsrecht ist neben der Informations- und Benachrichtigungspflicht das zentrale Betroffenenrecht, welches jeder natürlichen Person voraussetzungslos zusteht. Seine herausgehobene Stellung zeigt sich auch darin, dass der Verantwortliche die Auskunft grundsätzlich unentgeltlich zu erteilen hat, § 59 Abs. 3 BDSG. Die Anforderung einer beglaubigten Ablichtung eines amtlichen Ausweisdokuments ist mit dem Grundsatz der Unentgeltlichkeit nicht vereinbar. Zwar verlangt die Staatsanwaltschaft für die Auskunftserteilung keine Verwaltungsgebühr, gleichwohl wird für die Antragsbearbeitung eine beglaubigte Abschrift eines amtlichen Ausweisdokuments vorausgesetzt, was für den Betroffenen – neben dem Aufwand, sich eine solche Ablichtung zu beschaffen – Kosten verursacht und so zu einer nicht mehr vertretbaren Hürde zur Ausübung des Betroffenenrechts führt.

Das Anfordern einer einfachen Kopie des Personalausweises hingegen ist verhältnismäßig und unter Beachtung gewisser Rahmenbedingungen datenschutzrechtlich vertretbar. So ist gemäß § 20 Abs. 2 Satz 3 Personalausweisgesetz (PAuswG) eine datenschutzrechtliche Einwilligung der betroffenen Person zur Erhebung und Verarbeitung personenbezogener Daten aus dem Personalausweis erforderlich. Dementsprechend ist der Betroffene bei der Bitte um Zusendung einer Kopie seines Personalausweises um eine Einwilligung zu ersuchen, die insbesondere kurz erläutert, dass ohne Iden-

tifizierung keine Auskunft nach § 57 BDSG erfolgen kann, dass die Berechtigung zur Identifizierung aus § 59 Abs. 4 BDSG folgt und worin der Zweck der Anforderung der Kopie besteht. Bei der Anforderung der Personalausweiskopie ist dem Betroffenen ebenso mitzuteilen, dass solche Angaben auf der Kopie geschwärzt werden können, die für die Identitätsfeststellung nicht erforderlich sind (Grundsatz der Datenminimierung). In der Regel sind Vorname, Name, Anschrift, gegebenenfalls zur Vermeidung von Verwechslungen bei möglicher Namensgleichheit auch Geburtsdatum und -ort, nicht aber Lichtbild, Augenfarbe, Größe, Serien- oder Zugangsnummer des Ausweises erforderlich. Die Kopie muss gemäß § 20 Abs. 2 Satz 1 PAuswG als solche gekennzeichnet sein und unterliegt einer strengen Zweckbindung, das heißt, sie darf nur zur Identifizierung im Rahmen der Auskunftserteilung verwendet werden. Danach ist sie unwiederbringlich zu vernichten oder dem Betroffenen zurückzugeben. Vorstehendes kann sinngemäß auf die Kopie des Reisepasses übertragen werden.

Was ist zu beachten?
Im Rahmen einer Auskunftserteilung ist die Anforderung einer beglaubigten Ablichtung eines amtlichen Ausweisdokuments der Antragstellerin bzw. des Antragstellers unverhältnismäßig.

Ich bat die Generalstaatsanwaltschaft daher, die oben zitierte Passage der Rundverfügung des Generalstaatsanwalts des Freistaates Sachsen vom Januar 2020 zeitnah unter Berücksichtigung meiner Anregungen abzuändern. Dem ist die Generalstaatsanwaltschaft unverzüglich nachgekommen.

3.2.2 Auskunft zu Zugriffsmöglichkeiten aus Ratsinformationssystemen

↗ § 4 Abs. 1 Nr. 3 SächsDSDG, § 203 Abs. 2 und § 22 Abs. 1 und 4 SächsDSDG, § 28 Abs. 4 SächsGemO, Art. 15 Abs. 1 Buchst. c DSGVO

Der Datenschutzbeauftragte einer sächsischen Gemeinde wandte sich mit dem folgenden Sachverhalt an mich: Der Stadtrat hatte über eine vertrauliche Personalangelegenheit gemäß § 28 Abs. 4 SächsGemO zu befinden. Nach dieser Vorschrift muss der Gemeinderat im Einvernehmen mit dem Bürgermeister über diverse grundsätzliche Belange betreffend Gemeindebediensteter entscheiden, wie Ernennung, Einstellung, Entlassung und anderes.

In diesem Zusammenhang wurde eine vertrauliche Vorlage mit Personalbezug in das Ratsinformationssystem der Gemeinde eingestellt. Da die Angelegenheit allem Anschein nach auch von gewissem Lokalinteresse war, musste die Gemeinde alsbald feststellen, dass die Presse berichtete und auch auf Dokumente aus eben dieser Vorlage zitierte. Da die Vorlage nicht öffentlich zugänglich war, lag es sehr nahe, dass jemand aus dem Kreis der Zugriffsberechtigten diese Dokumente an die Presse weitergeleitetet hatte. Die Meldung einer Datenschutzpanne nach Art. 33 Datenschutz-Grundverordnung (DSGVO) wurde durch die Gemeinde auch entsprechend der gesetzlichen Vorgaben veranlasst.

Nun hat aber der oder die Betroffene, um deren Personalangelegenheit es bei der Vorlage ging, einen Auskunftsanspruch über die eigenen, bei der Gemeinde und ihrem Stadtrat verarbeiteten Daten gemäß Art. 15 DSGVO gestellt und wollte hierzu auch alle Personen benannt wissen, die ein Zugriffsrecht bzw. eine Zugriffsmöglichkeit auf die Vorlage im Ratsinformationssystem hatten. Gesetzlich normiert ist, dass der betroffenen Person im Rahmen der Auskunft nach Art. 15 DSGVO auch ein Anspruch auf Information über die Empfänger oder Kategorien von Empfängern zusteht, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden sollen, Art. 15 Abs. 1 Buchst. c DSGVO.

So bezog sich die an mich gerichtete Frage des Datenschutzbeauftragten der Gemeinde darauf, ob im Rahmen einer solchen Auskunft auch potenzielle Empfänger personenbezogener Daten zu benennen sind; sprich diejenigen, die zwar ein Zugriffsrecht auf die entsprechenden Dokumente hatten, es aber nicht bekannt ist, ob tatsächlich ihrerseits Zugriffe stattgefunden haben.

In meiner Stellungnahme an den Datenschutzbeauftragten konnte ich die Frage verneinen. Das Auskunftsrecht beschränkt sich auf die konkreten Empfänger von personenbezogenen Daten, umfasst jedoch nicht die potenziellen Empfänger bzw. Zugriffsrechte. Eine bloße Möglichkeit des Datenempfangs reicht nicht aus. Im Rahmen eines Auskunfts-

ersuchens nach Art. 15 DSGVO sind somit als Empfänger nach Art. 15 Abs. 1 Buchst. c DSGVO nur Stellen zu benennen, die die personenbezogenen Daten (in diesem Fall die fragliche Vorlage) auch tatsächlich erhalten haben.

Ich habe der Gemeinde indes dringend geraten, den Vorfall der zuständigen Staatsanwaltschaft anzuzeigen. Denn das unbefugte Offenbaren von Personalangelegenheiten durch Gemeinderätinnen und -räte oder Gemeindebedienstete an die Presse und andere Stellen kann eine Straftat nach § 203 Abs. 2 Strafgesetzbuch (StGB) und § 22 Abs. 4 Sächsisches Datenschutzdurchführungsgesetz (SächsDSDG) darstellen. Nach § 203 Abs. 2 StGB wird bestraft, wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis, offenbart, das ihm als Amtsträger anvertraut worden oder sonst bekannt geworden ist. Nach § 22 Abs. 4 SächsDSDG wird bestraft, wer eine Ordnungswidrigkeit nach § 22 Abs. 1 SächsDSDG, hier die unbefugte Übermittlung von Personalinformationen an die Presse, in der Absicht begeht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, wobei die Schädigung auch ideeller Art sein kann. Kurz gesagt: Wer Personalinformationen unbefugt an die Presse oder Dritte weiterleitet, um den betroffenen Personen oder der Stadt als Arbeitgeber etwa „eins auszuwischen", macht sich strafbar. Die Datenverarbeitung durch die Staatsanwaltschaft der zum einen im Ratsinformationssystem und zweitens im Server protokollierten Zugriffe wäre zweckändernd nach § 4 Abs. 1 Nr. 3 SächsDSDG ohne Weiteres möglich.

Theoretisch könnte auch die Gemeinde selbst – in ihrer Funktion als Ordnungsbehörde – eine Ordnungswidrigkeit, vorliegend die unbefugte Offenbarung von Personalinformationen nach § 22 Abs. 1 SächsDSDG selbst ermitteln und hierzu auch selbst zweckändernd Daten verarbeiten. Ich vertrete indes die Ansicht, Fälle, in denen eine Straftat (und nicht bloße Ordnungswidrigkeit) im Raum steht, stets bei der Staatsanwaltschaft anzuzeigen und nicht eigenhändig durch die Behörde zu ermitteln.

Was ist zu tun?

Die Vergabe von Zugriffsrechten in Informationssystemen sollte exakt geprüft und Zugriffe sollten zur Abschreckung von Missbräuchen und einer etwaigen Strafverfolgung protokoliert werden.

3.2.3 Erfüllung des Auskunftsanspruchs unter Beachtung des Schutzes von Rechten und Freiheiten Dritter

↗ § 630a und f BGB, Art. 15 Abs. 3 DSGVO, Art. 15 Abs. 4 DSGVO

Gegenstand häufiger Anfragen ist die Auskunftserteilung nach Art. 15 Abs. 1 Datenschutz-Grundverordnung (DSGVO) sowie die Erteilung einer Kopie nach Art. 15 Abs. 3 DSGVO von Patientenakten.

Im letzten Berichtszeitraum wurde ich um Stellungnahme gebeten, inwieweit es sich bei den Namen von Beschäftigten um überwiegende Rechte und Freiheiten anderer Personen im Sinne des Art. 15 Abs. 4 DSGVO handelt. Hintergrund war, dass im Rahmen der Beauskunftung, in Form der Erteilung einer Kopie einer Patientenakte, die Handzeichen und Namen von Beschäftigten des Krankenhauses geschwärzt wurden. Das Krankenhaus berief sich darauf, dass die Erteilung einer Kopie nicht die Rechte und Freiheiten Dritter, wozu die Beschäftigten des Krankenhauses zählten, beeinträchtigt werden dürften.

Ich habe dazu mitgeteilt, dass die Auskunftsrechte betroffener Personen, insbesondere das Recht auf Bereitstellung einer Kopie nach Art. 15 Abs. 3 DSGVO, nach Auffassung meiner Behörde verletzt sind, soweit der Verantwortliche Handzeichen und Namen Beschäftigter in Behandlungsunterlagen schwärzt, sich pauschal auf die Rechte und Freiheiten anderer Personen gemäß Art. 15 Abs. 4 DSGVO beruft und so die Kopie der Dokumentation der Behandlung verändert oder teilweise unkenntlich macht.

Die Beschränkung des Rechts auf Erhalt einer Kopie nach Art. 15 Abs. 4 DSGVO setzt die Beeinträchtigung von Rechten und Freiheiten „anderer Personen" voraus. Dabei ist zu berücksichtigen, dass nur unter den erschwerten Bedingungen des Art. 23 DSGVO eine Beschränkung des Art. 15 Abs. 4 DSGVO möglich ist. Im Hinblick auf die Auslegung des Art. 15 Abs. 4 DSGVO, insbesondere in Bezug auf die Rechte und Freiheiten anderer Personen, die gegebenenfalls zu einer Einschränkung des Rechts auf Erteilung einer Kopie nach Art. 15

Abs. 3 DSGVO führen können, ist eine pauschale Schwärzung von Handzeichen und Namen nicht mit der DSGVO vereinbar. Nach Auffassung meiner Behörde handelt es sich bei den Handzeichen und Namen von Beschäftigten, die an der Behandlung des Patienten mitwirken, schon nicht um „andere Personen" im Sinne des Art. 15 Abs. 4 DSGVO.

Der Verantwortliche (Krankenhaus) setzt im Rahmen der geschuldeten Behandlungsleistungen nach § 630a Bürgerliches Gesetzbuch (BGB) Beschäftigte zur Erfüllung dieser Leistungen ein. Zum geschuldeten Leistungsumfang zählt insbesondere auch die Behandlungsdokumentation nach § 630f BGB. Soweit die Identität der Beschäftigten durch Auskunftsersuchen im Kontext mit einem Behandlungsvertrag, insbesondere der Behandlungsdokumentation, offenbart wird, sind diese jedoch nicht in ihrer persönlichen Sphäre bzw. nicht zur Selbstverwirklichung ihres Persönlichkeitsrechts betroffen, sondern in Bezug auf ihre Funktionsausübung im Rahmen ihrer dienstlichen Tätigkeit, respektive als Erfüllungsgehilfe des zwischen Klinikum und Patienten (Betroffenem) geschlossenen Behandlungsvertrages.

Der allgemeine Einwand, dass es sich um besonders sensible Beschäftigtendaten handele und dem Arbeitgeber (Krankenhaus) eine Fürsorgepflicht gegenüber seinen Beschäftigten obliege, die eine Offenbarung der Identität der Beschäftigten, die in den Behandlungsunterlagen genannt sind, entgegenstehe und damit eine Schwärzung von Handzeichen und Namen erfordere, führt im Kontext eines Behandlungsvertrages und entsprechender Behandlungsdokumentation entsprechend den vorherigen Ausführungen nicht zu einer Beschränkung des Rechts auf Erteilung einer Kopie nach Art. 15 Abs. 4 DSGVO.

Regelmäßig ist bei Beschäftigtendaten auch ein unvermeidbarer Doppelbezug gegeben, was den Erfüllungsgehilfen des Verantwortlichen und dessen Handlungen und die als Patienten und (datenschutzrechtlich) selbstbetroffene Person, die behandelt wird, angeht. Allerdings werden die Daten gerade nicht zum Zwecke des Beschäftigungsverhältnisses verarbeitet, sondern um den gesetzlichen Verpflichtungen

zur Behandlungsdokumentation nach § 630f BGB nachzukommen.
Selbst bei der Annahme, dass es sich bei den Handzeichen und Namen von Beschäftigten, die an der Behandlung des Patienten mitwirken, um andere Personen im Sinne des Art. 15 Abs. 4 DSGVO handeln würde, wären diese im Rahmen des zuvor beschriebenen Behandlungskontextes lediglich in ihrer Sozialsphäre betroffen, sodass eine auskunftsbeschränkende Beeinträchtigung im Sinne des Art. 15 Abs. 4 DSGVO gerade nicht vorliegt.
Im Übrigen habe ich mitgeteilt, dass der pauschale Hinweis auf die Beeinträchtigung von Rechten und Freiheiten der Beschäftigten den Anforderungen des Art. 15 Abs. 4 DSGVO nicht genügt. Vielmehr muss eine konkrete Beeinträchtigung drohen. Des Weiteren ist der Verantwortliche verpflichtet abzuwägen, inwieweit er gegebenenfalls durch eine Teilauskunft die Rechte der Betroffenen erfüllen kann.

Was ist zu beachten?
Erfüllungsgehilfen des Verantwortlichen sind regelmäßig nicht im Sinne des Art. 15 Abs. 4 DSGVO zu berücksichtigende „andere Personen".

3.2.4 Exzessiver Auskunftsanspruch

↗ Art. 12 Abs. 5 DSGVO, Art. 15 DSGVO

Eine Kommune fragte mich an, ob folgender Sachverhalt eine offensichtlich unbegründete Geltendmachung des Auskunftsrechtes nach Art. 15 Datenschutz-Grundverordnung (DSGVO) gemäß Art. 12 Abs. 5 DSGVO darstelle, welche dazu berechtigen würde, dem Antrag nicht nachzukommen (Art. 12 Abs. 5 Buchst. b DSGVO) oder ein Entgelt für die Bearbeitung gemäß Art. 12 Abs. 5 Buchst. a DSGVO zu fordern.
Einer ihrer Bürger stellte im Oktober 2019 ein Auskunftsersuchen, welches vollständig beantwortet wurde. Im September 2021 stellte derselbe Betroffene ein Löschungsersuchen, welches auf Nachfrage von ihm präzisiert wurde und dann durch Löschung der E-Mail-Adresse ebenfalls erfüllt wurde.
Mit Schreiben vom Februar 2022 ersuchte er erneut um Auskunft. In dem Antragsschreiben findet sich der Satz: „Meine Anfrage schließt expliziert auch sämtliche weiteren Angebote und Unternehmen ein, für die Sie Verantwortlicher im

Sinne des Art. 4 Nr. 7 DSGVO sind." Dies erschien der Kommune zu weitgehend.

Ich teilte der anfragenden Kommune mit, dass vorliegend die Voraussetzungen des Art. 12 Abs. 5 Satz 2 DSGVO nicht erfüllt sind. Weder ist die Anfrage wegen zu häufiger Wiederholung oder wegen Rechtsmissbrauchs exzessiv, noch ist sie offensichtlich unbegründet.

Durch Art. 12 Abs. 5 Satz 2 DSGVO wird gewährleistet, dass der Unentgeltlichkeitsgrundsatz nicht in Missbrauchsfällen gilt. Zwar hat der Antragsteller zuvor einen Auskunftsantrag im Oktober 2019 und einen Löschungsantrag im September 2021 gestellt, aber eine exzessive Ausübung des Auskunftsrechts ist darin noch nicht zu erblicken.

In Anlehnung an die Frist des Art. 78 Abs. 2 DSGVO für eine Untätigkeitsklage ist eine Anfrage pro Quartal nicht exzessiv, da sich die bei einer Kommune erfassten personenbezogenen Daten eines Bürgers innerhalb weniger Wochen ändern können.

Der Satz „Meine Anfrage schließt explizit auch sämtliche weiteren Angebote und Unternehmen ein, für die Sie Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO sind" weist so noch nicht darauf hin, dass der Betroffene den Antrag aus schikanösen Gründen stellte. Ein Exzess kann jedoch dann vorliegen, wenn das Informationsverlangen sich offensichtlich von dem Regelungszweck des Auskunftsanspruchs entfernt hat.

In der Rechtsprechung wird Rechtsmissbrauch angenommen, wenn ein anderer Zweck als die Information über personenbezogene Daten dem Ersuchen zugrunde liegt, zum Beispiel, wenn der Auskunftsanspruch der Überprüfung etwaiger Prämienanpassungen von Versicherungen wegen möglicher formeller Mängel nach § 203 Abs. 5 Versicherungsvertragsgesetz dienen soll (vgl. Oberlandesgericht Hamm, B. vom 15.11.2021 – 20 U 269/21, ZD 2022, 237 Rdnr. 11). Auch ein Auskunftsverlangen im Zusammenhang mit einem Zahlungsbegehren in Höhe von über 110.000 Euro, welches erst rechtshängig gemacht wurde, nachdem der Verantwortliche seinen Vorstellungen nicht entsprochen und er auf den er-

heblichen aus der Beauskunftung resultierenden Arbeitsaufwand hingewiesen hatte, war deshalb exzessiv (Landesarbeitsgericht Sachsen, Urteil vom 17.2.2021 – 2 Sa 63/20, ZD 2022, 171 Rdnr. 66, 67).

Nach anderer Auffassung darf die bzw. der Betroffene mit seinem Ersuchen auch „datenschutzfremde Zwecke" verfolgen, da der Schutzzweck der DSGVO umfassend ist (Kühling/Buchner/Bäcker, 3. A. 2020, DSGVO Art. 15 Rdnr. 42d). Letzterem ist zuzustimmen, da auf diese Weise auch eine Ausforschung der Antragstellerinnen und Antragsteller über die Motive der Geltendmachung ihrer Rechte verhindert wird.

Die Anfrage ist auch nicht von vornherein offensichtlich unbegründet. Offensichtlich unbegründet ist ein Antrag nur dann, wenn die Antragstellung von jeder bzw. jedem Einsichtigen als völlig aussichtslos angesehen werden muss. Beispiele sind, dass ein unberechtigter Dritter Rechte der betroffenen Person geltend macht oder dass eine betroffene Person die Löschung ihrer Daten von einem Verantwortlichen verlangt, der ihm bereits mitgeteilt und nachgewiesen hat, dass er keine Daten von ihr verarbeitet. In einer unklaren Formulierung des Anliegens liegt noch kein offensichtlich unbegründeter Antrag vor, sondern der Verantwortliche hat sich bei der bzw. dem Betroffenen nach dem Inhalt seines Antrages zu erkundigen, da er gemäß Art. 12 Abs. 2 Satz 1 DSGVO die Pflicht hat, der betroffenen Person die Ausübung ihrer Rechte zu erleichtern.

Die Auskunft konnte deshalb nicht gemäß Art. 12 Abs. 5 Satz 2 DSGVO verweigert werden.

4 Pflichten Verantwortlicher und Auftragsverarbeiter

4.1 Verantwortung für die Verarbeitung, Technikgestaltung

4.1.1 Was ist bei der Gestaltung von Websites und Apps zu beachten?

↗ DSGVO, TTDSG

Mich erreichen viele Beschwerden von Betroffenen über Apps und Websites. Auch Verantwortliche sind immer noch verunsichert, welche Verarbeitungen erlaubt sind oder wann Einwilligungen für Cookies eingeholt werden müssen. Die Aufsichtsbehörden haben mit der Orientierungshilfe Telemedien 2021 (in überarbeiteter Version nach Anhörung von Verbänden in Version 1.1) umfangreiche Hilfestellungen für Verantwortliche veröffentlicht. Dieser Beitrag soll in verkürzter Form die wesentlichen Fragestellungen in diesem Zusammenhang behandeln und transparent machen, worauf ich bei Prüfungen und Beschwerden konkret achtet.

OH Telemedien 2021 (Version 1.1):
↗ sdb.de/tb2206

1. TTDSG-relevante Speicherungen

Seit Dezember 2021 ist das Gesetz zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien (TTDSG) in Kraft. Damit wurde die ePrivacy-Richtlinie der EU aus dem Jahr 2002 in deutsches Recht umgesetzt. § 25 TTDSG fordert eine klare und umfassend informierte Einwilligung für die „Speicherung von Informationen in der Endeinrichtung des Endnutzers oder [den] Zugriff auf Informationen, die bereits in der Endeinrichtung gespeichert sind". Ausnahmen bestehen

dann „wenn die Speicherung von Informationen in der Endeinrichtung des Endnutzers oder der Zugriff auf bereits in der Endeinrichtung des Endnutzers gespeicherte Informationen unbedingt erforderlich ist, damit der Anbieter eines Telemediendienstes einen vom Nutzer ausdrücklich gewünschten Telemediendienst zur Verfügung stellen kann". Was bedeutet das in der Praxis?

Zunächst einmal, dass jedes Cookie, jedes Objekt im Local-Storage eines Browsers oder jede Geräte-ID bei der Nutzung einer App vom Gesetz umfasst ist und einer Betrachtung bedarf (nachfolgend wird der Einfachheit halber immer von Cookies gesprochen, davon umfasst sind aber auch die genannten anderen Objekte und Speicherungen). Und dass grundsätzlich eine Einwilligung erforderlich ist, welche vor einer Speicherung oder einem Zugriff ausreichend über das Ansinnen des Betreibers informiert. Und dass eine solche Einwilligung auch verweigert werden kann.

In der täglichen Prüfung von Beschwerden wird es dann oftmals unübersichtlich, da viele Websites trotz der Gesetzeslage entweder eine Vielzahl von Cookies direkt beim Aufruf der Website setzen oder nach einer nicht den Anforderungen entsprechenden „Einwilligung" ohne Auswahlmöglichkeit noch einmal eine ganze Reihe weiterer Cookies speichern und im Verlauf der Nutzung der Website oder App auch auslesen. Die Verbraucher/innen sind von der Vielzahl von Bannern und Hinweisen oftmals nur noch genervt, eine echte Wahlfreiheit im Sinne einer informierten Entscheidung findet bei realistischem Blick auf das tägliche Surfen kaum statt.

Eine häufige Frage aus der Praxis lautet daher: Braucht jede Website oder App ein Cookie-Banner? Nun, im Prinzip nein, aber… Dann müssen alle verwendeten Cookies auch unter die Ausnahmetatbestände des TTDSG fallen. Diese lauten Erforderlichkeit und Wunsch des Nutzers. Zunächst kurz zum etwas schwammigen Begriff des Nutzerwunsches. Häufig wird dieser von Betreibern eines Angebots einfach unterstellt, nach dem Motto: Wer meine Seite besucht, der will doch auch die Cookies. Diesem Argument kann keine Aufsichtsbehörde folgen, die Interessenlage des Nutzerwun-

sches ist eng an einer tatsächlich plausibel begründbaren Erwartungshaltung auszulegen und nicht am Interesse des Betreibers einer Website. Für den Tatbestand der Erforderlichkeit ist die Lage klarer, die Aufsichtsbehörde prüft im Wesentlichen vier Kriterien:

a) Wann wird ein Cookie gesetzt/ausgelesen?
   Der Zeitpunkt ist für die Erforderlichkeit entscheidend. Wird eine Auswahlentscheidung, zum Beispiel über eine Auswahl am Cookie-Banner, gespeichert, dann ist dieser Cookie eben erst dann erforderlich, wenn eine Interaktion tatsächlich stattgefunden hat. Wenn ein Nutzer bzw. eine Nutzerin eine Website ohne Entscheidung wieder verlässt, weil der Cookie-Banner eventuell zu abschreckend war, dann ist eine Speicherung von Cookies für diesen Zweck eben genau nicht erforderlich.
b) Wie wird ein Cookie gesetzt/ausgelesen?
   Beim „Wie" ist vom Inhalt der Information im Cookie selbst die Rede. Oftmals werden sogenannte ID-Cookies verwendet – Zufallszahlen, welche ein Endgerät und damit eine/n Nutzer/in eindeutig mit einem Pseudonym markieren. Damit sind je nach Dauer eines Cookies (siehe c)) exakte Rückschlüsse auf individuelles Verhalten möglich, es handelt sich also um einen starken Eingriff in den Schutzbereich des TTDSG, die Privatsphäre. Erforderlich sind solche Cookies nur in engen Ausnahmefällen, wie bei Log-in-Prozessen, Warenkörben beim Online-Einkauf oder zum Mitführen einer Session. Nicht erforderlich sind solche ID-Cookies beispielsweise für das Speichern einer Entscheidung über Einwilligungen. Hier reicht es, wenn die Entscheidung ohne Bezug auf eine konkrete Person gespeichert wird (statt „ID=817387" also „Tracking=false;Comfort=true…). ID-Cookies werden von den Aufsichtsbehörden besonders kritisch gesehen, weil diese neben dem oftmals angegebenen legitimen Zweck auch andere Möglichkeiten bieten, zum Beispiel die Nachverfolgung individuellen Verhaltens, im Sprachgebrach auch Tracking genannt.

Und genau diese Cookies hatte der Gesetzgeber bereits beim Entwurf der ePrivacy-Richtlinie im Sinn, als Gefahr für die Privatsphäre im Internet.

c) Wie lange ist ein Cookie gültig?
Die zeitliche Komponente ist ebenfalls unter dem Gesichtspunkt der Erforderlichkeit zu sehen. Cookies haben eine Lebensdauer, ebenso IDs in Apps oder ähnliche Techniken. Will ein Betreiber ein Cookie über die Dauer eines laufenden Besuchs einer Website einsetzen, muss eine Erforderlichkeit vorliegen, ansonsten bedarf es einer Einwilligung. Als Beispiel sei der Warenkorb eines Online-Shops genannt. Erforderlich ist ein Cookie für den Warenkorb für die Dauer des Besuchs (Session-Cookie). Möchte eine Online-Händlerin oder ein Online-Händler einen Warenkorb ohne Anmeldung im Shop auch über die Session hinaus speichern, um zum Beispiel bei einem späteren Besuch auf Objekte im Warenkorb erneut hinzuweisen (was sicherlich im Interesse der Shop-Betreiberin oder des Shop-Betreibers ist), dann bedarf es dafür einer Einwilligung, weil dies schlicht nicht erforderlich ist. Unkritisch in diesem Zusammenhang sind Cookies zu sehen, welche keine Implikation auf die Privatsphäre haben. Ein Cookie, mit dem ein/e Nutzer/in eine Sprachpräferenz einer Website einstellt und als Text nur die Sprache beinhaltet (Bsp.: „Lang.:DE") ist unkritisch auch bei einer Speicherdauer von beispielsweise einem Jahr.

d) Wer darf Cookies setzen und auslesen?
Cookies können im Kontext der besuchten Website oder durch Elemente gesetzt werden, welche von dritter Seite in die eigentliche Website eingebunden sind (sogenannte third parties). Cookies, die von solchen „third parties" gesetzt werden, haben prinzipiell das Potenzial, Nutzer/innen über mehrere/sehr viele Websites nachzuverfolgen. Eine Erforderlichkeit ist hierfür kaum denkbar, es bedarf für das Setzen und Auslesen solcher Cookies im Regelfall einer Einwilligung.

Neben den klassischen Cookies, die stets im Mittelpunkt der Diskussion und der Regulierung stehen, gibt es weitere Techniken, die ebenfalls einen Eingriff in das Endgerät und damit auch einen TTDSG-relevanten Sachverhalt darstellen. Dazu zählen zum Beispiel sogenannte Fingerprints, bei denen Merkmale eines Endgeräts zielgerichtet ausgelesen werden. Ebenso können individualisierte Tracking-Pixel und -URLs als Speichern und/oder Auslesen gewertet werden. In jedem Fall sind solche Verarbeitungen DSGVO-relevant, worum es im nächsten Absatz gehen soll.

2. DSGVO-relevante Verarbeitungen

Werden personenbezogene Daten verarbeitet, bedarf es einer Rechtsgrundlage. Dies gilt auch dann, wenn Daten mithilfe von vermeintlich anonymen Cookies erhoben und verarbeitet werden. Um es noch einmal klar zu sagen: Daten, die mithilfe von Cookies oder anderer Parameter, welche eine Vereinzelung einer natürlichen Person ermöglichen, verarbeitet werden, sind keine anonymen Daten. Erwägungsgrund 30 der DSGVO stellt dies explizit klar. Vereinfacht gesagt gilt: Wenn Daten über Personen verarbeitet werden, bedarf es einer Rechtsgrundlage. Diese sind in Art. 6. Abs. 1 DSGVO aufgelistet. Im Bereich der Privatwirtschaft sind das berechtigte Interesse und die Einwilligung die beiden relevanten Rechtsgrundlagen. Für öffentliche Stellen ist neben der Einwilligung (welche im Verhältnis Bürgerinnen/Bürger und Staat nur sehr eingeschränkt eingesetzt werden kann, weil bei staatlichen Handlungen oftmals keine Freiwilligkeit gegeben ist) auch – stark eingeschränkt – die Wahrnehmung von Aufgaben im öffentlichen Interesse denkbar.

Die Rechtsgrundlagen haben ihre Grenzen, welche in der Praxis oftmals überdehnt werden. Das berechtigte Interesse muss dargelegt werden können, und eine Interessenabwägung mit Grundrechten und Grundfreiheiten natürlicher Personen muss vorgenommen werden. Eine bloße Nützlichkeit ist nicht ausreichend. Eine Interessenabwägung setzt voraus, dass ein Verantwortlicher genau erklären kann, was

mit den Daten passiert. Dies ist oft nicht der Fall. So manche Website oder App, deren Nutzung in irgendeiner Weise hilfreich erscheint, verarbeitet – verborgen hinter schwammigen Datenschutzerklärungen – gewonnene Daten für eigene Zwecke, die Datenerhebung ist viel umfangreicher als für den konkreten Zweck des Verantwortlichen erforderlich, die Daten werden weltweit, auch in unsicheren Drittstaaten verarbeitet. Dies sind drei klassische Mängel-Beispiele für Drittdienste in Websites oder Apps, die ein berechtigtes Interesse ausschließen. Auch wenn man bei Prüfungen gelegentlich Gegenteiliges zu hören bekommt: Für die Übermittlung von Nutzungsdaten an Drittdienste ist der Verantwortliche genauso verantwortlich wie für Verarbeitungen in vollständig eigener Hoheit.

Kommen wir zur Einwilligung: Diese muss freiwillig und vollständig informiert vor einer Verarbeitung erfolgen. Was sich einfach liest, ist in der Praxis mitunter schwierig und wird dann umso schwieriger, je komplexer und vielfältiger Art und Umfang der Einwilligungen sind. Nachfolgende Hinweise bzw. Grundsätze seien an dieser Stelle gestattet:

Nein heißt nein: Eine Einwilligung ist dann nicht wirksam, wenn es keine Einwilligung gibt. Ein „Okay", „Verstanden" oder Ähnliches ist keine solche.

Werden Einwilligungen gebündelt eingeholt, muss dieses Bündel genauso einfach abgelehnt werden können, wie ihm zugestimmt werden kann.

Die Nachweispflicht für eine Einwilligung enthält keine Befugnis, um Besucherinnen und Besucher über den gesamten Besuch einer Website zu verfolgen. Ein Einwilligungsmanagement, welches neben der Abgabe der Entscheidung auch Zwecke wie Analyse, A/B-Testing, Einwilligungsoptimierung bietet, kann seinerseits nicht ohne eine gesonderte Einwilligung eingesetzt werden.

Einfacher wird es natürlich auch durch eine Reduzierung von einwilligungsbedürftigen Datenverarbeitungen und Cookies. Meine Behörde erhält regelmäßig Beschwerden über Websites ohne „Cookie-Banner". Nicht immer, aber gelegentlich, kann die Beschwerde mit dem Hinweis eingestellt werden,

dass ein solches Banner keine gesetzliche Vorschrift ist, sondern nur dann erforderlich ist, wenn eine Einwilligung eingeholt werden muss.

3. Drittstaatenproblematik

Was ist zu tun?
Verantwortliche für Websites müssen diese auf datenschutzrechtliche Aspekte prüfen. Insbesondere die Einbindung von Drittinhalten sowie das Verwenden von Cookies müssen auf den Prüfstand und dürfen nur mit tragfähigen Rechtsgrundlagen verwendet werden.

Fast alle Beschwerden im Online-Bereich haben einen mehr oder weniger stark ausgeprägten Drittland-Bezug. Meist sind es Dienste oder Einbindungen aus den USA, über die sich Betroffene unter Hinweis auf die Rechtsprechung des Europäischen Gerichtshofs beschweren. Die Situation ist nach wie vor nicht einfach zu lösen, auch wenn es in diesem Jahr Bewegung gegeben hat (siehe 5.1).

4.1.2 Abmahnungen zu Google Fonts

↗ Art 6. Abs. 1 Buchst. f DSGVO

Urteil des LG München vom 20.01.2022:
↗ sdb.de/tb2207

Mit dem Inkrafttreten der Datenschutz-Grundverordnung (DSGVO) wurden bedrohliche Abmahnwellen wegen kleinster Verstöße prognostiziert. In der Praxis bleiben diese bislang weitgehend aus, im Jahr 2022 ist nun allerdings eine größere Welle von Abmahnungen losgeschwappt. Auslöser war ein Urteil des Landgerichts München vom 20. Januar 2022, in welchem festgestellt wurde, dass die Übertragung von Nutzungsdaten im Internet durch die Einbindung von Schriftarten von Google eine Verletzung des Persönlichkeitsrechts durch einen Datenschutzverstoß darstellt. Die Einbindung der Schriftarten als sogenannte Webfonts erfolgte im Fall des Urteils dynamisch, das heißt, dass Google die Schriftarten auf eigenen Servern bereitstellt und der oder die Websitebetreiber/-in diese Schriftarten in das eigene Angebot integriert. Wird die Website aufgerufen, werden IP-Adresse und Gerätedaten automatisch an Google übertragen. Da diese Datenübertragung durch den Aufruf einer Website erfolgt, ist die Betreiberin oder der Betreiber der Website auch datenschutzrechtlich Verantwortlicher. Hierfür ist eine Rechtsgrundlage erforderlich. Art 6. Abs. 1 Buchst. f DSGVO („berechtigtes Interesse") ist aufgrund der möglichen Übermittlung in einen Drittstaat außerhalb der EU nicht anwendbar (zudem ist die

Übermittlung für den Zweck der Darstellung von Schriftarten schlicht nicht erforderlich), es bedarf also einer Einwilligung. Auch diese Rechtsgrundlage ist infrage zu stellen, da eine vollständige Information von Betroffenen über die Datenverarbeitung von Google sowie mögliche Rechtsfolgen einer Übermittlung nicht möglich sind. Dennoch wird eine Einwilligung geduldet, wenn klar erkennbar ist, dass ein Datentransfer stattfinden kann und die Nichterteilung einer Einwilligung problemlos möglich ist.

Die dynamische Einbindung von Google Fonts stellt, wie seitens der Aufsichtsbehörden seit vielen Jahren angemahnt und durch das oben genannte Urteil bestätigt, einen klaren Verstoß gegen das Datenschutzrecht dar. Die im Urteil zugestandenen 100 Euro Schadensersatz haben nun Abmahnanwälte auf den Plan gerufen, welche im Namen der Mandantschaft Websites mit dynamisch eingebundenen Google Fonts abmahnen. Neben den 100 Euro werden dann noch Anwaltskosten gefordert. So fragwürdig dieses Vorgehen sein mag, so vermeidbar ist es auch. Die Schriftarten von Google können nämlich auch von der Betreiberin oder dem Betreiber der Website kostenlos heruntergeladen und in das eigene Angebot integriert werden. Der Aufwand hält sich in Grenzen und zumindest was Schriftarten betrifft, ist man sicher vor Post vom Abmahnanwalt oder auch von der Datenschutzaufsicht. Es gibt aber auch in diesem Jahr bei meiner Behörde trotz der umfangreichen Berichterstattung zum konkreten Thema noch reichlich Beschwerden über den Einsatz von Google Fonts, in vielen Fällen auch berechtigt. Im Gegensatz zum Abmahnanwalt versucht meine Behörde, den Missstand zunächst durch einen Hinweis mit Fristsetzung zu beheben und nicht gleich mit einem Bußgeld zu ahnden. Es ist dennoch zu empfehlen, den eigenen Webauftritt auf problematische Datenverbindungen zu prüfen, mitunter werden diese nicht absichtlich implementiert, sondern entstehen durch die Nutzung von Website-Baukästen oder Content-Management-Systemen. Eine einfache Möglichkeit der Prüfung ist neben der Nutzung von Browser-Tools der Online-Scanner Webkoll. Es ist davon auszugehen, dass solche

Online-Scanner Webkoll:
↗ webbkoll.dataskydd.net

Abmahnungen, wie zu Google Fonts, in Zukunft auch andere weitverbreitete Dienste in den Blick nehmen, das Vorgehen lässt sich leicht übertragen.

Aus der Praxis

Zum Schluss ein Tipp aus der Prüf-Praxis: Ein Verantwortlicher hatte sich im Beschwerdeverfahren zurückgemeldet, dass er Google Fonts nur einsetze, wenn mithilfe eines Cookie-Banners eine Einwilligung erteilt werde. Keine schöne Lösung, aber noch tolerabel. Beim Test durch meine Behörde tauchten die Verbindungen zu den Google Fonts aber trotz Bestätigung des Ablehnen-Buttons hartnäckig weiter auf. Es stellte sich heraus, dass zwar für die direkte Einbindung von Google Fonts eine Einwilligung abgefragt und bei Nichterteilung auch korrekt nicht ausgespielt wurde. Allerdings war ein YouTube-Video (ohne Einwilligung) eingebunden, welches seinerseits weitere Ressourcen von Google abgerufen und ausgeliefert hat, darunter auch Google Fonts.

Zum einen ist die Einbettung des YouTube-Videos ohne Einwilligung an sich bereits ein Datenschutzverstoß. Wenn jedoch vorher gefragt wird, ob Google Fonts genutzt werden und bei einem klaren „Nein" dennoch ausgespielt werden, lädt das Beschwerden (und gegebenenfalls auch ein/e Abmahner/in) förmlich ein. Als Betreiber/in einer Website sollte man daher genau hinschauen und im Auge behalten, dass eingebettete Inhalte Dritter immer eine Datenverbindung auslösen und damit einer Rechtsgrundlage bedürfen sowie weitere Dienste ihrerseits nachladen. Es bleibt kompliziert …

Was ist zu tun?
Auf eine dynamische Einbindung von Schriftarten im eigenen Webangebot sollte verzichtet werden. Es sei denn, es gibt eine klare Regelung zur Auftragsverarbeitung, und eine Datenübermittlung außerhalb der EU ist ausgeschlossen.

4.1.3 Nichtöffentliche Sitzungen des Gemeinderats

↗ § 37 SächsGemO

Ein Petent wandte sich an mich, weil er der Meinung war, dass sein Name zu Unrecht im öffentlichen Teil einer Gemeinderatssitzung erwähnt wurde. Hintergrund war die Wahl für die Stelle einer Bürgeramtsleiterin bzw. eines Bürgeramtsleiters einer Kommune. Diese erfolgte rechtmäßig durch eine

geheime Wahl im nichtöffentlichen Teil der Gemeinderatssitzung. Gegen diese legte der Petent Beschwerde ein.
Ein entsprechender Beschlussvorschlag sah nun jedoch vor, dass der im nichtöffentlichen Teil gefasste Beschluss nun im öffentlichen Teil aufgehoben werden soll. Dabei wurden namentlich die Teilnehmer und vor allem Nichtteilnehmer der nichtöffentlichen Sitzung sowie der Name des Petenten öffentlich benannt. Nach § 37 Sächsische Gemeindeordnung (SächsGemO) sind die Sitzungen des Gemeinderats jedoch dann nicht öffentlich, wenn berechtigte Interessen Einzelner eine nichtöffentliche Verhandlung erfordern. Davon umfasst sind alle rechtlich geschützten oder anerkannten Interessen, wie zum Beispiel Personalsachen oder Steuersachen.
Der zur Stellungnahme aufgeforderte Bürgermeister teilte mir – ohne Begründung – lediglich mit, dass seiner Auffassung nach die Aufhebung des Beschlusses, welcher in nichtöffentlicher Sitzung behandelt wurde, durchaus im öffentlichen Teil behandelt werden konnte. Es liege daher kein Datenschutzverstoß vor.
Mittlerweile hatte jedoch auch das zuständige Landratsamt, das der Petent ebenfalls kontaktierte, dem Bürgermeister mitgeteilt, dass es von einem Verstoß gegen § 37 SächsGemO ausgehe. Der Inhalt der Beschlussvorlage für die Sitzung stelle über den Wortlaut des Beschlusses hinaus Informationen bereit, die durch die Veröffentlichung im Ratsinformationssystem und die Verlesung der vollständigen Beschlussvorlage in der öffentlichen Sitzung nicht nur den Gemeinderätinnen und -räten, sondern auch der Öffentlichkeit frei zugänglich waren.
Nach einem dennoch umfangreichen Schriftwechsel mit der Gemeinde hat diese schließlich eingeräumt, dass „aus heutiger Sicht deutlich geworden ist, dass der Verfahrensablauf zur Behandlung der Aufhebung des Beschlusses nicht ordnungsgemäß verlaufen ist". Zudem wurde zugesichert, dies künftig zu beachten. Ich erachtete dies als ausreichend und schloss den Vorgang.

4.2 Auftragsverarbeitung

4.2.1 Datenweitergabe bei Beteiligung privatrechtlicher Unternehmen an kommunaler Bauleitplanung

↗ §§ 3, 4b, 11 BauGB, §§ 2 Abs. 1 Satz 2 und 3 Abs. 1 SächsDSDG, Art. 6 Abs.1 und Abs. 3 Buchst. b DSGVO, Art. 13 und Art. 28 DSGVO

Im Berichtszeitraum wandten sich zwei Petenten zu demselben Problemkreis an mich. Sie hätten sich (neben anderen Gemeindebürgerinnen und -bürgern) im Auslegungsverfahren eines vorhabenbezogenen Bebauungsplans beteiligt und Einwendungen gegen das Vorhaben eingebracht. Es sollte eine Fabrik erweitert werden. Die Anwohnerinnen und Anwohner befürchten hierdurch steigende Emissionen und exzessive Nutzung der Zufahrtsstraße, die durch ihre Siedlung führt, durch Lkw. Die an mich gewandte Datenschutzbeschwerde richtete sich nun dagegen, dass die federführende Gemeinde ungefragt ihre personenbezogenen Daten an ein Planungsbüro und etwaig an den Vorhabenträger (bzw. dessen Rechtsanwalt) weitergereicht habe. Die Petenten seien stutzig geworden, da sie zu ihren Einwendungen Schreiben nicht von der Gemeinde selbst, sondern von dem Planungsbüro erhalten haben.

Zur Stellungnahme von mir aufgefordert, teilte die betroffene Gemeinde mit, dass sie von der gesetzlich vorgegebenen Möglichkeit, private Dienstleister in dem Bauleitverfahren zu beteiligen, Gebrauch gemacht hat, § 4b Baugesetzbuch (BauGB). Das Vorhaben wäre durch einen städtebaulichen Vertrag nach § 11 BauGB mit dem Investor gesichert, der ebenfalls die Beteiligung des Planungsbüros vorsieht. Die Architekten seien durch diesen unter anderem zur Erarbeitung der Planunterlagen und Auswertung der Beteiligungen berufen. Dass das Planungsbüro an dem Vorhaben beteiligt ist, sei auch aus den Auslegungsunterlagen ersichtlich, sodass im Rahmen der Bürgerbeteiligung an dem Bauleitplan damit zu rechnen war, dass die personenbezogenen Daten der Bürgerinnen und Bürger auch an dieses weitergereicht werden. Hierüber seien auch die Bürgerinnen und Bürger mit entsprechenden Aushängen gemäß der Art. 13, 14 Datenschutz-Grundverordnung

(DSGVO) informiert worden. Durch diese Legitimationskette sah die Gemeinde die Datenweitergabe an das Planungsbüro als rechtmäßig an.

Hierbei musste ich der Gemeinde widersprechen. Es ist zunächst durchaus richtig, dass aus bauplanungsrechtlicher Sicht die Beteiligung von privaten Dritten gesetzlich zulässig und mitunter auch vorgesehen ist. Wenn hierbei aber personenbezogene Daten von Bürgerinnen und Bürgern verarbeitet werden sollen, bedarf es hierzu einer expliziten Rechtsgrundlage. Eine Verarbeitung auf Grundlage der Einwilligung gemäß Art. 6 Abs.1 Buchst. a DSGVO kann indes bereits deswegen nicht in Betracht kommen, da hierfür die notwendige Freiwilligkeit nicht gewährleistet sein kann: Es kann durchaus sein, dass sich Bürgerinnen und Bürger von der Eingabe ihrer Einwendungen abgehalten fühlen, wenn dies nur mit Weitergabe ihrer Daten an Dritte erfolgen könne.

Da das beauftragte Planungsbüro zudem keine öffentliche Stelle und insbesondere auch kein Beliehener, sondern lediglich ein sogenannter Verwaltungshelfer sein kann, ist auch der Anwendungsbereich des Sächsischen Datenschutzdurchführungsgesetzes (SächsDSDG) nicht eröffnet. Nach § 2 Abs. 1 Satz 2 SächsDSDG wird ein Beliehener als öffentliche Stelle behandelt, insoweit an ihn hoheitliche Aufgaben übertragen worden sind. Dem Planungsbüro werden aber gerade keine hoheitlichen Aufgaben übertragen. Diese Norm verleiht der Gemeinde vielmehr ein Recht, bestimmte Bereiche der Bauleitplanung zur Beschleunigung des Verfahrens auszulagern bzw. zu privatisieren. Anders ausgedrückt: Die Privatisierung der für die Bauleitplanung erforderlichen Schritte und Vorbereitungstätigkeiten wird durch die Norm ermöglicht, nicht etwa vorgeschrieben. Die Verwaltungsaufgabe „Bauleitplanung" verbleibt bei der Gemeinde, diese behält die Verantwortung für sämtliche Verfahrensabschnitte, das Planungsbüro nimmt die Stellung des Verwaltungshelfers ein.

Somit ist auch der Anwendungsbereich des SächsDSDG – der die Datenverarbeitung durch öffentliche Stellen regelt – nicht eröffnet, eine Ermächtigungsnorm kann sich für die Datenübermittlung an das Planungsbüro hieraus nicht ergeben.

Somit verbleibt für die Gemeinde nur noch die Möglichkeit, mit dem Planungsbüro einen Vertrag zur Auftragsverarbeitung nach den Regeln des Art. 28ff. DSGVO abzuschließen.
Dies ist auch datenschutzrechtlich zulässig, denn das Planungsbüro verfolgt bei der Verarbeitung keine eigenen Zwecke außer der Erbringung einer Dienstleistung gegenüber der Gemeinde und auf der Grundlage dokumentierter Weisungen – sie verfolgt mit der Verarbeitung somit keinen eigenen, selbstständigen Zweck. Zudem muss das Planungsbüro bei der Verarbeitung der Daten durch die Gemeinde überwacht werden.
Ich habe der Gemeinde daher empfohlen, mit dem Planungsbüro einen Vertrag zur Auftragsverarbeitung abzuschließen, da ansonsten die Rechtmäßigkeit der Datenverarbeitung nicht gegeben ist.
In dem Vertrag sind die rechtliche Bindung des Auftragsverarbeiters an den Verantwortlichen, der Gegenstand und die Dauer der Verarbeitung, Art und Zwecke der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien von betroffenen Personen festzulegen, Art. 28 Abs. 3 DSGVO (sogenannter Mindestgehalt eines Auftragsverarbeitungsvertrages). Zudem sind in dem Vertrag vom Auftragsverarbeiter Garantien einzuholen, dass seinerseits geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der DSGVO erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet, Art. 28 Abs. 5 DSGVO.
Die Gemeinde als Verantwortlicher und das Planungsbüro als Auftragsverarbeiter bilden für Ansprüche betroffener Personen nach der DSGVO eine Gesamtschuldnerschaft, beide haften gegenüber der betroffenen Person bei Verstößen gegen die Datenschutzvorschriften.
Auch habe ich der Gemeinde mitgeteilt, dass, sollten zudem Daten der betroffenen Bürgerinnen und Bürger auch an den Vorhabenträger selbst bzw. dessen anwaltlichen Vertreter erfolgen, dies ebenfalls nur nach den oben beschriebenen Grundsätzen im Rahmen einer Auftragsdatenverarbeitung möglich und zulässig wäre.

Was ist zu tun?
Bei der Beteiligung privater Dritter an der Erfüllung hoheitlicher Aufgaben ist zunächst an die Beleihung zu denken. Ist diese gesetzlich nicht vorgesehen, bleibt für private Verwaltungshilfe nur der Abschluss eines Auftragsverarbeitungsvertrages, wenn hierdurch personenbezogene Daten verarbeitet werden sollen.

4.2.2 Auftragsverarbeitungsvertrag, Auftragsverarbeitung und Verpflichtungsgesetz

↗ IfSG, DSGVO, Verpflichtungsgesetz

Ein Landratsamt hatte einem Auftragsverarbeiter Zugriff auf personenbezogene Daten beziehungsweise Gesundheitsdaten in der Cloud des Landratsamtes gewährt. Konkret betraf die Auftragsverarbeitung vorgelagerte Tätigkeiten des Gesundheitsamtes in Bezug auf die Aufgabe gemäß § 16 Abs. 1 Infektionsschutzgesetz (IfSG), die notwendigen Maßnahmen zur Abwendung der dem Einzelnen oder der Allgemeinheit drohenden Gefahren durch das Coronavirus zu treffen. Es handelte sich um Tätigkeiten wie die Erfassung der Daten von Erkrankten und die Ermittlung von Kontaktpersonen. Der Zugriff war Gegenstand des abgeschlossenen Auftragsverarbeitungsvertrags. Dies wurde mir im Zuge einer Beschwerde eines Betroffenen bekannt, der in Zweifel zog, dass eine private Stelle im Auftrag der Behörde diese Aufgabe wahrnehmen darf.

Hoheitliche Tätigkeiten können ohne gesetzliche Regelung (Beleihung) nicht von privaten Stellen ausgeübt werden. Öffentliche Aufgaben nichthoheitlicher Art können grundsätzlich ganz oder teilweise auch von privaten oder anderen Stellen durchgeführt werden.

Es lag keine Vollübertragung der hoheitlichen Aufgaben des Gesundheitsamts des Landratsamtes im Rahmen des IfSG, insbesondere keine Erstellung von Bescheiden an den Auftragsverarbeiter, vor. Bei der übertragenen Tätigkeit handelte es sich um eine nichthoheitliche Aufgabe. Im Lichte des Umfangs der Auslagerung einer vorgelagerten Tätigkeit wurde die Auftragsverarbeitung von mir noch für zulässig erachtet und daher nicht beanstandet.

Beim Abschluss eines Auftragsverarbeitungsvertrags durch eine Behörde, beispielsweise durch ein Landratsamt, ist darauf zu achten, ob für die Wahrnehmung der Aufgabe seitens des Auftragsverarbeiters eine Verpflichtung gemäß dem Verpflichtungsgesetz vorzunehmen ist (vgl. hierzu: Arbeitspapier des Bayerischen Beauftragten für den Datenschutz).

Arbeitspapier zur förmlichen Verpflichtung als Instrument des Datenschutzes:
↗ sdb.de/tb2208

Die öffentliche Stelle sollte die förmliche Verpflichtung immer dann erwägen, wenn sie externen Personen einen tatsächlichen Zugang zu personenbezogenen Daten eröffnet, der nicht einer Vorabkontrolle im Einzelfall (durch eine entsprechende zugangsgewährende Entscheidung) unterliegt. Dies gilt insbesondere dann, wenn es sich um Daten im Sinne von Art. 9 Abs. 1 Datenschutz-Grundverordnung (DSGVO) handelt. Soll ein nichtöffentlicher Auftragsverarbeiter für eine verpflichtungsberechtigte öffentliche Stelle besondere Kategorien personenbezogener Daten verarbeiten, sollte diese Stelle vertraglich den Einsatz von förmlich verpflichtetem Personal fordern. Dies gilt auch dann, wenn Unter-Auftragsverarbeiter Zugang zu personenbezogenen Daten erhalten sollen oder können. Die Verpflichtung ist von der verpflichtungsberechtigten öffentlichen Stelle durchzuführen.

Was ist zu tun?
Schließt eine öffentliche Stelle mit einem nichtöffentlichen Auftragsverarbeiter einen Auftragsverarbeitungsvertrag ab, durch den dieser Zugang zu personenbezogenen Daten beziehungsweise Gesundheitsdaten erhält, so hat diese darauf zu achten, dass bei den Beschäftigten des Auftragsverarbeiters eine Verpflichtung nach dem Verpflichtungsgesetz erfolgt.

Das Landratsamt wurde von mir aufgefordert, dies bei künftigen Auftragsverarbeitungsverträgen zu beachten.

4.3 Sicherheit der Verarbeitung

4.3.1 Anbieter dürfen Passwörter nicht im Klartext speichern

↗ Art. 32 DSGVO

Das erste nach der DSGVO in Deutschland verhängte Bußgeld ging 2018 an das Soziale Netzwerk „Knuddels". Die Passwörter von Kundinnen und Kunden wurden im Klartext gespeichert und durch einen Hackerangriff mit anderen Daten erbeutet. Dies kostete das Unternehmen 20.000 Euro, trotz umfassender Zusammenarbeit mit der Aufsichtsbehörde. Warum also dürfen Passwörter nicht im Klartext gespeichert werden? Weil so bei einem Datenleck die Kombination aus E-Mail-Adresse und Passwort in die Hände von Unbefugten gelangt, welche diese nutzen können, um Zugang zu anderen Benutzerinnen- und Benutzerkonten zu bekommen. Die Nutzung von im Internet oder Darknet angebotenen Identitäts-Datenbanken ist leider eine sehr erfolgreiche Methode, um durch eine Anmeldung geschützte Zugänge zu überwinden, da ein hoher Anteil der Nutzerinnen und Nutzer die Kombi-

nation aus E-Mail-Adresse und Passwort bei verschiedenen Diensten/Websites/Nutzerkonten wiederverwendet.

Aber wie kann eine Anbieterin oder ein Anbieter ein Passwort überprüfen, wenn es nicht im Klartext speichern darf? Dafür stellt in der IT-Sicherheit seit einiger Zeit die Nutzung von Hash-Funktionen den Stand der Technik dar und ist in der Praxis auch üblich. Diese Funktionen erlauben die Transformation einer beliebigen Zeichenfolge in eine feste Anzahl von Bits – dem sogenannten Hashwert. Die gleiche Zeichenfolge führt dabei immer zu dem gleichen Hashwert, aber aus dem Hashwert lässt sich weder die ursprüngliche Zeichenfolge errechnen noch irgendeine andere Zeichenfolge, welche den gleichen Hashwert generieren würde. Die Anbieterin oder der Anbieter speichert bei sich also statt des Passwortes nur dessen Hashwert. Wenn sich der oder die Nutzer/in anmeldet, gibt er bzw. sie sein/ihr Passwort an, die Anbieterin oder der Anbieter berechnet daraus den Hashwert und vergleicht diesen Wert mit dem gespeicherten Wert. Sind die beiden identisch, wird die Nutzerin bzw. der Nutzer eingeloggt. Sollten Unbefugte Zugriff erlangen oder der Anbieterin oder dem Anbieter diese Daten durch eine Datenpanne gestohlen werden, hat die oder der Unbefugte nur die Hashwerte, welche sie oder er nicht zum Einloggen nutzen kann.

Dieses Vorgehen ist nicht nur sicherheitstechnisch vorbildlich, sondern nach meiner Auffassung eindeutig durch Art. 32 Datenschutz-Grundverordnung (DSGVO) gesetzlich erfasst. Das Risiko, welches sich durch vulnerable Datenbanken mit Klartextpasswörtern ergibt, ist in Anbetracht der weit verbreiteten Lösung und einfachen Umsetzbarkeit nicht hinnehmbar. Ich folge hierbei der umfangreichen Praxis und den Vorgaben des Bundesamts für Sicherheit in der Informationstechnik (BSI). Passwörter und Konten von Kundinnen und Kunden dürfen nicht im Klartext gespeichert werden. Dies betrifft auch verschlüsselte Passwörter, wenn der Schlüssel bei der Anbieterin oder dem Anbieter liegt. Die Authentifizierung muss mittels Hashwerten erfolgen.

Dieses Jahr erreichte mich auch eine Beschwerde zu diesem Thema. Ein Unternehmen mit einer hohen Anzahl von Nutzerinnen- und Nutzerkonten, welche teilweise auch empfindliche Informationen wie E-Mails betrafen, zeigte seinen Kundinnen und Kunden die Passwörter im eigenen Kundenportal im Klartext an. Das ist nur möglich, wenn die Passwörter (auch) im Klartext gespeichert werden. Da dies offen sichtbar war, musste es nicht erst zu einem Datenleck kommen, um diesen Umstand zu entdecken. Ich machte die Unternehmensleitung auf den Umstand aufmerksam, und in den nachfolgenden Gesprächen zeigte man sich einsichtig, wollte aber aus Komfortgründen die Funktionalität der Klartextanzeige beibehalten. Eine klassische Abwägung also, zwischen Sicherheit und Komfort für die Nutzerinnen und Nutzer? Nein, denn hinsichtlich der Sicherheit sind an dieser Stelle keine Abstriche zugunsten der „bequemen" Erfahrung zulässig. Die Anbieterin oder der Anbieter hat die Speicherung nachfolgend mit einem internen Passwortmanager realisiert, welcher die Passwörter der Kundinnen und Kunden enthält, aber mit einem Masterpasswort verschlüsselt ist, das nur die Kundin bzw. der Kunde kennt. Diese Lösung ist zwar etwas unorthodox, aber akzeptabel – das Prinzip von Passwortmanagern ist etabliert, und die Verwendung wird jeder Nutzerin und jedem Nutzer nahegelegt.

Was ist zu tun?
Es sind hashbasierte Anmeldeverfahren zu nutzen. Passwörter dürfen nicht im Klartext gespeichert werden. Nutzerinnen und Nutzer sollten Passwortmanager nutzen.

4.4 Meldung von Datenschutzverletzungen

4.4.1 Erstmals Rückgang der Meldungen nach Artikel 33 DSGVO

↗ Art. 33 DSGVO

Nach Art. 33 DSGVO sind Verantwortliche verpflichtet, im Falle der Verletzung des Schutzes personenbezogener Daten unverzüglich und möglichst binnen 72 Stunden nach Bekanntwerden der Verletzung diese der Aufsichtsbehörde zu melden, es sei denn, dass die Verletzung des Schutzes per-

Datenpanne per Webformular melden:
↗ datenschutz.sachsen.de

sonenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.
Im Berichtszeitraum sind bei mir 809 solcher Meldungen eingegangen. Im Vergleich zum vorjährigen Berichtszeitraum (923 Meldungen) entspricht dies einem Rückgang um rund 12 Prozent. Damit ist erstmalig seit dem Inkrafttreten der Datenschutz-Grundverordnung eine Abnahme der Meldungen von Datenschutzverletzungen zu verzeichnen.

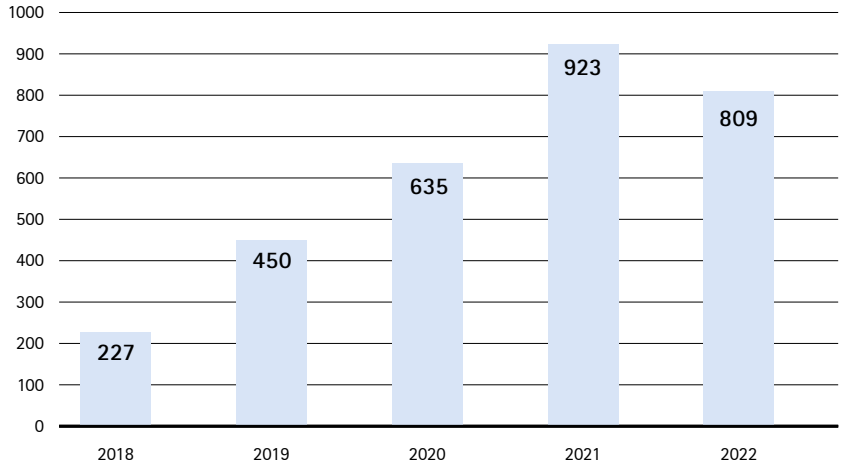


Abbildung 1:
Meldungen von Datenschutzverletzungen nach Art. 33 DSGVO

Die folgenden Fallgruppen sind im Berichtszeitraum besonders häufig gemeldet worden:

Fehlversendung

Nach wie vor stellt die Fehlversendung von Unterlagen mit personenbezogenen Daten mit ca. einem Drittel der Meldungen von Datenschutzverletzungen die häufigste Fallgruppe dar. Dem liegt in der Regel ein unbeabsichtigter Versand zugrunde, welcher auf falsche Zuordnung von Unterlagen, fehlerhafte maschinelle Kuvertierung, falsche Adressdaten oder schlicht auf Namensverwechslung zurückzuführen ist. Das Risiko für die betroffenen Personen ist in der Regel kein hohes, da bei dieser Fallgruppe die Datenschutzverletzung

durch die falsche Empfängerin oder den falschen Empfänger gegenüber dem Verantwortlichen angezeigt wird und somit das datenschutzrechtlich Erforderliche, wie zum Beispiel Löschung oder Rücksendung sowie Korrektur der Fehlerursache einschließlich erneuter Versand, durch den Verantwortlichen in die Wege geleitet werden kann.

Offener E-Mail-Verteiler

Ebenfalls ist der sogenannte offene E-Mail-Verteiler, bei welchem die E-Mail-Adressen nicht in das Blindkopie-Feld (bcc), sondern in der Regel versehentlich in das Kopie-Feld (cc) eingetragen werden, eine typische Fallgruppe der Datenschutzverletzungen, die bei mir gemeldet werden. Der offene E-Mail-Verteiler ist dann meldepflichtig, wenn die E-Mail-Empfänger/innen mit der offenen Verbreitung ihrer E-Mail-Adresse nicht ausdrücklich einverstanden waren, da es dann an einer Rechtsgrundlage für die Verarbeitung personenbezogener Daten mangelt. Diese Art der Datenschutzverletzung ist regelmäßig auf ein Versehen der Absenderin bzw. des Absenders zurückzuführen, sodass gerade bei dieser Fallgruppe wiederholte Sensibilisierungsmaßnahmen sinnvoll sind.

Verlust auf dem Postweg

Neben der Fehlversendung ist der Verlust von Unterlagen mit personenbezogenen Daten auf dem Postweg ein regelmäßiger Meldefall. Der wesentliche Unterschied zur Fehlversendung ist der, dass beim Verlust der Verbleib im Unklaren bleibt und somit das Risiko für die betroffenen Personen stets höher einzustufen ist als bei der Fehlversendung, bei der sich die falsche Empfängerin oder der falsche Empfänger meldet und daher eine abschließende Bewertung des Risikos vorgenommen werden kann.

Einbruch und Diebstahl

Datenschutzverletzungen im Rahmen von Diebstählen und Einbrüchen stellen ebenfalls auch in diesem Berichtszeitraum eine typische Fallgruppe dar, welche bei mir gemeldet

wurde. Festzustellen ist, dass sich hierbei die kriminellen Handlungen nicht zwingend auf die Erlangung der personenbezogenen Daten richtet, sondern vielmehr auf die Gegenstände, auf denen die personenbezogenen Daten gespeichert sind, wie zum Beispiel Digitalkameras, Laptops und so weiter. Dies führt jedoch nicht dazu, dass das verbundene Risiko bei derartiger Beschaffungskriminalität für die Betroffenen als gering einzustufen ist, da in der Regel nicht ausgeschlossen werden kann, dass im Nachhinein die personenbezogenen Daten ebenfalls in den Blick der Kriminellen gelangen, um hieraus einen finanziellen Vorteil zu erlangen. Insbesondere bei dieser Fallgruppe gilt es, bereits den Anreiz so gering wie möglich zu halten, indem entsprechende technische Geräte nicht unbeaufsichtigt gelassen, sondern ordnungsgemäß verwahrt werden. Des Weiteren empfiehlt es sich, die auf den technischen Geräten gespeicherten personenbezogenen Daten zu verschlüsseln, regelmäßige Backups durchzuführen und einen ausreichenden Passwortschutz einzurichten.

Cyberkriminalität

Wie bereits in den Berichtszeiträumen zuvor stellen die Meldungen, die unter den allgemeinen Begriff der Cyberkriminalität zusammengefasst werden können, eine wesentliche Fallgruppe der Datenschutzverletzungen dar. Generell fallen hierunter sämtliche Handlungen/Straftaten, die durch die Nutzung von Kommunikations- und Informationstechniken begangen werden. Problematisch ist, dass solche Handlungen nahezu von jedem Ort der Welt aus durchgeführt und ihre Spuren relativ gut verschleiert werden können. Typische Fälle im Bereich der Cyberkriminalität sind Spam- und Phishing-Mails, die Verschlüsselung von Systemen mit Ransomware oder allgemein die Verwendung von Schadsoftware (Malware) bzw. das Ausnutzungen von Schwachstellen.
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 nachfolgenden Hinweise zu vorbeugenden Maßnahmen.

4.4.2 Vorbeugende Maßnahmen

↗ Art. 28, 32, 33, 34 DSGVO

Wie bereits im letztjährigen Tätigkeitsbericht vermerkt, sind Prävention und Vorsorge die richtigen Mittel, um einer Datenschutzverletzung und damit verbundenen Risiken für Betroffene sowie der Notwendigkeit der Meldepflicht gemäß Art. 33 Datenschutz-Grundverordnung (DSGVO) entgegenzuwirken. Folgende Vorkehrungen sind nach wie vor zu empfehlen:

- Daten sichern! Die Daten von Firmen und Organisationen müssen unbedingt gesichert sein. Sichere Offline-Datensicherungen sollten so verwahrt werden, dass sie 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, Datenabflüsse zu erkennen und so 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 IT-Administrator, interne Datenschutzbeauftragte, die Datenschutzaufsichtsbehörde oder auch die Mitarbeiter, Unternehmensleitung und Kunden zu informieren sind.
- Reservetechnik vorhalten! Eine dringende Empfehlung ist zudem, Reservetechnik vorzuhalten. Ermittler können so das angegriffene IT-System forensisch sorgfältig 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(n) Daten betroffen sind.

- Weiterbildung! IT-Verantwortliche und all jene, die in Unternehmen und Organisationen für die Informationssicherheit zuständig oder am jeweiligen Prozess beteiligt sind, benötigen regelmäßig Weiterbildung.

Im Zusammenhang mit der Meldepflicht von Datenschutzverletzungen gemäß Art. 33 DSGVO weise ich darauf hin, dass sämtliche Datenschutzverletzungen mir gegenüber zu melden sind. Dies ist lediglich dann ausgeschlossen, wenn die Datenschutzverletzung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.
Darüber hinaus weise ich auf die neben der grundsätzlich bestehenden Rechenschaftspflicht gemäß Art. 5 Abs. 2 DSGVO im Besonderen für die Meldefälle bestehende Dokumentationspflicht gemäß Art. 33 Abs. 5 DSGVO sowie auf die mögliche Pflicht der Benachrichtigung der betroffenen Person nach Art. 34 DSGVO hin.
Im Rahmen der Verpflichtungen nach Art. 32 DSGVO hat der Verantwortliche grundsätzlich dafür Sorge zu tragen, dass die erforderlichen technischen und organisatorischen Maßnahmen umgesetzt und regelmäßig zu überprüfen sind, damit Datenschutzverletzungen, soweit es möglich ist, vermieden werden. Verstöße gegen Art. 32 DSGVO wären beispielsweise fehlende Sicherheitsupdates, fehlende Backups, fehlende Verschlüsselung, aber auch fehlende Sensibilisierungsmaßnahmen gegenüber Beteiligten.
Verstöße sowohl gegen Schutzmaßnahmen gemäß Art. 32 DSGVO als auch gegen formelle Anforderungen der Meldung bzw. Benachrichtigung gemäß Art. 33, 34 DSGVO können Gegenstand eines bußgeldrechtlichen Verfahrens gemäß Art. 83 Abs. 4 Buchst. a DSGVO werden. Daher empfehle ich sowohl zum Schutz der Interessen der Betroffenen als auch der eigenen wirtschaftlichen Interessen der Verantwortlichen, die oben genannten dargelegten Vorkehrungen zu prüfen und stets auf aktuellem Stand zu halten.

4.4.3 Erwähnenswerte Einzelmeldungen nach Art. 33 DSGVO

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

Landesweit eingesetzte elektronische Fachanwendung mit Zugriffsgefahr durch externe Gutachterinnen und Gutachter

Im Berichtszeitraum meldete mir eine kommunale Stelle die potenzielle Gefahr eines Zugriffs auf personenbezogene Daten in einer landesweit eingesetzten elektronischen Fachanwendung durch externe Gutachterinnen und Gutachter über die Suchfunktion.

Wie die meldende Stelle mitteilte, werden im Rahmen der Anwendung der betreffenden elektronischen Fachanwendung externe Gutachterinnen und Gutachter grundsätzlich bezogen auf jeden zu begutachtenden Einzelfall beauftragt. Gleichwohl stellte sich heraus, dass Gutachterinnen und Gutachter abweichend von der üblichen Vorgangsbearbeitung auch über die Möglichkeit der Suchfunktion über den berechtigten Zugriff hinaus Einsicht in personenbezogene Daten hätten nehmen können.

Im Rahmen der Prüfung der Meldung einschließlich eines Videokonferenztermins mit der meldenden Stelle (Verantwortlicher) sowie dem für die Fachanwendung beauftragten Auftragsverarbeiter wurde der Sachverhalt und das bestehende Risiko für die potenziell betroffenen Personen umfassend erörtert. Die meldende Stelle teilte mit, dass ihr keine tatsächlichen unberechtigten Zugriffe bekannt seien, dies jedoch technisch nicht ausgeschlossen werden könne. Daher wurden Abhilfemaßnahmen durch Anpassungen des Ablagesystems in der elektronischen Fachanwendung besprochen und entsprechend festgelegt.

Die Umsetzung dieser Maßnahmen zeigte mir die meldende Stelle fristgemäß an, sodass das potenzielle Risiko für die betroffenen Personen abschließend beseitigt wurde.

Schwachstelle einer Hochschuldatenbank in Entwicklungsumgebung

Eine sächsische Hochschule meldete mir im Berichtszeitraum eine Schwachstelle in einer MySQL-Datenbank, welche sich in einer ungeschützten Entwicklungsumgebung befand und personenbeziehbare Echtdaten enthielt.

Die Datenbank lief auf dem Arbeitsplatzrechner eines IT-Mitarbeiters, welcher eine Sicherheitslücke aufwies. Durch einen Konfigurationsfehler war die Datenbank weltweit erreichbar und hatte zudem einen mangelhaften Passwortschutz. Seitens der meldenden Stelle wurde festgestellt, dass sich in der Datenbank ein Erpressungstext befand, welcher die Veröffentlichung von Daten androhte, sollte keine Zahlung in Bitcoin erfolgen.

Der Sachverhalt wurde mit der meldenden Stelle umfassend erörtert. Es wurde mitgeteilt, dass der betroffene Rechner vom Netz getrennt und der Log-in des Mitarbeiters gesperrt wurde. Es kam zu keinen Löschungen oder Verschlüsselungen, sodass sogar davon ausgegangen werden kann, dass möglichweise keine Daten abgegriffen wurden. Gleichwohl wurden weiteren Untersuchungen und Sicherheitsmaßnahmen ergriffen. Des Weiteren wurden die betroffenen Nutzerinnen und Nutzer informiert.

Im Rahmen der Besprechung mit der meldenden Stelle wurde festgelegt, dass entsprechende technisch-organisatorische Regelungen für Test- und Entwicklungsumgebungen dahingehend zu präzisieren sind, wonach in solchen Umgebungen grundsätzlich keine personenbeziehbaren Echtdaten verwendet werden dürfen, was in einer entsprechenden Dienstanweisung für den IT-Bereich umgesetzt wurde.

Was ist zu tun?
Siehe vorbeugende Maßnahmen unter 4.4.2

4.5 Datenschutzbeauftragte/r

4.5.1 Datenschutz-Folgenabschätzung

↗ Art. 35 DSGVO

Die Datenschutz-Folgenabschätzung (DSFA) gemäß Art. 35 Datenschutz-Grundverordnung (DSGVO) ist eine frühzeitige Risikoanalyse des angestrebten Prozesses mit seinen Ver-

arbeitungsvorgängen. Die Prognose ist jedoch aus der Betroffenensicht durchzuführen und nicht aus der Risikosicht des Verantwortlichen. Daher kann auch nicht, wie im IT-Sicherheitsmanagement möglich, ein Risiko für die Betroffenen durch den Verantwortlichen je nach Risikoappetit im Rahmen der Risikobehandlung übernommen oder auf Dritte verlagert werden.

Dabei ergibt sich die Perspektive der Betroffenensicht bereits aus Art. 35 Abs. 1 Satz 1 DSGVO für die durchzuführende vorgelagerte Schwellenprüfung zur Erforderlichkeit einer DSFA, in welcher ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen als Folge der Verarbeitung personenbezogener Daten gefordert wird. Sie folgt aber auch aus Art. 35 Abs. 7 Buchst. c und Buchst. d DSGVO für die nachgelagerte und von der Schwellenwertprüfung abzugrenzenden DSFA, bei der in zwei von vier Mindestinhaltspunkten einer DSFA eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen natürlichen Personen sowie die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, durch die der Schutz personenbezogener Daten sichergestellt wird, konkret benannt werden. Art. 35 Abs. 7 Buchst. d DSGVO spricht im Übrigen klar von einer Bewältigung der Risiken.

Schwellenwertprüfung zur Erforderlichkeit einer DSFA

Der Gesetzgeber hat in Art. 35 Abs. 3 DSGVO eine nicht abschließende Aufzählung von Verarbeitungsvorgängen mit zwingender Pflicht zur Durchführung einer DSFA vorgenommen. Soweit eine Verarbeitung hierunter fällt, ist eine Schwellenwertprüfung nicht mehr erforderlich, sondern die DSFA zwingend durchzuführen. Die Sächsische Datenschutz- und Transparenzbeauftragte veröffentlicht hierzu eine Muss-Liste auf ihrer Website, welche aber ebenfalls nicht abschließend ist. Die Schwellenwertprüfung wird in dem Erwägungsgrund 84 Satz 1 zur DSGVO dahingehend erläutert, dass schon ein wahrscheinlich hohes Risiko der Verarbeitungsvorgänge für die Rechte und Freiheiten natürlicher Personen ausreicht, um eine DSFA erforderlich zu machen. Die eigene Schwellenwertprüfung der Verarbeitungsvorgänge erfolgt dabei ohne

DSFA-Muss-Liste:
↗ sdb.de/tb2209

Berücksichtigung von technischen und organisatorischen Maßnahmen. Sie ist ergebnisunabhängig zu dokumentieren. Als Hilfsmittel empfiehlt sich die Heranziehung der Leitlinien der Artikel-29-Datenschutzgruppe zur Datenschutz-Folgenabschätzung (DSFA) und die Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt".

Leitlinien zur DSFA:
↗ sdb.de/tb2210

Hier wird auf den Seiten 9ff. erläutert, wann eine DSFA verpflichtend ist und wann auf eine DSFA verzichtet werden kann. Der Europäische Datenschutzausschuss (Nachfolger der Artikel-29-Datenschutzgruppe) hat diese Leitlinien gebilligt.

DSFA vor dem Einsatz der Verarbeitungsvorgänge

Häufig mangelt es in der vorab durchzuführenden DSFA schon an einer vollständigen systematischen Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, einschließlich der vom Verantwortlichen verfolgten berechtigten Interessen, wie es Art. 35 Abs. 7 Buchst. a DSGVO als ersten Schritt der Risikoanalyse fordert.

Die Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck, als zweiter Schritt der Analyse gemäß Art. 35 Abs. 7 Buchst. b), wird regelmäßig nicht lückenlos dargestellt.

Im dritten erforderlichen Schritt der Risikobewertung gemäß Art. 35 Abs. 7 Buchst. c DSGVO werden mögliche Risiken für Betroffene hinsichtlich der Schwere und der Eintrittswahrscheinlichkeit oft nicht in der Gesamtheit erfasst, oder sie werden vielfach wieder aus der hier unzulässigen Sicht des Verantwortlichen heraus bewertet, obwohl sich diese Risiken im Wesentlichen anhand der Beschreibung im Erwägungsgrund 75 zur DSGVO entnehmen lassen.

Oftmals endet die Analyse in den DSFA mit diesem dritten Schritt, oder er wird mit den geplanten Abhilfemaßnahmen (technische und organisatorischen Maßnahmen) bereits vermengt. Dies führt zu einer Verkürzung der Analyse (Mindestanforderung), da der vierte Schritt gemäß Art. 35 Abs. 7 Buchst. d DSGVO die Auflösung bringen soll, ob es dem Verantwortlichen durch geplante Abhilfemaßnahmen gelingt,

die im dritten Schritt identifizierten Risiken tatsächlich zu bewältigen.

Streng genommen wäre dieser vierte Schritt also aufzuteilen in a) Dokumentation der geplanten Abhilfemaßnahmen, b) erneute Risikoanalyse unter Berücksichtigung der geplanten Abhilfemaßnahmen und c) Ergebnis. Im Idealfall kommt das Ergebnis zu einem angemessenen Datenschutzniveau sowie dem Nachweis, dass die Verarbeitungsvorgänge die Anforderungen der DSGVO einhalten.

Was ist zu tun?

Die Schwellenwertprüfung und die eventuell nachfolgende DSFA ist aus der Betroffenensicht heraus durchzuführen und nicht aus der Risikosicht des Verantwortlichen. Ein identifiziertes Risiko ist einzudämmen.

5 Internationaler Datenverkehr

5.1 Drittstaatentransfer – Quo vadis?

↗ DSGVO

Ein Thema, welches innerhalb der Aufsichtsbehörden ein Dauerbrenner ist, ist der Drittstaatentransfer. Seit im Jahr 2020 der Europäische Gerichtshof den Privacy Shield für unwirksam erklärt hat, wird trefflich darüber gestritten, was nun erlaubt ist bzw. was eigentlich Datentransfer bedeutet. Denn auch wenn der Auftragsverarbeiter eine Datenverarbeitung in europäischen Rechenzentren zusagt, kann ein Datentransfer in Drittstaaten nicht ausgeschlossen sein. Sei es durch Ausnahmen in den Verträgen, in denen dann doch ein Drittstaat im Support-Fall involviert ist, oder aufgrund der nicht mit europäischen Grundrechten zu vereinbarenden Befugnisse von ausländischen Behörden.

Was ist seit dem Urteil passiert? Ist das Internet abgeschaltet worden? Haben Google, Apple, Facebook und Microsoft aufgehört, ihre Dienste in Europa anzubieten? Nun, offensichtlich nicht. Der Europäische Gerichtshof (EuGH) hat zwar den Privacy Shield für unwirksam erklärt, ein Datenexport auf Basis der Standardvertragsklauseln ist jedoch nach wie vor möglich. Der Europäische Datenschutzausschuss hat Empfehlungen veröffentlicht, die dem Datenexporteur auferlegen, mithilfe von zusätzlichen Maßnahmen für ein Schutzniveau wie in Europa zu sorgen. Sprich: Ein Zugriff Unbefugter, zum Beispiel ausländischer Behörden, soll wirksam ausgeschlossen werden. Aus der Informationssicherheit weiß man, dass Geheimdienste neben Kriminellen und pri-

vilegierten Innentäterinnen und Innentätern (zum Beispiel Administratorinnen bzw. Administratoren) die potentesten denkbaren Angreifer sind. Die Versuche, wirksame zusätzliche Maßnahmen zu ergreifen, sind daher in vielen Fällen zum Scheitern verurteilt. Denn auch wenn Verschlüsselung eingesetzt wird, kommt es stets darauf an, für wen, wie lange verschlüsselt wird, wer entschlüsseln kann und wie zukunftsfest Verschlüsselungsalgorithmus und -verfahren sind. Gerade beim letzten Punkt wird es schwierig, Aussagen zu finden, welche über einen Zeitraum von fünf Jahren hinausgehen. So haben beispielsweise Gesundheitsdaten auch nach Ablauf dieser Zeit ein Schutzniveau über dem „normalen Schutzbedarf". Auch bringen Verschlüsselungsformen wie Transportverschlüsselung oder Datenträgerverschlüsselung keinen Zugewinn im Sinne der Vorgaben, da die Klardaten in aller Regel beim Exporteur verfügbar sind. Bestimmte Dienstleistungen funktionieren auch nur dann, wenn Klardaten vorliegen. Schlussendlich gilt darüber hinaus immer: Wer hat uns verraten? Meta-Daten! Die IP-Adresse und Endgerätedaten von Betroffenen sind bei vielen Diensten, Apps und Websites immer mit im Spiel.

In diesem Jahr ist Bewegung in die Sache gekommen, es gab einige Urteile und Entscheidungen zu Content-Delivery-Networks, zum Einsatz von Cloud-Diensten oder zu Schriftarten. Im Aufsichtsgeschäft war zum einen der Trend zu beobachten, dass einige Verantwortliche mehr oder weniger aus eigenem Antrieb auf die Integration von Dienstleistern aus dem außereuropäischen Ausland verzichten und diese Dienste entweder durch eigene Dienste oder rein europäisch agierende Dienstleister ersetzen. Zum anderen bemühen sich die außereuropäischen Dienstleister um technisch-organisatorische Loslösungen der europäischen Töchter. Oftmals steckt dann aber der Teufel im Detail. Es bedarf daher einer genauen Prüfung der vertraglichen Grundlagen. Nicht immer heißt „on premises" tatsächlich, dass alle Daten vollständig beim Verantwortlichen verbleiben.

Auch auf der oberen Ebene der Verhandelnden hat sich, zumindest was den transatlantischen Datenverkehr betrifft,

etwas getan. Die Executive Order zur US-Überwachung vom 7. Oktober 2022 soll die Urteile des Europäischen Gerichtshofs berücksichtigen und die EU-Kommission zu einem erneuten Angemessenheitsbeschluss bewegen. So hat die EU-Kommission am 13. Dezember 2022 das Verfahren zur Annahme eines Angemessenheitsbeschlusses für den Datenschutzrahmen EU-USA eingeleitet. Der Beschlussentwurf wurde veröffentlicht und dem Europäischen Datenschutzausschuss zur Stellungnahme übermittelt. Es ist davon auszugehen, dass der Angemessenheitsbeschluss trotz Kritik kommen wird. Es ist aber auch davon auszugehen, dass damit noch nicht alle offenen Fragen dauerhaft beantwortet sein werden.

Angemessenheitsentscheidung für den EU-USA-Datenschutzrahmen:
↗ sdb.de/tb2211

> „Auch wenn die Kommission einen Angemessenheitsbeschluss erlassen hat, muss die zuständige nationale Aufsichtsbehörde, an die sich eine Person mit einer Beschwerde bezüglich des Schutzes ihrer Rechte und Freiheiten bei der Verarbeitung ihrer personenbezogenen Daten wendet, daher in völliger Unabhängigkeit prüfen können, ob bei der Übermittlung dieser Daten die in der DSGVO aufgestellten Anforderungen gewahrt werden, und gegebenenfalls Klage vor den nationalen Gerichten erheben können, damit diese, wenn sie die Zweifel der Aufsichtsbehörde an der Gültigkeit des Angemessenheitsbeschlusses teilen, um eine Vorabentscheidung über dessen Gültigkeit ersuchen." (EuGH, Urteil vom 16.07.2020, Schrems II, C-311-18, Rdnr. 120)

6 Sächsische Datenschutzbeauftragte

6.1 Zuständigkeit und Anforderungen an Beschwerden

6.1.1 Die „einäugige" Kameraattrappe

↗ § 1 Abs. 1 Satz 2 BDSG, Art. 2 Abs. 1, Art. 58 Abs. 1 Buchst. a DSGVO

In einem kuriosen Fall einer Videoüberwachung wandte sich eine sächsische Gemeinde hilfesuchend an meine Behörde. Was war passiert? Der einzige Mieter eines Wohnhauses hatte auf der Fensterbank seiner Wohnung ein Gerät mit dem Aussehen einer Videokamera angebracht. Die Nachbarinnen und Nachbarn informierten die Gemeinde hierüber, da sie sich einer ständigen Beobachtung ausgesetzt sahen. Der Aufforderung der Gemeinde, die Videokamera zu entfernen, kam der Mieter allerdings nicht nach. So landete der Vorgang letztlich bei meiner Behörde.

Mir zugeleitete Aufnahmen der Fensterfront vermittelten den Eindruck, es könne sich bei dem kugelförmigen Objekt aufgrund des daran angebrachten Kabels um eine Videokamera handeln. Ich wandte mich daraufhin mit mehreren Schreiben an den Mieter, in dem ich diesen unter Verweis auf seine Auskunftspflicht meiner Behörde gegenüber (Art. 58 Abs. 1 Buchst. a Datenschutz-Grundverordnung {DSGVO}) um eine Stellungnahme bat. Obwohl der Mieter mir telefonisch eine schriftliche Mitteilung zusicherte, ließ er die Antwortfrist jedes Mal tatenlos verstreichen.

Eine unerwartete Wendung nahm der Fall dann, als ich plötzlich eine Mitteilung des zuständigen Polizeireviers erhielt. Dieses hatte den Mieter in der gleichen Angelegen-

heit aufgesucht und stellte dabei fest, dass es sich bei der vermeintlichen Kamera um das Porzellanauge einer Schaufensterpuppe (!) handelte. Kurzerhand nahm die Polizei das fragliche „Objekt" an sich und stieß dabei in der Wohnung auch auf mein letztes Schreiben an den Mieter. Dies erklärte, weshalb die Polizei von dem bei meiner Behörde anhängigen Vorgang erfuhr und mich überhaupt erst über die Beschaffenheit der „Kamera" informieren konnte.

Letztlich konnte ich den Sachverhalt ohne weitere Maßnahmen abschließen, da eine Attrappe, auch wenn es sich dabei um ein „Puppenauge" handelt, nicht in meine Kontrollzuständigkeit fällt. Denn anders als bei tatsächlich funktionsfähigen Videokameras, die aktiv betrieben werden, findet mit einer Kameraattrappe keine (automatisierte) Datenverarbeitung statt. Infolgedessen kommt das Datenschutzrecht auch nicht zur Anwendung, Art. 2 Abs. 1 DSGVO, § 1 Abs. 1 Satz 2 Bundesdatenschutzgesetz (BDSG).

Betroffenen Personen ist in Fällen eines von Kameraattrappen ausgehenden Überwachungs- und Anpassungsdrucks anzuraten, den Zivilrechtsweg zu beschreiten. Einzig darüber lassen sich je nach der Ausgestaltung des konkreten Einzelfalls Beseitigungs-, Unterlassungs- oder sogar Entschädigungsansprüche durchsetzen.

Was ist zu beachten?
Auf Kameraattrappen finden die Datenschutzvorschriften keine Anwendung. Bei diesen fehlt es an der tatsächlichen Verarbeitung personenbezogener Daten. Betroffene haben einzig die Möglichkeit, zivilrechtlich dagegen vorzugehen.

6.2 Zahlen und Daten zu den Tätigkeiten 2022

6.2.1 Überblick zu den Arbeitsschwerpunkten

Analog zu den Vorjahren verzeichnete meine Dienststelle 2022 bei Beschwerden/Kontrollanregungen und Beratungsanfragen die meisten Vorgänge – zusammen 42 Prozent. Weiterhin bildete die Zusammenarbeit mit den anderen deutschen Aufsichtsbehörden einen Schwerpunkt.

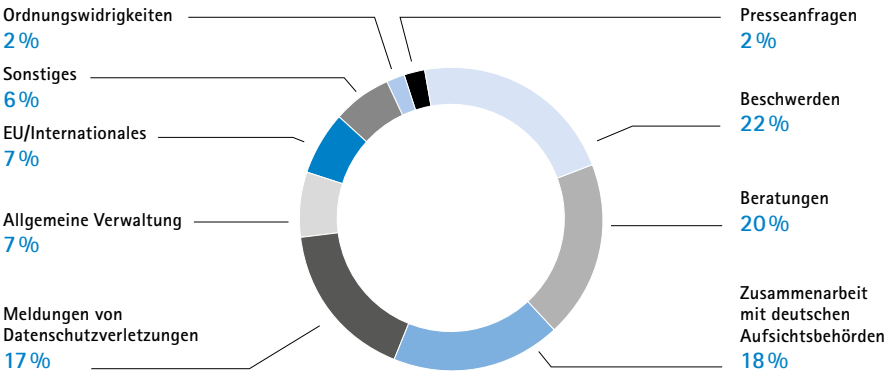
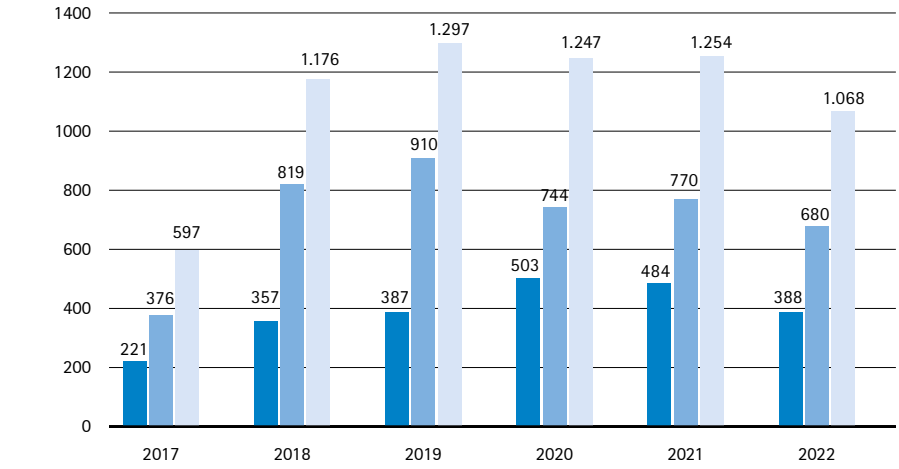


Abbildung 2:
Arbeitsschwerpunkte nach Anzahl der Vorgänge

6.2.2 Beschwerden und Kontrollanregungen

Meine Behörde erreichten im Berichtszeitraum insgesamt 1.068 Eingaben von betroffenen Personen und Hinweisgebern. Das Aufkommen lag damit unter dem der Vorjahre, aber weiterhin auf hohem Niveau. Ob das Jahr 2022 diesbezüglich eine Ausnahme oder sogar eine Trendumkehr darstellt, werden die kommenden Jahre zeigen. Auffällig ist, dass der Rückgang sowohl den öffentlichen als auch den nichtöffentlichen Bereich betraf.

Abbildung 3:
Beschwerden und Kontrollanregungen



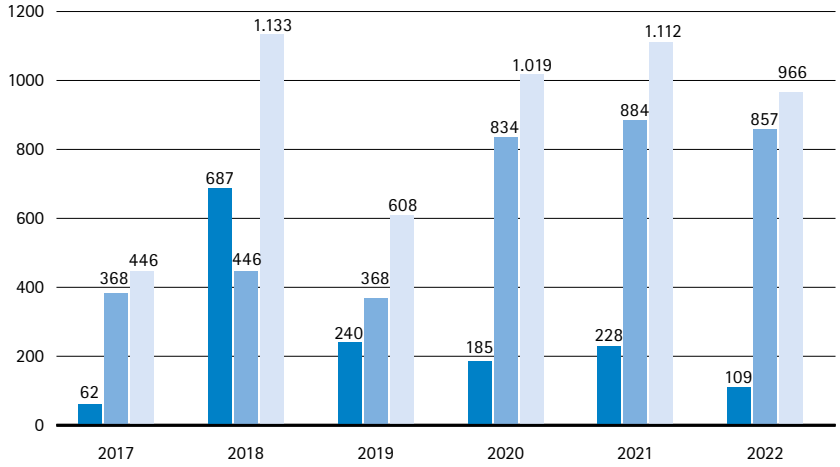


Abbildung 4:
Beratungen

- öffentlicher Bereich
- nichtöffentlicher Bereich
- Beratungen gesamt

6.2.3 Beratungen

Beratungen umfassen alle schriftlichen datenschutzrechtlichen Auskünfte gegenüber privaten und öffentlichen Stellen. Mit 966 Anfragen verzeichnete meine Behörde im Jahr 2022 etwas weniger Vorgänge als in den ersten zwei Corona-Jahren. Hinzu kam eine Vielzahl telefonischer Auskünfte, die statistisch nicht erfasst wurden. Der Rückgang bei den Beratungen betraf in erster Linie den nichtöffentlichen Bereich, im öffentlichen Bereich blieb der Bedarf unverändert hoch.

6.2.4 Meldungen von Datenpannen

Der Trend bei der Meldung von Datenschutzverletzungen gemäß Art. 33 Datenschutz-Grundverordnung (DSGVO) zeigt seit Jahren nach oben. Im Berichtszeitraum meldeten Verantwortliche insgesamt 809 Datenpannen. Das waren weniger als 2021 (923), jedoch deutlich mehr als in den Vorjahren. Neben der Registratur der Vorgänge sind die Meldungen auszuwerten und gegebenenfalls für eine aufsichtliche Nacharbeit zu kategorisieren. Einen statistischen Überblick und inhaltliche Details liefert der Beitrag 4.4.1.

6.2.5 Abhilfemaßnahmen

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

- Warnungen: 7
- Verwarnungen: 26
- Anweisungen und Anordnungen: 20
- Geldbußen (nur nach DSGVO): 16
- Widerruf von Zertifizierungen: 0

6.2.6 Zusammenarbeit mit europäischen Aufsichtsbehörden – Internal Market Information System

↗ Art. 56–67 DSGVO

Wie schon im letzten Tätigkeitsbericht 2021 (6.2.5, Seite 166) dargestellt, handelt es sich bei der Datenschutzaufsicht in der Europäischen Union um eine Verbundverwaltung im Mehrebenensystem (Kühling/Raab in: Kühling/Buchner, DS-GVO BDSG, 3. Auflage, 2020, A. Einführung Rdnr. 133). Deren Kommunikation findet über das „Internal Market Information System" (IMI) statt, wobei sich die deutschen Aufsichtsbehörden, teilweise koordiniert durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI), mitunter direkt äußern. Die Mitarbeit an IMI verlangt ein ständiges Monitoring, genaue Terminplanung und die Übersetzung der Beiträge ins Englische. Ich erhalte Benachrichtigungen zu denjenigen Verfahren, die an alle 45 europäischen staatlichen Aufsichtsbehörden in der EU gehen oder für die ich als Empfängerin von der sendenden Behörde ausgewählt wurde. Diese ständigen „notifications" vermitteln einen guten Überblick über das Geschehen in der Europäischen Union, etwa dass im Berichtszeitraum die Anzahl der endgültigen Beschlüsse stark gestiegen ist.
Wie schon im vorangegangenen Jahr habe ich mich an mehreren Verfahren beteiligt.

Im Berichtszeitraum meldete ich mich in einem Fall als federführende Aufsichtsbehörde gemäß Art. 56 Abs. 1 Datenschutz-Grundverordnung (DSGVO), allerdings im Rahmen eines Verfahrens der freiwilligen Amtshilfe, da gegen das Unternehmen, gegen das sich eine betroffene Person an „ihre" schwedische Aufsichtsbehörde gewandt hatte, noch ein anderes Verfahren in Sachsen anhängig war. Dafür bearbeitete die schwedische Partnerbehörde federführend eine Beschwerde gegen ein schwedisches Unternehmen, die in Sachsen erhoben worden war, in einem erneuten Verfahren nach Art. 61 DSGVO. Meine Behörde war insgesamt in sechs Verfahren die federführende Aufsichtsbehörde.

In zwei Fällen, in denen die Verantwortlichen Zweigniederlassungen in Sachsen hatten, erklärte ich mich nach sorgfältiger Prüfung der Voraussetzungen zur betroffenen Aufsichtsbehörde gemäß Art. 60 Abs. 1 DSGVO. Dies bedeutete vor allem, dass Entscheidungsentwürfe in diesen Verfahren von mir (mit-)geprüft werden und gegebenenfalls Einspruch eingelegt wird.

In einem Verfahren, in dem ein in Sachsen ansässiger Beschwerdeführer Beschwerde bei mir erhoben hatte und die an die Aufsichtsbehörde am einzigen Sitz des Unternehmens in der Europäischen Union abgegeben worden war, legte ich gegen den Bescheidentwurf erstmals einen maßgeblichen und begründeten Einspruch gemäß Art. 60 Abs. 4 DSGVO ein. Da sich mehrere deutsche Aufsichtsbehörden in diesem Verfahren für betroffen erklärt hatten, fiel mir nicht nur die Formulierung des Einspruchs zu, sondern auch die Koordinierung mit den übrigen deutschen Aufsichtsbehörden. Die federführende Aufsichtsbehörde setzte sich in einer informellen Konsultation nach Art. 60 DSGVO mit meinen Argumenten auseinander und riet zur Rücknahme des Einspruchs. Nach erneuter innerdeutscher Koordinierung wurde dieses Ansinnen im IMI zurückgewiesen. Derzeit findet eine weitere Sachverhaltsaufklärung statt, bevor dann ein überarbeiteter Beschlussentwurf gemäß Art. 60 Abs. 5 Satz 2 DSGVO von der federführenden Aufsichtsbehörde im IMI eingestellt werden wird.

Nicht immer geht es im IMI so kompliziert zu. Es gab auch einfache Anfragen in Zusammenhang mit grenzüberschreitenden Fällen und von allgemeiner Natur.

In zwei Verfahren nach Art. 61 DSGVO wurde ich von betroffenen Aufsichtsbehörden nach dem Sachstand der grenzüberschreitenden Fälle gefragt, damit diese ihrer Informationspflicht gemäß Art. 77 Abs. 2 DSGVO nachkommen konnten. Diese Anfragen habe ich pünktlich und ausführlich beantwortet.

In Rahmen von informellen Verfahren nach Art. 61 DSGVO stellen Aufsichtsbehörden auch allgemein interessierenden Fragen an die anderen „supervisory authorities". Manchmal möchte eine wissen, ob auch andere europäische Aufsichtsbehörden Mitteilungen von einer größeren Datenpanne eines grenzüberschreitend arbeitenden Unternehmens erhalten haben oder Beschwerden gegen eine Firma bearbeiten. Es können aber auch abstrakte Rechtsfragen an alle gerichtet werden. Häufig gelangen diese Anfragen gar nicht bis zu mir, da die Beantwortung vom BfDI koordiniert wird. In vier Verfahren habe ich solche Anfragen beantwortet, manche allerdings nur mit dem Hinweis, dass eine solche Datenpanne in Sachsen nicht gemeldet worden war.

Zahlenmäßig am häufigsten wird IMI zur Herstellung eines einheitlichen deutschen Standpunktes nach § 18 Bundesdatenschutzgesetz (BDSG) verwandt. Im Berichtszeitraum (Stand: 30.11.22) habe ich auf diese Weise in 19 Fällen dem vorgeschlagenen Vorgehen, zum Beispiel dem Entwurf eines Antwortschreibens des Europäischen Datenschutzausschusses (EDSA) oder der Stellungnahme des EDSA zu verbindlichen internen Datenschutzvorschriften nach Art. 47 DSGVO, zugestimmt.

6.2.7 Register der benannten Datenschutzbeauftragten

↗ Art. 37 Abs. 1 und 7 DSGVO

Im Berichtszeitraum gingen 994 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 Datenschutz-Grundverordnung (DSGVO) sieht gemäß Art. 37 Abs. 1 für den Verantwortlichen (öffentliche Stellen generell; nichtöffentliche Stellen unter bestimmten Voraussetzungen) die Pflicht vor, einen Datenschutzbeauftragten zu benennen. Nach Art. 37 Abs. 7 der 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.
Die übersandten Mitteilungen werden von den Fachreferaten meiner Behörde unter anderem genutzt, um die Erfüllung der Meldepflicht gemäß Art. 37 Abs. 7 DSGVO oder ein mögliches Vorliegen von Interessenskonflikten nach Art. 38 Abs. 6 DSGVO zu prüfen.

6.2.8 Förmliche Begleitung von Rechtsetzungsvorhaben

↗ Art. 36 Abs. 4 DSGVO

Nach Art. 36 Abs. 4 der Datenschutz-Grundverordnung (DSGVO) hat der Freistaat Sachsen mich bei der Ausarbeitung eines Gesetzentwurfs oder eines Rechtsverordnungsentwurfs, der die Verarbeitung personenbezogener Daten regelt, zu konsultieren. Im Berichtszeitraum hat meine Behörde daher etliche Rechtsetzungsvorhaben begleitet. Zumeist geschah dies bereits zu einem frühen Zeitpunkt, nämlich bei der Fertigung von Referentenentwürfen in den Staatsministerien.
Die im Jahr 2022 abgegebenen Stellungnahmen betrafen unter anderem die Novellierung des Sächsischen Wassergesetzes, das Sächsische Krankenhausgesetz, das Gesetz über die berufsständische Vertretung der Heilberufe im Freistaat Sachsen, das Gesetz zur Förderung des Einsatzes von Videokonferenztechnik in der Zivilgerichtsbarkeit und den

Fachgerichtsbarkeiten, die Änderung des Sächsischen Strafvollzugsgesetzes und die Überarbeitung von Verwaltungsvorschriften für Sportbetonte Schulen sowie den Bedarf und Schuljahresablauf 2023/2024.

Darüber hinaus 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 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 etwa im Bereich des Datenschutzes auch dann erschweren, wenn sie die Beteiligten als erforderlich ansehen.

Weiterhin beteiligten mich die Landtagsfraktionen regelmäßig bei der Erarbeitung von Gesetzentwürfen und Änderungsanträgen, so etwa bei der Kommunalrechtsnovelle oder beim Sächsischen Mietspiegel-Zuständigkeitsgesetz.

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

Zudem bezog ich Stellung zu verschiedenen Vorhaben, die im Zusammenhang mit der Bundesgesetzgebung standen und mit denen sich auch die Datenschutzkonferenz befasste.

6.2.9 Ressourcen

Im fünften Jahr der Datenschutz-Grundverordnung (DSGVO) sank die Anzahl der Beschwerden, Beratungen und Datenpannen-Meldungen nur leicht. Das Arbeitsaufkommen in diesen wichtigen Tätigkeitsbereichen meiner Behörde lag weiterhin auf einem hohen Niveau.

Dies wird besonders im Vergleich zur Anzahl der Fälle vor der Corona-Pandemie deutlich, die aufgrund des überdurchschnittlichen Aufkommens bei Eingaben bzw. Beratungsanfragen eine außergewöhnliche Belastungsprobe darstellte.

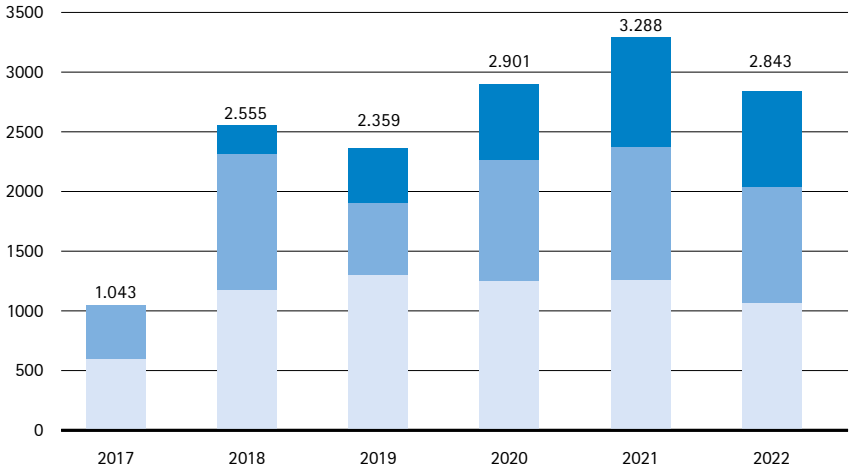


Abbildung 5:
Arbeitsaufkommen in wichtigen Tätigkeitsbereichen nach Anzahl der Vorgänge

- Meldungen von Datenpannen
- Beratungen
- Beschwerden

Die für die Erfüllung meiner Aufgaben erforderlichen Haushaltsmittel (Personal- und Sachausgaben) werden seit Inkrafttreten des Sächsischen Datenschutzdurchführungsgesetzes (SächsDSDG) vom 26. April 2018 im Einzelplan 13 des jeweiligen Staatshaushaltsplanes abgebildet.

Im Haushaltsjahr 2022 standen mir insgesamt 39 Stellen des Personalsolls A zur Verfügung. Die darunter im Doppelhaushalt 2021/2022 neu hinzugekommenen acht Stellen konnte ich bis zum Ende des Berichtszeitraumes alle besetzen.

Die Erfüllung meiner Aufgaben als Sächsische Datenschutzbeauftragte ist nach wie vor herausfordernd. Die Kapazitäten meiner Behörde werden durch reaktive Tätigkeiten absorbiert – die Bearbeitung von Beschwerden, die Begleitung von Rechtssetzungsvorhaben, die Koordinierung mit den übrigen Aufsichtsbehörden in der Europäischen Union und so weiter. Für die zwingend erforderliche Fähigkeit einer Aufsichtsbehörde, proaktiv zu kontrollieren und zu beraten, steht nach wie vor zu wenig Kapazität zur Verfügung.

Erfreulicherweise sind aus dem Doppelhaushalt 2023/2024 zwei Stellen für meine neue Aufgabe als Sächsische Transparenzbeauftragte verwendbar. Dafür danke ich. In meiner neuen Funktion werde ich ab dem 1. Januar 2023 für die Kontrolle der Einhaltung

des Sächsischen Transparenzgesetzes, die Bearbeitung von Petitionen, die Beratung der transparenzpflichtigen Stellen sowie die Erstattung von Gutachten und Berichten zuständig sein. Ich gehe davon aus, dass das Recht auf Informationszugang von den Bürgerinnen und Bürgern von Anfang an rege in Anspruch genommen werden wird und die ersten Beschwerden wegen der Verletzung des Transparenzanspruchs spätestens im Laufe des zweiten Quartals 2023 eingehen werden. Bereits vor Inkrafttreten des Gesetzes hatten sich noch im Berichtszeitraum transparenzpflichtige Stellen mit Fragen zur Umsetzung an mich gewandt. Mit der Übernahme dieser Aufgabe geht eine enge und inhaltlich anspruchsvolle Zusammenarbeit mit den Informationsfreiheitsbeauftragten der anderen Länder einher. Diese stimmen sich in der Konferenz der Informationsfreiheitsbeauftragten und des dazugehörigen Arbeitskreises regelmäßig ab.

Fortbildung von Beschäftigten

In meiner Dienststelle verfügt inzwischen ein weiterer Bediensteter über eine Qualifizierung zum Fachbegutachter der Deutschen Akkreditierungsstelle GmbH (DAkkS), der nationalen Akkreditierungsstelle der Bundesrepublik Deutschland mit Sitz in Berlin. Er ist damit zur Mitwirkung im Rahmen der Akkreditierung von Zertifizierungsstellen befähigt und erfüllt die Voraussetzungen zur Erteilung von Zertifikaten im Bereich des Datenschutzes nach der Datenschutz-Grundverordnung.

Des Weiteren nahmen mehrere Mitarbeiterinnen und Mitarbeiter an Veranstaltungen zur Internet- und Computersicherheit teil. Außerdem besuchten Bedienstete Fortbildungen unter anderem zur elektronischen Aktenführung, zum Prozessmanagement und zur Volks- und Betriebswirtschaftslehre.

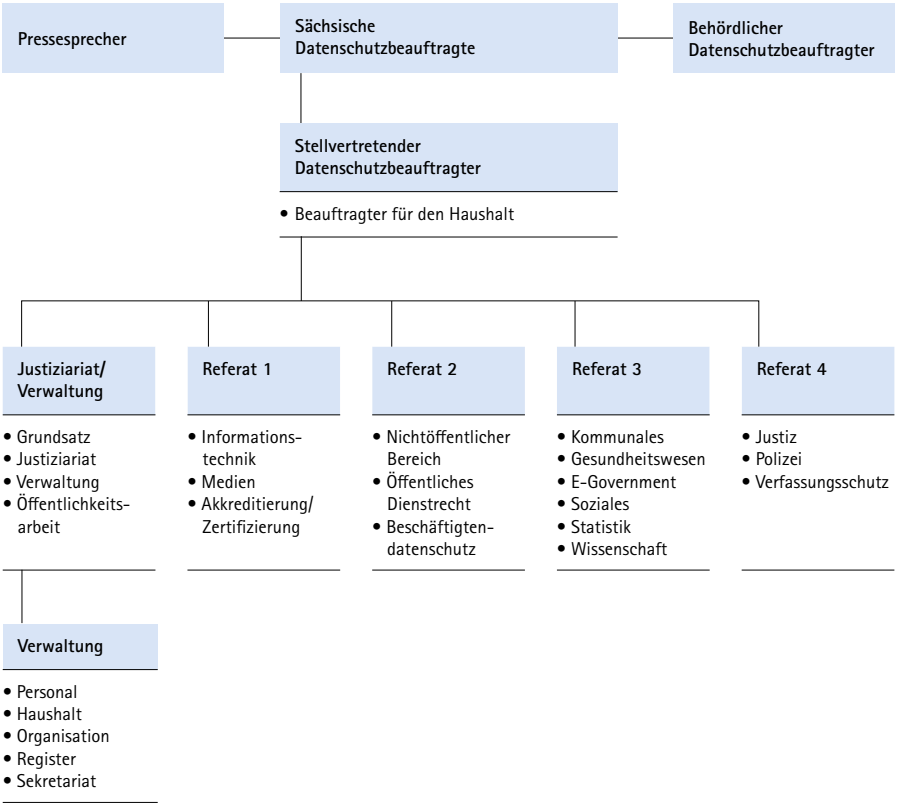


Abbildung 6:
Vereinfachtes Organigramm der Behörde (Stand: 31.12.2022)

6.3 Datenschutzaufsichtliche Befugnisse, verwaltungsrechtliche Entscheidungen

6.3.1 Zwangsgeldverfahren im nichtöffentlichen Bereich

↗ § 19 Abs. 5 SächsVwVG, § 40 Abs. 4 BDSG, § 92 Abs. 2 VwGO, Art. 30, 31 DSGVO

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

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

Soweit Verantwortliche dieser Kooperationspflicht nicht nachkommen bzw. davon ausgehen, sich durch Schweigen oder Nichtreagieren ihrer Pflicht zur Erteilung von Auskünften oder zur Bereitstellung von Unterlagen entziehen zu können, bleibt mir regelmäßig nur der Übergang ins förmliche Heranziehungsverfahren. Auskunftsheranziehungsbescheide (verbunden mit der Androhung eines Zwangsgeldes) sind insoweit ein adäquates und wirksames Mittel, um von Verantwortlichen, die mindestens zwei aufsichtsbehördliche Schreiben ignoriert haben oder die Auskunftserteilung aktiv verweigern, die zur Aufgabenerfüllung erforderlichen Auskünfte zu erhalten. Spätestens nach der Festsetzung eines Zwangsgeldes reagieren dann die meisten Verantwortlichen und stellen mir die geforderten Auskünfte und Unterlagen bereit. Im Berichtszeitraum habe ich sieben Zwangsgelder mit einer Gesamtsumme von 12.000 Euro festgesetzt. Verantwortliche, die meine zunächst formlosen Auskunftsersuchen ignoriert und anschließend auch nicht auf einen Heranziehungsbescheid reagiert haben, melden sich im Allgemeinen dann aber jedenfalls nach Erhalt des darauffolgenden Zwangsgeldbescheides. Zu diesem Zeitpunkt ist eine Klage gegen den Heranziehungsbescheid regelmäßig nicht mehr möglich, denn ein Zwangsgeldbescheid wird erst dann erlassen, wenn der vorangegangene Heranziehungsbescheid bereits bestandskäftig ist. Allerdings gibt es immer wieder

auch Ausnahmen, indem Verantwortliche glauben, dass die Angelegenheit mit der Zahlung des Zwangsgeldes für sie erledigt ist. Spätestens mit der Festsetzung eines weiteren Zwangsgeldes dürfte dieser Irrglaube dann aber ausgeräumt sein, denn auch mit der Zahlung eines Zwangsgeldes erlischt die Auskunftspflicht der verantwortlichen Stelle nicht. Nach § 19 Abs. 5 Sächsisches Verwaltungsvollstreckungsgesetz (SächsVwVG) dürfen Zwangsmittel wiederholt und so lange angedroht werden, bis der Verantwortliche seinen Verpflichtungen nachgekommen ist. Das Zwangsverfahren wird aber eingestellt, sobald die geforderten Auskünfte erteilt worden sind. Von zwei insoweit herausragenden Fällen möchte ich kurz berichten:

Videoüberwachung in einer Diskothek

Nach längerem, wenig ergiebigem und von zahlreichen Anträgen auf Fristverlängerung geprägtem Schriftverkehr mit einem anwaltlich vertretenen Diskothekenbetreiber hatte ich bereits 2021 einen Auskunftsheranziehungsbescheid erlassen. Nachdem als einzige Reaktion auf diesen Bescheid ein erneuter anwaltlicher Antrag auf Fristverlängerung zu verzeichnen war, habe ich das angedrohte Zwangsgeld festgesetzt und die Vollstreckung eingeleitet. Der Verantwortliche hat das Zwangsgeld dann schließlich bezahlt, darüber hinaus aber in keiner Weise reagiert.

Folgerichtig musste ich ein weiteres, doppelt so hohes Zwangsgeld festsetzen. Gegen den – sofort vollziehbaren – Festsetzungsbescheid hat der Bevollmächtigte des Verantwortlichen gerade noch rechtzeitig vor Eintritt der Bestandskraft Klage eingereicht und insbesondere auch Antrag auf Wiederherstellung der aufschiebenden Wirkung gestellt, verfiel danach aber wieder in sein altes Muster, indem er gegenüber dem Gericht zunächst einen Antrag auf Fristverlängerung stellte, sich danach aber nicht mehr meldete. Folgerichtig wurde der Antrag auf wiederherstellende Wirkung auch abgewiesen. Das Verwaltungsgericht hat dazu festgestellt, dass der Heranziehungsbescheid bestandskräftig, mit einer zutreffenden Rechtsmittelbelehrung versehen und

auch ordnungsgemäß zugestellt worden ist. Es sei auch nicht ersichtlich, dass der Bescheid nichtig sein könnte. Das betreffende (zweite) Zwangsgeld sei unter angemessener Fristsetzung angedroht und schriftlich festgesetzt worden. Bis zum Zeitpunkt der gerichtlichen Entscheidung sei der Verantwortliche seiner Pflicht zur Vornahme der geschuldeten Handlung, nämlich der Auskunftserteilung gemäß der Regelungen im ursprünglichen Heranziehungsbescheid, nicht nachgekommen.

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

Im Ergebnis blieb mir jetzt nichts weiter übrig, als nun erneut ein weiteres, wiederum doppelt so hohes Zwangsgeld festzusetzen. Auch gegen diesen Festsetzungsbescheid hat der Bevollmächtigte Klage erhoben. Ich werde im nächsten Tätigkeitsbericht über den Fortgang in dieser Angelegenheit berichten. Ergänzend prüfe ich die parallele Einleitung eines Bußgeldverfahrens.

Vorlage des Verarbeitungsverzeichnisses

In einem Aufsichtsverfahren gegen einen Pizza-Lieferdienst war zuletzt lediglich noch die Vorlage des Verzeichnisses der Verarbeitungstätigkeiten offen. Nach Art. 30 Abs. 4 DSGVO hat ein Verantwortlicher das Verzeichnis auf Anfrage der Aufsichtsbehörde zur Verfügung zu stellen. Nachdem der diesbezüglich erlassene Heranziehungsbescheid keine Wirkung gezeigt hatte, hatte ich zunächst ein Zwangsgeld angedroht und anschließend auch festgesetzt. Auf die Ankündigung der Vollstreckung hin wurde zwar das Zwangsgeld bezahlt, allerdings kein Verarbeitungsverzeichnis übersandt.

Ich hatte daher die Vermutung, dass der Verantwortliche gar kein solches Verzeichnis erstellt hatte und nun irrigerweise davon ausging, durch Bezahlung des Zwangsgeldes die Vorlagepflicht gegenüber der Aufsichtsbehörde aus der Welt zu schaffen. Ich musste daher auch hier ein zweites, nunmehr doppelt so hohes Zwangsgeld festsetzen, welches nun aber die erhoffte Wirkung zeigte. Zwar bestand diese (noch) nicht in der geforderten Vorlage des Verarbeitungsverzeichnisses, jedoch bestand nunmehr Hoffnung, dass ein solches Verzeichnis erstmalig erstellt und mir sodann vorgelegt würde. Denn ich erhielt von einer Mitarbeiterin des Verantwortlichen zunächst die Information, dass das Unternehmen eine externe Datenschutzbeauftragte hinzugezogen habe, die mich alsbald auch selbst kontaktierte und auf den – von ihr festgestellten – erheblichen datenschutzrechtlichen Handlungsbedarf im Unternehmen hinwies. Offensichtlich war das Thema Datenschutz bei diesem Pizza-Lieferdienst bislang vollkommen ignoriert worden. Die neu benannte Datenschutzbeauftragte sicherte mir die kurzfristige Vorlage eines ersten groben Entwurfs des Verarbeitungsverzeichnisses zu und kündigte an, im Unternehmen auf ein adäquates Datenschutzmanagement hinwirken zu wollen. Vor diesem Hintergrund habe ich von weiteren Zwangsmaßnahmen zunächst Abstand genommen.

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

Zwangsgelder auch gegen öffentliche Stelle möglich

Bei den im Jahr 2022 festgesetzten Zwangsgeldern waren ausschließlich nichtöffentliche Stellen betroffen. Aber auch gegen öffentliche Stellen kann bei Auskunftsverweigerung ein Zwangsgeld verhängt werden, siehe Tätigkeitsbericht 2021, 6.3.2., Seite 176f.

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 alte Fassung),
- § 22 Abs. 1 Sächsisches Datenschutzdurchführungsgesetz (§ 22 Abs. 3 SächsDSDG),
- § 48 Abs. 1 Sächsisches Datenschutz-Umsetzungsgesetz (§ 48 Abs. 3 Satz 1 SächsDSUG),
- Art. 83 Datenschutz-Grundverordnung (Art. 58 Abs. 2 Buchst. i DSGVO, § 14 Abs. 1 SächsDSDG) und
- § 85a Zehntes Buch Sozialgesetzbuch – Sozialverwaltungsverfahren und Sozialdatenschutz – in Verbindung mit § 41 Bundesdatenschutzgesetz, Art. 83 Abs. 5 Datenschutz-Grundverordnung (Art. 58 Abs. 2 Buchst. i DSGVO, § 14 Abs. 1 SächsDSDG).

Im Berichtszeitraum waren im öffentlichen Bereich insgesamt 74 Bußgeldverfahren anhängig. Davon wurden 18 mit einem Bußgeld abgeschlossen. In 36 Verfahren erfolgte eine Einstellung bzw. wurde von der Verfolgung abgesehen. In einem Verfahren wurde eine Verwarnung ohne Verhängung eines Verwarngeldes ausgesprochen, ein Verfahren wurde an die zuständige Behörde abgegeben. 18 Verfahren befanden sich zum Ende des Berichtszeitraumes noch in Bearbeitung. In zwei Verfahren aus dem vorangegangenen Berichtszeitraum erging im Jahr 2022 eine Entscheidung vor dem Amtsgericht.

Berichtszeitraum		01.01.–31.12.2022
anhängig gesamt		**74**
davon	Verfahren aus vorherigem Berichtszeitraum	56
	neu eingegangene Verfahren	18
abgeschlossen		**56**
davon	mit Bußgeld	18
	mit Verwarnungsgeld	0
	mit Verwarnung ohne Verwarnungsgeld	1
	eingestellt/von Verfolgung abgesehen	36
	an zuständige Behörde abgegeben	1
noch in Bearbeitung		**18**
Summe festgesetzter Buß- und Verwarnungsgelder in Euro		**17.310**

Tabelle 1:
Ordnungswidrigkeiten-verfahren im öffentlichen Bereich

Die Summe der rechtskräftig festgesetzten Buß- und Verwarngelder belief sich auf 17.310 Euro. Der starke Anstieg dieser Summe im Vergleich zum vergangenen Berichtszeitraum ist auf in Einzelfällen sehr hohe Bußgelder zurückzuführen.

Gegenüber dem vergangenen Berichtszeitraum ist die Zahl der neu eingegangenen Ordnungswidrigkeitenverfahren zurückgegangen. Daher konnten im Vergleich zum Berichtszeitraum 2021 wesentlich mehr Verfahren zügig abgeschlossen werden.

Die mitunter ungünstig langen Bearbeitungszeiten während der Corona-Pandemie konnten im Berichtszeitraum wieder verkürzt werden. Ab Eingang der Anzeige wird ein Verfahrensabschluss nach spätestens sechs Monaten angestrebt.

Erneut standen beziehungsweise stehen in einem Großteil (ca. 75 Prozent) der Ordnungswidrigkeitenverfahren Bedienstete der sächsischen Polizei in Verdacht, unbefugt personenbezogenen Daten in ihnen ausschließlich für dienstliche Zwecke zur Verfügung stehenden, nicht allgemein zugänglichen

elektronischen Informationssystemen abgerufen bzw. personenbezogene Daten in diesem Zusammenhang unerlaubt verarbeitet zu haben.

Des Weiteren bestand/besteht gegenüber Bediensteten unterschiedlichster sächsischer (Sozial-)Behörden der Verdacht, nicht offenkundige personenbezogene Daten unbefugt verarbeitet zu haben.

Bei den im Berichtszeitraum mit einem rechtskräftigen Bußgeld abgeschlossenen Verfahren handelte es sich fast ausschließlich um unbefugte Abrufe nicht offenkundiger personenbezogener Daten aus den polizeilichen Datenbanken (§ 38 Abs. 1 Nr. 1 a SächsDSG alte Fassung bzw. § 48 Abs. 1 Nr. 1 SächsDSUG), und/oder unbefugte Verarbeitungen nicht offenkundiger personenbezogener Daten (§ 38 Abs. 1 Nr. 1 a SächsDSG alte Fassung bzw. § 48 Abs. 1 Nr. 1 SächsDSUG) durch Polizeivollzugsbedienstete.

Der anhaltend große Anteil von Ordnungswidrigkeitenverfahren gegen sächsische Polizeibedienstete deutet darauf hin, dass nach wie vor Unklarheiten im Zusammenhang mit der Nutzung polizeilicher Datenbanken bestehen. Regelmäßig handelt es sich um privat motivierte Datenabrufe aus den polizeilichen Auskunfts- bzw. Informationssystemen zu befreundeten oder benachbarten Personen, Kolleginnen und Kollegen, anderen Bekannten oder auch zu Personen des öffentlichen Lebens. Wie bereits in vorangegangenen Tätigkeitsberichten ausführlich erläutert, dürfen im gesamten Polizeivollzugsdienst nur die personenbezogenen Daten verarbeitet werden, die zur Erfüllung seiner Aufgaben erforderlich sind (§ 53 Sächsisches Polizeivollzugsgesetz {SächsPVDG}) in Verbindung mit § 3 SächsDSUG). Somit ist auch die/der einzelne Polizeibedienstete nur berechtigt, die zur Erfüllung ihrer/seiner konkreten dienstlichen Aufgabe erforderlichen Daten zu verarbeiten. Eine dienstliche Befugnis und Notwendigkeit sind zwingende Voraussetzungen für jede Verarbeitung und für jeden Abruf von personenbezogenen Daten aus den polizeilichen Datenbanken. Es wäre im Übrigen lebensfremd und abwegig anzunehmen, dass Polizeibedienstete ernsthaft davon ausgehen könnten, es

sei zulässig, sich ohne dienstliche Veranlassung mittels Abfragen in polizeilichen Dateien etwa darüber zu informieren, ob befreundete oder bekannte Personen in polizeilichen Verfahren erfasst sind, nur weil derartige Recherchen in den polizeilichen Datenbanken technisch möglich sind. Auch „Eigenrecherchen" stellen regelmäßig eine Ordnungswidrigkeit dar. Hintergrund ist der Umstand, dass der Bedienstete auch in dieser Konstellation unbefugt nicht offenkundige Daten abruft (auf das Eigeninteresse oder eine Art „naturgemäße" Einwilligung kommt es nicht an, vgl. Oberlandesgericht Bamberg, Beschluss vom 27.04.2010, Aktenzeichen 2 Ss 531/10) und sich in den zum Vorgang gespeicherten Unterlagen in aller Regel Daten zu Dritten finden (Anzeigeerstatterinnen bzw. -erstatter, Verdächtige, Geschädigte, Zeuginnen bzw. Zeugen etc.). Persönliche Neugier bzw. eine private Motivation ersetzen auch hier nicht die zum Verarbeiten und/oder Abrufen nicht offenkundiger personenbezogener Daten erforderliche dienstliche Befugnis. Der einzig gesetzkonforme Weg für die Beschuldigten, über ein laufendes Verfahren Auskunft bzw. Einsicht in die Unterlagen zu erhalten, ist und bleibt im Ermittlungsverfahren derjenige über § 147 Strafprozessordnung (StPO). Die Staatsanwaltschaft entscheidet über Auskunft bzw. Einsicht. Die (beschuldigten) Polizeibediensteten sind insoweit ganz „normale" Verfahrensbeteiligte. Über die zu ihrer/seiner Person gespeicherten Daten – unabhängig von eventuell laufenden Verfahren – erhält sie/er nach § 92 SächsPVDG und § 57 BDSG Auskunft.

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. Die Ahndung von Ordnungswidrigkeiten im öffentlichen Bereich ist daher nach wie vor unerlässlich, um die Bediensteten der Behörden und öffentlichen Stellen in Sachsen auch künftig zu ihrer besonderen Pflichtenwahrung und Vorbildwirkung zu ermahnen.

6.4.2 Ordnungswidrigkeitenverfahren im nichtöffentlichen Bereich

↗ Art. 58, 83 DSGVO, OWiG

Im Berichtszeitraum hatte ich 71 neue Ordnungswidrigkeitenanzeigen zu verzeichnen – die Anzahl bewegte sich damit geringfügig unter dem Niveau des Vorjahres. Wie bereits im vergangenen Jahr bezogen sich etwa zwei Drittel der Anzeigen (47) auf die Anfertigung von Videoaufnahmen (stationäre Kameras [27], Dashcams [13], Handy- und Fotoaufnahmen [7]). Damit liegt der Schwerpunkt (66 Prozent) der bei mir eingegangenen Ordnungswidrigkeitenanzeigen auch weiterhin klar bei der Videoüberwachung (Vorjahr: 64 Prozent).
Insgesamt waren damit im Berichtszeitraum 205 Ordnungswidrigkeitenverfahren bei mir anhängig. Von diesen konnte ich 135 Fälle abschließen und habe dabei 16 Bußgelder festgesetzt.

Tabelle 2:
Ordnungswidrigkeitenverfahren im nichtöffentlichen Bereich

Berichtszeitraum		**01.01.–31.12.2022**
anhängig gesamt		**205**
davon	Verfahren aus vorherigem Berichtszeitraum	134
	neu eingegangene Verfahren	71
abgeschlossen		**135**
davon	mit Bußgeld	16
	eingestellt/von Verfolgung abgesehen	119
noch in Bearbeitung		**70**
Summe festgesetzte Bußgelder in Euro		**11.600**

Neun Bußgelder habe ich wegen eines rechtswidrigen Einsatzes von Dashcams festgesetzt; ihre Höhe bewegte sich zwischen 200 Euro und 1.000 Euro. Die verbleibenden Bußgelder betrafen den Betrieb stationärer Videokameras (4),

Internetveröffentlichungen (2) sowie einen Verstoß gegen die Auskunftspflicht des Art. 15 Datenschutz-Grundverordnung (DSGVO).

Bei den stationären Videokameras handelte es sich in zwei Fällen um Wildkameras. Zum einen hatte ein Fahrzeugbesitzer eine solche Kamera im öffentlichen Verkehrsraum am Mast einer Straßenlampe angebracht, um – nach einer vorangegangenen Sachbeschädigung – den regelmäßigen Stellplatz seines Pkw zu überwachen; zum anderen hatte eine Grundstückseigentümerin über ihrer Hofeinfahrt eine Wildkamera angebracht, weil sie sich durch das ständige Gebell des Hundes ihrer auf der gegenüberliegenden Straßenseite wohnenden Nachbarn belästigt gefühlt hatte. Der dritte Fall betraf ein im Eigentum einer Wohnungseigentümergemeinschaft stehendes Wohn- und Geschäftshaus; dort hatte einer der Eigentümer nach verschiedenen Auseinandersetzungen mit Miteigentümern den Hauseingang sowie den vor dem Gebäude befindlichen Verkehrsraum überwacht (vgl. dazu 6.4.4). Schließlich habe ich noch den Einsatz einer Bauüberwachungskamera auf einem Privatgrundstück mit einem Bußgeld geahndet. Mit dieser Kamera waren zum einen die Mitarbeiterinnen und Mitarbeiter der dort tätigen Baufirmen, zum anderen aber auch Nachbarinnen und Nachbarn oder Passantinnen und Passanten auf den umliegenden öffentlichen Verkehrswegen erfasst worden.

Bei einem der beiden wegen unzulässiger Veröffentlichung im Internet festgesetzten Bußgelder handelte es sich um einen sogenannten Mitarbeiterexzess, der seinen Ursprung in einer Videoüberwachung des betreffenden Arbeitgebers, eines Einzelhändlers für Arbeitsschutzbekleidung, hatte. Bedienstete eines staatlichen „Kontrollteams zur Einhaltung der Corona-Schutz-Bestimmungen" hatten sich dort Teile ihrer Ausrüstung beschafft. Ein Mitarbeiter hatte dies erkannt und Screenshots dieser Personen aus der hauseigenen Überwachungsanlage im Pausenraum ausgelegt, angeblich um die Kollegen und Kolleginnen in Bezug auf die Einhaltung der Corona-Schutzmaßnahmen zu sensibilisieren und ihnen zu demonstrieren, dass tatsächlich mit diesbezüglichen

staatlichen Kontrollen zu rechnen sei. Wenig später tauchten diese Fotos dann mit entsprechenden Kommentaren in Sozialen Medien auf. Meine Ermittlungen haben ergeben, dass eine Mitarbeiterin diese Screenshots mit ihrem Smartphone abfotografiert und an einen Bekannten weitergeleitet hatte. Ab diesem Zeitpunkt war die weitere Verbreitung dieser Fotos weder für sie noch für ihren Arbeitgeber noch in irgendeiner Weise zu kontrollieren bzw. zu unterbinden.
Neben den oben genannten Bußgeldern habe ich in 26 Fällen noch datenschutzrechtliche Verwarnungen ausgesprochen (vgl. Art. 58 Abs. 2 Buchst. b DSGVO).

6.4.3 Personenverwechslung im Bußgeldverfahren

↗ OWiG

Im letzten Tätigkeitsbericht hatte ich unter 6.4.2 ein Bußgeldverfahren gegen den ehemaligen Inhaber eines Fitnessstudios erwähnt, der sich über Facebook öffentlich für das verspätete Öffnen seines damaligen Studios entschuldigt hatte, dabei aber die Schuld zugleich unter Offenlegung weiterer personenbezogener Daten auf einen namentlich benannten Mitarbeiter abgewälzt und diesen somit gegenüber den Clubmitgliedern bloßgestellt und angeprangert hatte, vgl. auch Tätigkeitsbericht 2021, Seite 182.
Nachdem das Bußgeldverfahren ohne Einwendungen, sogar ohne irgendeine Reaktion des Betroffenen erfolgt und der Bußgeldbescheid erlassen und rechtskräftig geworden war, aber der Betroffene weiterhin keine Reaktion zeigte, waren seitens meiner Behörde entsprechende Vollstreckungsmaßnahmen einzuleiten. Es folgte eine Mahnung und anschließend die Ankündigung der Vollstreckung. In dieser Phase wachte der Betroffene dann aber doch (erstmalig) auf und machte geltend, dass er den Verstoß nicht begangen habe. Es liege ein Irrtum, was die Identität seiner Person angehe, vor.
Die daraufhin durch die Verwaltungsbehörde bei der Gewerbeaufsicht sowie im Einwohnermelderegister geführten ergänzenden Ermittlungen bestätigten schließlich diesen Vor-

halt. Tatsächlich gab es eine namensgleiche Person, die etwa gleichaltrig, allerdings in einem anderen Ort wohnhaft war. Im vorliegenden Ermittlungsverfahren war der Betroffene bereits durch die Polizei ermittelt und als Betroffener ausgewiesen worden. Es stellt sich die Frage, weshalb dieser im Laufe des Verfahrens weder auf Anschreiben bzw. Anhörungen der Polizei noch solche der Verwaltungsbehörde reagiert hatte. Selbst den gegen ihn erlassenen Bußgeldbescheid hat er akzeptiert. Dieser war damit zwar formell rechtskräftig, vor dem dargestellten Hintergrund aber möglicherweise nichtig. Eine Rücknahmemöglichkeit für die Verwaltungsbehörde (nach Rechtskraft) sieht das Gesetz indes nicht vor. Allerdings kann und sollte in so einem Fall von der Vollstreckung abgesehen werden, was seitens meiner Dienststelle auch so praktiziert worden ist.

Da die Verjährung (Verjährungsfrist: 3 Jahre) vorliegend noch nicht eingetreten war, konnte die Verfolgung der Ordnungswidrigkeit nun gegenüber dem tatsächlichen Betroffenen nochmals aufgenommen und schließlich auch – ohne weitere Überraschungen – zu einem vergleichbaren Abschluss gebracht werden.

Was ist zu tun?
Wird man zu Unrecht einer Ordnungswidrigkeit bezichtigt, sollte man frühzeitig reagieren und der Ordnungswidrigkeitenbehörde umgehend Entsprechendes mitteilen.

6.4.4 Durchsuchung als adäquate Ermittlungsmaßnahme bei unzulässigem Betrieb von Videokameras

↗ § 40 BDSG, Art. 13 GG, OWiG, StPO

In den Tätigkeitsberichten wurde im Zusammenhang mit Ordnungswidrigkeitenverfahren immer wieder auch von durchgeführten Durchsuchungen berichtet. Dabei sollte deutlich geworden sein, dass eine solche Ermittlungsmaßnahme nur im Ausnahmefall angewendet wird, denn damit wird regelmäßig in das Grundrecht der Unverletzlichkeit der Wohnung (Art. 13 Abs. 1 Grundgesetz {GG}) eingegriffen, was natürlich einer besonderen Begründung bedarf. Höchstrichterlich geklärt ist, dass durch dieses Grundrecht ebenso beruflich genutzte Räume geschützt werden. Gleichwohl ist eine Durchsuchung häufig die letzte verbleibende Aufklärungs-

möglichkeit. Alternativ verbleibt meist nur die Verfahrenseinstellung wegen eines nicht zu führenden Tatnachweises. Generell gilt aber, dass im Ordnungswidrigkeitenverfahren von Durchsuchungsmaßnahmen zurückhaltender Gebrauch gemacht werden soll, da hier das staatliche und auch das öffentliche Interesse geringer als im Strafverfahren einzuschätzen ist. Hat eine Ordnungswidrigkeit nur geringe Bedeutung, ist eine Durchsuchung also unverhältnismäßig. Die Anforderungen an die Stärke des Tatverdachts müssen demnach umso größer sein, je weniger schwer die dem Betroffenen zur Last gelegte Tat wiegt.

Gerade im Bereich der Videoüberwachung gehen die Meinungen über die Bedeutung diesbezüglicher Ordnungswidrigkeiten – und damit natürlich auch über die Zulässigkeit von Durchsuchungshandlungen – regelmäßig sehr stark auseinander. Für die einen, an die zunehmende Verbreitung videoüberwachter Bereiche bereits Gewöhnte oder an der Videoüberwachung Interessierte, sind unzulässige Videoüberwachungen lediglich geringfügige Verstöße; für die anderen, von einer Videoüberwachung und dem davon ausgehenden Überwachungsdruck permanent betroffene Personen, stellen sie äußerst starke Eingriffe in ihr Persönlichkeitsrecht dar. Vor dem Hintergrund, dass sich alle bisher erwirkten Durchsuchungsbeschlüsse auf Videoüberwachungsfälle bezogen haben, kommt damit den erforderlichen richterlichen Entscheidungen zur Anordnung und Zulässigkeit einer Durchsuchungsmaßnahme besondere Bedeutung zu.

Die erste und wesentliche von der eine Durchsuchungsmaßnahme planenden Verwaltungsbehörde zu überwindende Schwelle ist die Erlangung eines richterlichen Durchsuchungs- und Beschlagnahmebeschlusses. Gelingt es an dieser Stelle nicht, die Untersuchungsrichterin bzw. den Untersuchungsrichter am Amtsgericht von der Notwendigkeit und Zweckmäßigkeit eines solchen Beschlusses zu überzeugen, verbleibt abgesehen von einem diesbezüglichen Beschwerdeverfahren regelmäßig nur die Verfahrenseinstellung. Weitere Ermittlungsansätze zur Erhärtung des Tatverdachts mit dem Ziel eines erneuten Antrags auf Erlass eines solchen

Beschlusses sind meist nicht gegeben. Während der oder die Betroffene während der Durchsuchung praktisch keine Möglichkeit hat, den Vollzug des Durchsuchungsbeschlusses zu stoppen, steht es ihm aber frei, im Anschluss Beschwerde beim Amtsgericht zu erheben. Wird dieser Beschwerde durch das Amtsgericht nicht abgeholfen, legt dieses die Beschwerde dem Landgericht zur Entscheidung vor. Dessen Entscheidung hat zweifelsfrei eine besondere Bedeutung für die Verwaltungsbehörde; zum einen bestätigt (oder verneint) sie die Zulässigkeit und damit die Verhältnismäßigkeit der Durchsuchungsmaßnahme in dem konkreten Verfahren, zum anderen ist sie auch bedeutend für andere ähnlich gelagerte Verfahren und damit für die Grundsatzfrage, ob und wann für eine Bußgeldbehörde – beim (möglicherweise rechtswidrigen) Einsatz von Videokameras – eine Durchsuchung überhaupt als Ermittlungsmaßnahme in Betracht kommt.
Im Berichtszeitraum hat es diesbezüglich zwei insoweit richtungsweisende Beschwerdeverfahren gegeben, in denen das Landgericht Dresden zum einen eine Durchsuchung von Gewerberäumen und zum anderen von Wohnräumen als zulässig bewertet hat:

Durchsuchung von Gewerberäumen

Der Betroffene war Mitglied in einer Wohnungseigentümergesellschaft eines Wohn- und Geschäftshauses. In seinem Sondereigentum befanden sich die gastronomisch genutzten Geschäftsräume im Erdgeschoss. Ein Miteigentümer hatte ihn wegen des Betriebs einer Videokamera angezeigt. Diese Kamera war in einem neben der Hauseingangstür befindlichen Fenster eines Nebenraums aufgestellt und erfasste offensichtlich die davor befindlichen Parkflächen, den kompletten Hauseingang, den Zugang zu den außerhalb befindlichen Briefkästen sowie mutmaßlich auch vor dem Grundstück befindliche öffentliche Verkehrsbereiche. Den daraufhin vor Ort im Auftrag meiner Behörde ermittelnden Polizeibeamten hatte der (nicht anwesende, sondern nur telefonisch durch einen Mitarbeiter kontaktierte) Betroffene nicht erlaubt, den tatsächlichen Erfassungsbereich der Kamera mittels einer

Durchsicht der darin enthaltenen Speicherkarte zu überprüfen. Monitore existierten nicht; die Kamerabilder waren nur über das Smartphone des Betroffenen einsehbar. Im Rahmen der Anhörung hatte er sich lediglich per E-Mail gemeldet, die Vorwürfe abgestritten und eine schriftliche Äußerung angekündigt, diese aber nie eingereicht.

Auf meinen Antrag hin ordnete das Amtsgericht Dresden die Durchsuchung der Geschäftsräume des Betroffenen zum Zwecke der Beschlagnahme der auf Bereiche außerhalb des Gebäudes gerichteten Überwachungskamera einschließlich darin befindlicher Speichermedien an. Nach der Durchsuchung legte der anwaltlich vertretene Betroffene Beschwerde gegen den Durchsuchungsbeschluss ein. Das Amtsgericht Dresden hat der Beschwerde nicht abgeholfen und den Vorgang dem Landgericht Dresden zur Entscheidung vorgelegt. Dieses hat die zulässige Beschwerde als unbegründet verworfen und festgestellt, dass der angegriffene Beschluss rechtmäßig war und den Betroffenen insbesondere nicht in seinem Grundrecht aus Art. 13 Abs. 1 GG (Unverletzlichkeit der Wohnung) verletzt. Im Wesentlichen wurden dafür folgende Gründe angeführt:

Die bestehenden Verdachtsgründe gingen über vage Anhaltspunkte und bloße Vermutungen hinaus; der Verdacht einer Ordnungswidrigkeit gründete sich nicht nur auf die Aussage einzelner Personen einschließlich des Betroffenen selbst. Die Kamera war von außen für alle ersichtlich im Fensterbereich aufgestellt und in den Außenbereich ausgerichtet.

Die Durchsuchungsanordnung war auch verhältnismäßig. Die Anordnung der Durchsuchung war geeignet, um sowohl die Funktionstüchtigkeit als auch den Erfassungsbereich der Überwachungskamera zu ermitteln, und sie war zur Ermittlung und Verfolgung der vorgeworfenen Ordnungswidrigkeit auch erforderlich. Ein anderes erfolgversprechendes, weniger einschneidendes Mittel stand nicht zur Verfügung, zumal der Betroffene im Vorfeld der Durchsuchung eine Überprüfung des Erfassungsbereiches der Überwachungskamera durch die Ermittlungsbeamten ausdrücklich untersagt hatte. Die Durchsuchungsanordnung war zudem verhältnismäßig

im engeren Sinne. Im Hinblick darauf, dass es sich bei der Tat lediglich um eine Ordnungswidrigkeit handelt, war die Maßnahme angemessen im Verhältnis zur Schwere der Tat. Die Überwachungskamera ist potenziell geeignet gewesen, permanent und ohne besonderen Anlass eine Vielzahl an Personen – sowohl Bewohnerinnen und Bewohner oder Besucherinnen und Besucher des Wohn- und Geschäftshauses als auch Verkehrsteilnehmerinnen bzw. Verkehrsteilnehmer in den vor dem Gebäude befindlichen öffentlichen Verkehrsbereichen – unbemerkt zu überwachen und entsprechende Aufnahmen zu speichern. Hierdurch wird in erheblicher Weise in die allgemeinen Persönlichkeitsrechte Dritter eingegriffen, ohne dass dem erkennbar ein hinreichend gewichtiges Interesse des Betroffenen an der Videoüberwachung gegenüberstünde.

Bleibt zum Abschluss noch das Ergebnis der Durchsuchung nachzutragen. In der Tat konnte dem Betroffenen nach Auswertung der Speicherkarte eine unzulässige Videoüberwachung der Parkflächen, des Hauseinganges sowie auch des öffentlichen Verkehrsraums über einen Zeitraum von zehn Tagen vor dem Durchsuchungstermin nachgewiesen werden – mehr hatte die Kapazität der Speicherkarte nicht erlaubt. In den Videoaufnahmen war auch sichtbar, wie die Mitarbeiter der Verwaltungsbehörde zunächst am Grundstück vorbeigefahren waren und sich anschließend dort mit den Vertreterinnen und Vertretern von Polizei und Ordnungsamt getroffen hatten. Nachdem der Betroffene anfangs nicht vor Ort angetroffen, dann aber telefonisch über die Ermittlungsmaßnahme unterrichtet werden konnte und sein Eintreffen abgewartet worden war, war in den Videoaufnahmen auch ersichtlich, dass sich genau ab dem Zeitpunkt der telefonischen Unterrichtung der Erfassungsbereich der Videokamera wie von Geisterhand gesteuert automatisch verändert und fortan nur noch der Bereich unmittelbar vor dem Fenster aufgenommen wurde.

Durchsuchung von Wohnräumen

Dem betreffenden Ordnungswidrigkeitenverfahren war zunächst ein Aufsichtsverfahren vorangegangen. Mir lag eine Beschwerde vor, die unter anderem eine auf einem circa drei Meter hohen Mast auf dem Balkon eines Wohnanwesens angebrachte Videokamera mit Ausrichtung auch auf öffentliche Verkehrsbereiche sowie benachbarte Grundstücke beinhaltete. Der Verantwortliche hatte mir auf Anforderung über seinen Anwalt lediglich mitteilen lassen, dass weder fremde Grundstücke noch öffentliche Verkehrsflächen mittels Kamera aufgenommen würden, war aber detaillierte Auskünfte und insbesondere auch Nachweise (Screenshots) schuldig geblieben. Nach einer erneuten Aufforderung zur konkreten Auskunftserteilung berief er sich auf das Auskunftsverweigerungsrecht gemäß § 40 Abs. 4 Satz 2 Bundesdatenschutzgesetz (BDSG) (vgl. dazu Tätigkeitsbericht 2021, 6.3.1, Seite 172ff.). Gegen den im daraufhin wegen unrechtmäßiger Verarbeitung personenbezogener Daten eingeleiteten Bußgeldverfahren (erfolgreich) beantragten und vollzogenen Durchsuchungsbeschluss hatte der Betroffene Beschwerde eingelegt und dazu unter anderem ausgeführt, dass das Ordnungswidrigkeitenverfahren allein mit den vorhandenen Fotos hätte geführt werden können. Dem bin ich natürlich entgegengetreten, denn mit den Fotos hätte nur die Existenz der Videokameras, nicht jedoch deren Betrieb und deren Erfassungsbereich nachgewiesen werden können.

Tätigkeitsbericht 2021:
↗ sdb.de/tb2021

Das Amtsgericht Dresden – Ermittlungsrichter – hatte der Beschwerde dann auch nicht abgeholfen und sie dem Landgericht zur Entscheidung vorgelegt. Dieses hat festgestellt, dass die Beschwerde zwar zulässig, in der Sache aber unbegründet war. Zunächst habe ein ausreichender Tatverdacht bestanden, denn aus den Feststellungen des zuständigen Polizeireviers einerseits wie auch des zuständigen Ordnungsamtes andererseits ginge entsprechend hervor, dass der Betroffene auf seinem Grundstück zwei Videokameras errichtet habe, die auch auf Bereiche außerhalb seines Grundstücks, insbesondere auf öffentliche Verkehrsflächen und Nachbargrundstücke, ausgerichtet gewesen seien.

Die Durchsuchungsanordnung war auch verhältnismäßig. Ein für eine vollumfängliche Ahndung notwendiger sicherer Tatnachweis konnte nur durch die Durchsuchung geführt werden. Nur dadurch konnte das Ausmaß der Ordnungswidrigkeit geklärt werden. Die Durchsuchung verfolgte einen legitimen Zweck, indem sie zur Aufklärung und Ahndung einer Ordnungswidrigkeit nach der Datenschutz-Grundverordnung beitragen sollte. Die Durchsuchung war auch geeignet, diesen Zweck zu erfüllen. Infolge des bestehenden erheblichen Grads des Tatverdachts war es wahrscheinlich, dass sich in der Wohnung die gesuchten und im Ordnungswidrigkeitenverfahren als Beweismittel relevanten Gegenstände befinden. Durchsuchung und Beschlagnahme waren insoweit geeignet und erforderlich, um Feststellungen dazu zu treffen, ob und in welchem Umfang der Betroffene den öffentlichen Verkehrsraum und Nachbargrundstücke mittels Videokamera überwacht und ob und in welchem Umfang er diese Videoaufnahmen auch speichert.

Bei dem Eingriff in den grundrechtlich besonders geschützten Wohnbereich des Betroffenen habe es sich zwar um einen schwerwiegenden Eingriff gehandelt, jedoch stand der Eingriff in angemessenem Verhältnis zur Schwere und Dauer der Tat und des Tatverdachts, zumal der Betroffene durch die ihm vorgeworfene Ordnungswidrigkeit selbst seit Längerem in intensiver Weise in das Grundrecht auf informationelle Selbstbestimmung einer Vielzahl von gefilmten Personen eingegriffen habe, wobei auch der gesetzliche Bußgeldrahmen – um eine Bagatellordnungswidrigkeit handelte es sich jedenfalls nicht – zu berücksichtigen gewesen sei. Weniger einschneidende Mittel hätten zur Sachverhaltsaufklärung nicht zur Verfügung gestanden. Mit den vorliegenden Lichtbildern hätte kein Nachweis einer Ordnungswidrigkeit geführt werden können, da diese Lichtbilder gerade keinen Aufschluss über Betrieb, Funktionstüchtigkeit und Erfassungsbereich der Videokameras liefern konnten.

Interessant waren auch die ergänzenden Ausführungen des Landgerichts zum Auskunftsverweigerungsrecht. Der Betroffene habe für sich ein generelles Auskunftsverwei-

gerungsrecht reklamiert. Die Ausübung des Auskunftsverweigerungsrechts des § 40 Abs. 4 Satz 2 BDSG sei jedoch nur insoweit berechtigt, wie der an sich zur Auskunft Verpflichtete die Auskunft auf solche Fragen verweigert, deren Beantwortung ihn der Gefahr strafgerichtlicher Verfolgung oder eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten aussetzen würde. Stünde lediglich ein datenschutzrechtlicher Verstoß im Raum, könne die Auskunft nicht verweigert werden. Es gebe kein generelles, umfassendes Schweigerecht, das Gesetz gewähre vielmehr nur das Recht, auf bestimmte, einzelne Fragen zu schweigen. Zudem müsse dem Betroffenen eine bestimmte Gefahrenlage drohen.

Auch hier ist abschließend zu berichten, dass die Durchsuchungsmaßnahme zum Auffinden der erwarteten Beweismittel geführt hat. Es konnten Speichermedien sichergestellt werden, auf denen sich über 95 Tage erstreckende Zeitrafferaufnahmen der betreffenden Kamera befanden. Mithilfe dieser Videoaufzeichnungen kann nun der Nachweis einer rechtswidrigen Überwachung von Nachbarinnen und Nachbarn, Passantinnen und Passanten, Fahrzeugführerinnen und Fahrzeugführern sowie Bauarbeiterinnen und Bauarbeitern geführt werden. Die Kamera sollte wohl originär lediglich die Baustelle sichern, war aber tatsächlich so betrieben worden, dass sie auch während der Bautätigkeit in Betrieb war und ihr Erfassungsbereich sich nicht auf die Baustelle bzw. das eigene Grundstück beschränkte.

Was ist zu tun?
Hausdurchsuchungen kommen auch beim Verdacht rechtswidriger Videoüberwachungen als Ermittlungsmaßnahme in Betracht. Die Durchsuchung von Wohn- oder Geschäftsräumen kann aber vermieden werden, wenn man frühzeitig mit der Aufsichtsbehörde kooperiert.

6.5 Öffentlichkeitsarbeit

6.5.1 Online-Kommunikation und Publikationen

Während der Corona-Pandemie haben Soziale Netzwerke weiter an Bedeutung zugelegt. Sie sind bereits seit Jahren gern genutzte Kommunikationsmittel, nicht nur bei Privatpersonen, sondern ebenso bei Unternehmen und Behörden. Dominiert wird der Social-Media-Markt von internationalen IT-Konzernen. Sie betonen zwar stets, wie wichtig ihnen die Privatsphäre ihrer Nutzerinnen und Nutzer ist, doch die

zahlreich bekannt gewordenen Datenschutzskandale zeugen vom Gegenteil. Des Weiteren stehen Meta, Alphabet und Co. immer wieder wegen ihrer intransparenten Datenverarbeitung in der Kritik. Sie verstoßen damit massiv gegen die Datenschutz-Grundverordnung. Damit erübrigt sich auch jede weitere Frage, warum insbesondere öffentliche Stellen und vor allem Datenschutz-Aufsichtsbehörden diese Plattformen nicht nutzen können.

Folgen Sie mir auf Mastodon!

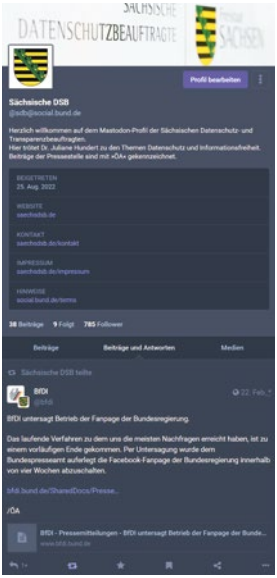


Abbildung 7:
Mastodon-Profil der SDTB

Umso erfreulicher ist es, dass in den vergangenen Jahren datenschutzfreundliche Alternativen entstanden sind. Dazu zählt beispielsweise der Microblogging-Dienst Mastodon, den ich seit November 2022 für meine Öffentlichkeitsarbeit einsetze. Mit meiner Behörde informiere ich dort regelmäßig über aktuelle Themen rund um den Datenschutz und die Informationsfreiheit.

Mastodon ist vergleichbar mit Twitter, unterscheidet sich aber vor allem in datenschutzrechtlichen Belangen vom bekannten US-Unternehmen. Die maximale Länge einer Mastodon-Nachricht beträgt 500 Zeichen. Bilder und Videos können ebenfalls eingebunden werden. Anders als bei Twitter gibt es auf Mastodon keinen zentralen Anbieter des Dienstes, denn das Mastodon-Netzwerk besteht aus einer Vielzahl an Servern, auf denen sogenannte Mastodon-Instanzen laufen. Sie lassen sich auch miteinander verbinden. Für mein Profil nutze ich eine Instanz des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI). Mein Kanal ist dort öffentlich und ohne Registrierung auf https://social.bund.de/@sdb einsehbar. Mitglieder des Kurznachrichtendiensts können mir unter @sdb@bfdi.bund folgen.

Die meisten Instanzen werden bislang aber von Privatpersonen eingerichtet und betrieben. Ein weiterer Unterschied zu Twitter: Bei Mastodon gibt es keinen Algorithmus, der auf Basis der detaillierten Auswertung des persönlichen Nutzungsverhaltens Nachrichten sortiert und damit sogenannte „Filter-Blasen" generiert. Stattdessen werden die Neuigkeiten der abonnierten Kanäle chronologisch geordnet.

Wer sich ein Mastodon-Profil einrichten und darüber kommunizieren möchte, findet beispielsweise auf https://joinmastodon.org/servers eine Liste mit verfügbaren Instanzen. Für die Nutzung von Mastodon auf Mobilgeräten stehen in den App-Stores zahlreiche kostenfreie und oftmals quelloffene Applikationen zum Download bereit.

Neugestaltung der Website

Abbildung 8:
Neue Website der SDTB

Sehr viele Eingaben in meiner Behörde sind auf Wissenslücken im Datenschutzrecht zurückzuführen. Etliche Verstöße gegen das Recht auf informationelle Selbstbestimmung ließen sich verhindern, wenn Verantwortliche über ihre Pflichten besser Bescheid wüssten und den Datenschutz von Anfang an berücksichtigten. Aus diesem Grund liegt einer meiner Arbeitsschwerpunkte auf der Prävention. Konkret bedeutet das, Verantwortliche frühzeitig zu sensibilisieren, ihnen praxisnahe Informationen an die Hand zu geben und betroffene Personen über ihre Rechte und Schutzmöglichkeiten aufzuklären. Deshalb wird die neue Website meiner Behörde auch inhaltlich stark erweitert. Im Jahr 2022 haben die Beschäftigten und ich intensiv an der Neugestaltung gearbeitet, sodass der Webauftritt demnächst online gehen kann. Das Informationsangebot ist nach Zielgruppen unterteilt und enthält sowohl Ausführungen zu den rechtlichen Grundlagen als auch themenspezifische Inhalte, beispielsweise zum Datenschutz in der Schule, im Homeoffice, bei Videokonferenzsystemen und zu vielen weiteren Lebensbereichen.

Neue Broschüren

Abbildung 9:
2022 herausgegebene Broschüren

Bei der Informationsvermittlung greife ich nicht nur auf die Möglichkeiten der Online-Kommunikation zurück, sondern nutze ebenso gedruckte Publikationen. Insbesondere für Präsenzveranstaltungen eignen sich Broschüren, um die Zielgruppen für das jeweilige Thema zu sensibilisieren. Im Berichtszeitraum habe ich zwei Broschüren herausgegeben: „Datenschutz in Sachsen – Aufgaben, Befugnisse und Rechtsstellung der Sächsischen Datenschutzbeauftragten" und „Das Transparenzgesetz – Ihr Recht auf Informationszugang".

Publikationsdatenbank des Freistaates Sachsen:
↗ publikationen.sachsen.de

Die beiden Veröffentlichungen wurden unter anderem beim Tag der offenen Tür des Sächsischen Landtags an die Besucherinnen und Besucher meines Standes herausgegeben. Beide Broschüren sind auch in der Publikationsdatenbank des Freistaates Sachsen als PDF-Datei erhältlich.

6.5.2 Presse- und Medienarbeit

Obwohl die Online-Kommunikation an Bedeutung gewonnen hat, bleibt die Presse- und Medienarbeit ein wichtiges Kommunikationsinstrument für meine Behörde. Pressemitteilungen erschienen unter anderem zum Zensus 2022, zum Tätigkeitsbericht des vorherigen Berichtszeitraums, zu Mastodon und dem Sächsischen Transparenzgesetz. Für die meisten Schlagzeilen sorgte allerdings die Medieninformation zur Nutzung von Facebook-Fanpages. Kein anderes Thema führte über das Jahr verteilt zu so vielen Presseanfragen. Davon abgesehen wendeten sich Journalistinnen und Journalisten aber auch mit anderen Sachverhalten an mich. Es ging beispielsweise um Microsoft 365, Cyberattacken, Online-Kartendienste, Bußgelder für Datenschutzverstöße, Parkraumüberwachung vor Supermärkten, Überwachungssoftware und vereinzelt um Corona. Nicht nur gegenüber der Tagespresse, sondern auch in Podcasts, Radio-Sendungen und TV-Interviews informierte ich über aktuelle Datenschutzthemen, unter anderem zum Beschäftigtendatenschutz.

6.5.3 Fortbildungen, Infoveranstaltungen und fachlicher Austausch

Der Schutz personenbezogener Daten spielt bekanntlich in vielerlei Lebensbereichen eine wichtige Rolle. Deshalb ist es keinesfalls verwunderlich, dass Referentinnen und Referenten meiner Behörde und ich mitunter stark nachgefragt sind. Das ist einerseits erfreulich, andererseits zwingt es uns zur Priorisierung und Begrenzung des Themenspektrums. Auf großes Interesse stößt weiterhin alles, was mit dem Betrieb einer Website oder App sowie Cookies, Einwilligungen und

internationalem Datentransfer zu tun hat – vor allem wenn US-Dienstleister eingebunden sind. Das zeigte sich auch auf einer Online-Veranstaltung mit Kreatives Sachsen, auf der ich vor allem Mitarbeitende von Agenturen und Verantwortliche über die datenschutzrechtlichen Anforderungen informierte. Reges Interesse am Datenschutz begegnete mir auch beim „Tag der offenen Tür des Sächsischen Landtags" und dem „Infotag für Rechtsreferendare", an denen sich meine Behörde ebenfalls beteiligte.

An dieser Stelle sei erwähnt, dass das (2022 noch: künftige) Amt als Sächsische Transparenzbeauftragte ebenfalls meine Zeit in Anspruch nahm. Bei Veranstaltungen – mit der Sächsischen Landeszentrale für politische Bildung und der Europäischen Akademie für Informationsfreiheit und Datenschutz e. V. – sprach ich über die Möglichkeiten und Grenzen des Sächsischen Transparenzgesetzes, das zum 1. Januar 2023 in Kraft trat.

Schulungen

Auch im aktuellen Berichtszeitraum waren Mitarbeiterinnen und Mitarbeiter meiner Dienststelle im Sinne der Prävention, trotz des stetig gestiegenen Arbeitsaufkommens, vielfältig im Bereich der Beratung bzw. Aus- und Fortbildung unterwegs. Sie hielten circa 20 Fortbildungsseminare, unter anderem an den staatlichen Aus- und Fortbildungseinrichtungen wie der Hochschule Meißen (FH) 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.

Insgesamt ist in diesem Bereich eine weiter fortschreitende Digitalisierung mit vermehrten Online-Seminaren, teils nunmehr auch im Hybrid-Format (Präsenz- und Online-Form), festzustellen.

Zusammenarbeit mit Behörden und Multiplikatoren

Wie üblich beginnen Amtszeiten mit Antrittsbesuchen – eine gute Gelegenheit, um Entscheiderinnen und Entscheider auf den Datenschutz aufmerksam zu machen. Neben Terminen in Ministerien fanden ebenso Treffen mit Abgeordneten, Behörden und anderen Organisationen statt, beispielsweise mit dem Bundesamt für Sicherheit in der Informationstechnik in Freital, mit der Verbraucherzentrale Sachsen, den Datenschutzbeauftragten der Kirchen, der Opferbeauftragten, dem DRK und der Stiftung Datenschutz.

Außerdem nahm ich als Mitglied bei der 28. Sitzung des Statistischen Beirats des Freistaates Sachsen und bei der Jährlichen Sitzung des Landespräventionsrats teil. Des Weiteren tauschte ich mich auf einem Treffen mit den Datenschutzbeauftragten der Landkreise und der Kommunen aus und stellte mich und meine Behörde im Erfahrungsaustauschkreis der Gesellschaft für Datenschutz und Datensicherheit e. V. vor.

7 Zusammenarbeit der Datenschutzaufsichtsbehörden, Datenschutzkonferenz

Den Vorsitz über die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hatte im Berichtszeitraum der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) inne. Wegen der Corona-Pandemie fand die erste Zwischenkonferenz noch als Videokonferenz statt; die erste Hauptkonferenz am 23. und 24. März 2022 erstmalig seit über zwei Jahren wieder in Präsenz.

Abbildung 10:
103. Konferenz der DSK im März 2022 in Bonn © BfDI

Abbildungen 11 und 12:
104. Konferenz der DSK auf dem Petersberg bei Bonn (Copyright BfDI)

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

Ein Blick auf die nachfolgenden Entschließungen, Beschlüsse, Orientierungshilfen, Stellungnahmen und Anwendungshinweise verdeutlicht, mit welcher Themenvielfalt sich meine Behörde im Rahmen der Datenschutzkonferenz befasste.

7.1 Materialien der Datenschutzkonferenz – Entschließungen

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

- Petersberger Erklärung zur datenschutzkonformen Verarbeitung von Gesundheitsdaten in der wissenschaftlichen Forschung (24.11.2022)
- Die Zeit für ein Beschäftigtendatenschutzgesetz ist „Jetzt"! (29.04.2022)
- Wissenschaftliche Forschung – selbstverständlich mit Datenschutz (23.03.2022)
- Parlamentarische Untersuchungsausschüsse und Löschmoratorien: Datenschutz durch klare Vorgaben und Verarbeitungsbeschränkungen für Behörden (23.03.2022)

7.2 Materialien der Datenschutzkonferenz – Beschlüsse

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

- Abschlussbericht der Arbeitsgruppe DSK „Microsoft-Online-Dienste" (07.12.2022)
- Auswirkungen der neuen Verbrauchervorschriften über digitale Produkte im BGB auf das Datenschutzrecht (29.11.2022)
- Festlegung zur Arbeitsgruppe DSK „Microsoft-Online-Dienste" (25.11.2022)
- Zusammenfassung des Berichts zur Arbeitsgruppe DSK „Microsoft-Online-Dienste" (25.11.2022)
- Zur Verarbeitung personenbezogener Daten im Zusammenhang mit der einrichtungsbezogenen Impfpflicht (13.04.2022)

- Hinweise der DSK – Datenschutzkonformer Online-Handel mittels Gastzugang (24.03.2022)
- Zur Task Force Facebook-Fanpages (23.03.2022)

7.3 Materialien der Datenschutzkonferenz – Orientierungshilfen

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

- Auswertung Konsultation zur Orientierungshilfe für Anbieter von Telemedien (05.12.2022)
- Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien ab dem 1. Dezember 2021 (OH Telemedien 2021) – Version 1.1 (05.12.2022)
- FAQ zu Facebook-Fanpages (22.06.2022)
- Orientierungshilfe der Aufsichtsbehörden zur Verarbeitung von personenbezogenen Daten für Zwecke der Direktwerbung unter Geltung der Datenschutz-Grundverordnung (18.02.2022)

7.4 Materialien der Datenschutzkonferenz – weitere Dokumente

Die Datenschutzkonferenz veröffentlichte im Jahr 2022 die folgenden Gutachten.

- Kurzgutachten zur datenschutzrechtlichen Konformität des Betriebs von Facebook-Fanpages – Version 1.1 (15.11.2022)
- Gutachten zum aktuellen Stand des US-Überwachungsrechts und der Überwachungsbefugnisse von Prof. Stephen I. Vladeck, University of Texas School of Law (25.01.2022)
- Wesentliche Befunde des Gutachtens von Stephen I. Vladeck vom 15.11.2021 zur Rechtslage in den USA (25.01.2022)

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

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

- Leitlinien 06/2022 für die praktische Anwendung der gütlichen Einigung – Version 2.0 (12.05.2022)
- Leitlinien 02/2022 zur Anwendung des Artikels 60 DSGVO – Version 1.1 (14.03.2022)
- Leitlinien 04/2021 über Verhaltensregeln als Instrument für Übermittlungen – Fassung 2.0 (22.02.2022)
- Leitlinien 01/2021 zu Beispielen für die Meldung von Verletzungen des Schutzes personenbezogener Daten – Version 2.0 (03.01.2022)

7.6 Gemeinsame Überprüfung von Medienunternehmen durch Datenschutzaufsichtsbehörden

↗ Art. 6 und 28 DSGVO

Tätigkeitsbericht 2021:
↗ sdb.de/tb2021

Bereits im Tätigkeitsbericht 2021 (vgl. 7.7, Seite 193f.) habe ich über eine gemeinsame Prüfung von Medienunternehmen berichtet, an der sich insgesamt elf der deutschen Datenschutzaufsichtsbehörden beteiligen. Im Jahr 2020 wurden hierfür Fragebögen erarbeitet und an die jeweils reichweitenstärksten Online-Medien im jeweiligen Bundesland versandt. Im ersten Halbjahr wurden die Fragebögen in den jeweiligen Bundesländern in Zuständigkeit der Aufsichtsbehörden ausgewertet und einzelne Dienste einer tieferen Prüfung unterzogen. Erkenntnisse zu einzelnen Diensten wurden hierzu unter den Aufsichtsbehörden ausgetauscht, Informationen zu den geprüften Unternehmen wurden jedoch strikt innerhalb des jeweiligen Zuständigkeitsbereichs belassen. Die Prü-

fung der zum Teil sehr komplexen Datenverarbeitungen und der vorliegenden vertraglichen Unterlagen gestaltete sich in Anbetracht der weit über 100 verschiedenen eingesetzten Dienste in zum Teil unterschiedlichen Konfigurationen als sehr aufwendig. Ebenso aufwendig wäre das Herbeiführen von abgestimmten Auffassungen zu einzelnen Diensten oder der zulässigen Ausgestaltung von Einwilligungslösungen.

Im Sommer bis in den Spätherbst fanden in meinem Zuständigkeitsbereich Gespräche mit allen von der Prüfung betroffenen Medienhäusern statt. Dabei wurden Fragen des Einsatzes von Diensten erörtert, bei denen Datentransfers ins außereuropäische Ausland infrage stehen, aber auch einzelne Lösungen zur Herbeiführung einer Zustimmungsentscheidung sowie Drittdienste und deren Erforderlichkeit besprochen. Ich habe deutlich gemacht, an welchen Punkten ich Änderungen für erforderlich halte, habe aber auch Argumente der Medienhäuser zur Finanzierung von Online-Journalismus zur Kenntnis genommen. Insgesamt verliefen die Gespräche sehr konstruktiv, es gab zwischenzeitlich bereits etliche Anpassungen, sodass ein deutlich besseres Datenschutzniveau im Vergleich zum letzten Jahr vor der gemeinsamen Prüfung zu verzeichnen ist.

Die Gespräche sind noch nicht abgeschlossen. Auch wenn ich bislang Fristverlängerungen zur Umsetzung der aus technischer und geschäftsprozessualer Sicht recht komplexen Änderungen gewährt habe, kann ich nicht ausschließen, dass einzelne Aspekte der Datenverarbeitungen auf aufsichtsrechtlichem Weg bereinigt werden müssen und sich gegebenenfalls Gerichte mit den Fragen der Zulässigkeit einzelner Verarbeitungen werden befassen müssen.

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

8.1 Einsichtnahme in und Ablichtungen aus Gefangenen-personal- sowie Gesundheits- und Therapieakten für Gefangene

↗ §§ 54, 55, 56 SächsJVollzDSG

Aus einer Justizvollzugsanstalt erreichte mich eine Anfrage Gefangener zu den Voraussetzungen, unter denen Strafgefangenen eine Einsichtnahme in ihre Gefangenenpersonal- sowie Gesundheits- und Therapieakten zu gewähren und Kopien hieraus herauszugeben sind. Hintergrund der Anfrage war die auf den Wortlaut von § 56 des Sächsischen Justizvollzugsdatenschutzgesetzes (SächsJVollzDSG) gestützte Weigerung der Anstalt, betroffenen Gefangenen Kopien aus den zu ihnen geführten Gesundheits- und Therapieakten auszuhändigen. Ein Anspruch auf Erhalt von Kopien sei gesetzlich nicht vorgesehen.
Weil die gesetzlichen Vorschriften in §§ 54, 55 und 56 Sächs JVollzDSG zu Auskunft aus und Einsicht in über Gefangene geführte Akten sowie die Fertigung von Kopien hieraus tatsächlich nicht völlig unmissverständlich formuliert sind, habe ich die Anfrage zum Anlass genommen, Inhalt und Reichweite der Regelungen ausführlicher zu erläutern.

Auskunft aus und Einsicht in Gefangenenpersonalakten

Das zentrale datenschutzrechtliche Betroffenenrecht ist das Recht auf Auskunft. Davon zu unterscheiden ist das Recht auf Einsicht in Akten, das regelmäßig Zugang zu mehr Infor-

mationen (unter Umständen auch über Dritte) eröffnet als das Auskunftsrecht, das auf die personenbezogenen Daten der betroffenen Person begrenzt ist.

Hinsichtlich des informatorischen Gehalts liegen Auskunft und Einsicht allerdings sehr eng beieinander, wenn es um Akten geht, die speziell zur betroffenen Person geführt werden. Angesichts der mit Blick auf die Rechtsprechung des Europäischen Gerichtshofs (vgl. EuGH, Urteil vom 17.07.2014, Az.: C-141/12) gebotenen weiten Auslegung des Begriffs der personenbezogenen Daten, die ohne Weiteres auf den Begriff der personenbezogenen Daten nach § 2 Nr. 3 SächsJVollzDSG übertragbar ist, dürfte eine Gefangenenpersonalakte nahezu ausschließlich personenbezogene Daten der oder des betreffenden Gefangenen enthalten, über die nach § 54 Abs. 1 Satz 2 Nr. 1 SächsJVollzDSG Auskunft zu erteilen ist. Gründe, aus denen eine Auskunft unterbleiben oder aufgeschoben werden kann – § 54 Abs. 2 SächsJVollzDSG verweist insoweit auf § 53 Abs. 2 und 3 SächsJVollzDSG – dürften regelmäßig nicht vorliegen oder, wenn überhaupt, nur bei einem Bruchteil der verarbeiteten Daten in Betracht kommen. Der Auskunftsanspruch wird flankiert von der in § 54 Abs. 5 Satz 1 SächsJVollzDSG vorgesehenen Möglichkeit, die Auskunft auch durch die Gewährung von Akteneinsicht oder die Aushändigung von Kopien oder Ausdrucken zu erteilen.

Unter Berücksichtigung der Weite des Auskunftsanspruchs nach § 54 Abs. 1 SächsJVollzDSG wird eine bloße mündliche Auskunft regelmäßig wenig praktikabel sein und der Bedeutung des hinter den einfachgesetzlichen Regelungen stehenden Grundrechts nicht gerecht werden, sodass eine Auskunftserteilung in Form der Gewährung von Akteneinsicht oder der Aushändigung von Kopien (§ 54 Abs. 5 Satz 1 SächsJVollzDSG) bereits zur Erfüllung des „bloßen" Auskunftsanspruchs sowohl für Gefangene als auch für die Vollzugsanstalt als das geeignetste Mittel der Umsetzung erscheint. In jedem Fall haben Gefangene einen Anspruch auf ermessensfehlerfreie Entscheidung der Vollzugsanstalt über die Erteilung von Auskunft durch die Gewährung von

Akteneinsicht oder die Aushändigung von Kopien, wobei die Vollzugsanstalt ihre Entscheidung im Licht des Grundrechts auf informationelle Selbstbestimmung zu treffen hat.

Ein Akteneinsichtsrecht nach § 55 SächsJVollzDSG besteht im Vergleich zum voraussetzungslosen Anspruch auf Auskunft nach § 54 SächsJVollzDSG nur unter relativ hohen Voraussetzungen. Der sächsische Gesetzgeber hat sich entschlossen, im Wesentlichen an der früheren Rechtslage festzuhalten und Gefangenen einen Anspruch auf Akteneinsicht nur zu eröffnen, soweit eine Auskunft für die Wahrnehmung ihrer rechtlichen Interessen nicht ausreicht, die Einsichtnahme hierfür erforderlich ist und überwiegende berechtigte Interessen Dritter nicht entgegenstehen.

Der Begriff des rechtlichen Interesses ist dabei recht unbestimmt; während die obergerichtliche Rechtsprechung einen vergleichsweise strengen Maßstab anlegt, wird in Teilen der Literatur bereits die mit der Einsicht verfolgte Ausübung des (Grund-)Rechts auf informationelle Selbstbestimmung als ein hinreichendes rechtliches Interesse im Sinn der Vorschrift betrachtet. In diesem Zusammenhang wird die Einsicht als notwendige Voraussetzung für die eventuell erforderliche Geltendmachung der Betroffenenrechte nach § 62 SächsJVollzDSG (Recht der betroffenen Person auf Berichtigung und Löschung sowie Einschränkung der Verarbeitung personenbezogener Daten) erachtet. Aus datenschutzrechtlicher Sicht ist eine weite Auslegung des Begriffs des rechtlichen Interesses vorzugswürdig und mit Blick darauf, dass die Gefangenenpersonalakte für den weiteren Vollzug und das Leben der Betroffenen ganz entscheidende Informationen enthält, geboten. Andererseits kann ich eine auf obergerichtliche Rechtsprechung gestützte strenge Auslegung des Begriffs des rechtlichen Interesses durch Justizvollzugsanstalten und eine infolgedessen zurückhaltende Gewährung von Akteneinsicht nicht beanstanden. Das Bundesverfassungsgericht hatte in einer Entscheidung aus dem Jahr 2003 ausdrücklich offengelassen, ob ein „rechtliches Interesse" schon im Hinblick auf das Recht des Gefangenen auf informationelle Selbstbestimmung zu bejahen ist (BVerfG, 2 BvR 406/02).

Gesundheits- und Therapieakten

Nach § 56 SächsJVollzDSG ist Gefangenen auf Antrag Auskunft aus ihren Gesundheitsakten und Therapieakten zu gewähren; sie können auf Antrag auch Akteneinsicht erhalten. Eine Ablehnung des Antrags kommt hinsichtlich solcher Aktenteile in Betracht, die mit Sperrvermerken im Sinne von § 57 SächsJVollzDSG versehen sind.

Auch wenn § 56 SächsJVollzDSG keinen ausdrücklichen Anspruch Gefangener auf Ablichtungen aus den sie betreffenden Gesundheits- oder Therapieakten enthält und von den Verweisungen in § 56 Satz 2 SächsJVollzDSG auf § 55 SächsJVollzDSG die Regelungen zu Ablichtungen und Ausdrucken nach § 55 Abs. 5 Satz 2 bis 4 SächsJVollzDSG nicht erfasst werden, bestünde nach dem Wortlaut des Gesetzes zumindest ein Anspruch der Gefangenen auf ermessensfehlerfreie Entscheidung über einen Antrag auf Ablichtungen aus Gesundheits- und Therapieakten. Allerdings würde das Fehlen eines direkten Anspruchs auf den Erhalt von Kopien aus den zu ihnen geführten Gesundheits- und Therapieakten das Grundrecht der betroffenen Gefangenen auf informationelle Selbstbestimmung rechtswidrig einschränken. Das Bundesverfassungsgericht wies in einer Entscheidung aus dem Jahr 2016 darauf hin, dass nach der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte aus Art. 8 Europäische Menschenrechtskonvention grundsätzlich ein Anspruch des Patienten gegenüber staatlichen Stellen auf umfassende Einsicht in seine Krankenakte und die Übermittlung von Kopien folge (BVerfG, 2 BvR 1541/15).

In der Praxis und in gerichtlichen Entscheidungen zu ähnlichen Vorschriften in anderen Bundesländern hat sich danach eine Auslegung der gesetzlichen Regelung zu Gesundheits- und Therapieakten etabliert, nach der die fehlende Verweisung auf Voraussetzungen der Erteilung von Kopien aus anderen Akten als Beleg dafür gesehen wird, dass Kopien aus Gesundheits- und Therapieakten den betroffenen Gefangenen auf Wunsch voraussetzungslos zu erteilen sind. Auf Nachfrage bestätigte mir das als oberste Aufsichtsbehörde zuständige Sächsische Staatsministerium der Justiz und für Demokratie,

Europa und Gleichstellung, dass es diese Lesart des Gesetzes für zutreffend hält. Nach Auffassung des Staatsministeriums ergibt sich aus dem Regelungszusammenhang der §§ 55, 56 SächsJVollzDSG nicht nur, dass Gefangenen Ablichtungen aus den Gesundheits- und Therapieakten zu überlassen seien, sondern dass dafür auch keine Kosten erhoben werden dürften. Darüber seien die Justizvollzugsanstalten nach Auskunft des Staatsministeriums informiert und zu einem entsprechenden Vorgehen angehalten worden.
Ich habe die Leitung der von der Anfrage betroffenen Justizvollzugsanstalt über die Rechtslage informiert und um Beachtung gebeten. Die Anstaltsleitung bestätigte mir gegenüber umgehend, dass bei künftigen Anträgen von Gefangenen auf Ablichtungen aus bzw. von Gesundheits- und Therapieakten diese unentgeltlich überlassen würden.

Was ist zu tun?
Gefangene haben einen Rechtsanspruch auf die Herausgabe von Ablichtungen aus den sie betreffenden Gesundheits- und Therapieakten. Die Justizvollzugsanstalten haben Ablichtungen ohne Erhebung von Kosten zu überlassen.

8.2 Bekanntgabe personenbezogener Daten im Rahmen einer Anhörung und schriftlichen Verwarnung

↗ §§ 55, 56 OWiG; § 66 Abs. 1 Nr. 4 OWiG; § 500 Abs. 1 StPO in Verbindung mit § 47 Nr. 1 BDSG

Im letzten Berichtszeitraum informierten mich mehrere Petenten, dass eine Bußgeldbehörde die personenbezogenen Daten des Anzeigeerstatters und/oder des Zeugen an Dritte in einer Anhörung und schriftlichen Verwarnung im Rahmen von Verkehrsordnungswidrigkeitsverfahren übermittelt.
Die Namensnennung der Anzeigeerstatterin bzw. des Anzeigeerstatters und/oder der Zeugin oder des Zeugen im Rahmen der Anhörung und schriftlichen Verwarnung ist datenschutzwidrig. Gemäß § 500 Abs. 1 Strafprozessordnung (StPO) in Verbindung mit § 47 Nr. 1 Bundesdatenschutzgesetz (BDSG) – die Vorschriften gelten über § 46 Abs. 1 Gesetz über Ordnungswidrigkeiten (OWiG) auch für das Bußgeldverfahren – müssen personenbezogene Daten auf rechtmäßige Weise und nach Treu und Glauben verarbeitet

werden. Verarbeitung ist auch die Offenlegung durch Übermittlung (§ 46 Nr. 2 BDSG). Dabei bedarf die Offenlegung durch Übermittlung grundsätzlich einer Rechtsgrundlage. Der Gesetzgeber hat lediglich hinsichtlich des Bußgeldbescheides in § 66 Abs. 1 Nr. 4 OWiG bestimmt, dass dieser die Beweismittel enthalten muss. Dann sind die Beweismittel ihrer Art nach zu bezeichnen. Zeuginnen bzw. Zeugen und Sachverständige sind mit Namen und Wohn- bzw. Dienstanschrift anzugeben. Weder in § 55 OWiG (Anhörung) noch in § 56 OWiG (Verwarnung) findet sich eine entsprechende gesetzliche Regelung. Somit existiert keine Rechtsgrundlage für eine Offenlegung personenbezogener Daten im Anhörungs- bzw. Verwarnungsverfahren. Dies läuft auch nicht einem womöglich vorhandenen Informationsinteresse der Verwarngeldadressatin bzw. des Verwarngeldadressaten zuwider, da diese/r ihre/seine Rechte im Rahmen eines Auskunftsverlangens oder einer Akteneinsicht gemäß § 49 Abs. 1 OWiG geltend machen kann. Eine abstrakte Bezeichnung der Beweismittel ihrer Art nach („Zeuge", „Lichtbild" etc.) in Anhörung und Verwarnung ist zwar gesetzlich nicht vorgeschrieben, wäre aber mangels Grundrechtseingriffs datenschutzrechtlich nicht zu beanstanden.

Auch eine Offenlegung durch Übermittlung aufgrund einer Einwilligung der Anzeigeerstatterin bzw. des Anzeigeerstatters oder der Zeuginnen bzw. Zeugen ist datenschutzwidrig. Eine Verarbeitung personenbezogener Daten aufgrund einer Einwilligung ist nur möglich, wenn dies nach einer Rechtsvorschrift auf der Grundlage einer Einwilligung erfolgen kann. Wie bereits erwähnt, ist die Benennung von Beweismitteln im Rahmen einer Anhörung und Verwarnung nicht gesetzlich normiert und daher für die Aufgabenwahrnehmung einer Ordnungswidrigkeitenbehörde nach § 35 OWiG nicht erforderlich. Die Behörde als Verantwortlicher ist grundsätzlich daran gehindert, diese personenbezogenen Daten dennoch zu verarbeiten, indem sie die Einwilligung der Anzeigeerstatterin bzw. des Anzeigeerstatters oder der Zeuginnen bzw. Zeugen einholt. Entsprechende Hinweise etwa in Anzeigeformularen der Verwaltungsbehörden entfalten keine Rechtswirkung.

Die betroffene Bußgeldbehörde stütze ihr datenschutzwidriges Vorgehen unter anderem auch darauf, dass man mit der Namensnennung der Anzeigeerstatterin bzw. des Anzeigeerstatters oder der Zeuginnen bzw. Zeugen der Bitte eines Amtsgerichts nachkomme. Auch eine richterliche „Bitte" ist diesbezüglich irrelevant, da eine richterliche Entscheidung kein parlamentarisches Gesetzgebungsverfahren ersetzen kann.

Ich habe die Bußgeldbehörde angewiesen, unverzüglich die Namensnennung der Anzeigeerstatterin bzw. des Anzeigeerstatters oder der Zeuginnen bzw. Zeugen in den Anhörungen und schriftlichen Verwarnungen zu unterlassen.

Was ist zu tun?
Die Namensnennung der Anzeigeerstatterin bzw. des Anzeigeerstatters und/oder Zeuginnen bzw. Zeugen im Rahmen der Anhörung und schriftlichen Verwarnung durch die Verwaltungsbehörde ist datenschutzwidrig.

8.3 Verwendung eines DNA-Identifizierungsmusters aus einer minder schweren Straftat für künftige Strafverfahren

↗ §§ 81a, 81e, 81f, 98c StPO

Ein Petent wandte sich an mich und schilderte folgenden Sachverhalt: In einem Ermittlungsverfahren wegen einer minder schweren Straftat sei im September 2020 auf Beschluss des zuständigen Amtsgerichts sein DNA-Identifizierungsmuster gemäß §§ 81a, 81e Strafprozessordnung (StPO) zum Zweck des Abgleichs mit Vergleichsmaterial vom Tatort erhoben worden. In einem davon unabhängigen, später wegen eines anderen Tatvorwurfs gegen ihn geführten Ermittlungsverfahren sei in einem gerichtlichen Durchsuchungsbeschluss vom Dezember 2021 erwähnt worden, dass das DNA-Identifizierungsmuster des Beschuldigten auf einem Tatmittel festgestellt worden sei. Der Petent bat um Aufklärung, weshalb sein DNA-Identifizierungsmuster, das im September 2020 nicht zur Identitätsfeststellung in künftigen Strafverfahren nach § 81g StPO erhoben worden sei, in einem mit dem ersten Verfahren nicht im Zusammenhang stehenden Ermittlungsverfahren verwendet wurde.

Ich bat die zuständige Polizeidienststelle um Informationen zum Vorgang und wies darauf hin, dass die Maßnahme nach §§ 81a, 81e StPO bzw. die entsprechende richterliche Anordnung vom September 2020 sich auf einen Abgleich in dem konkreten anhängigen Verfahren bezogen und gerade nicht auf eine Identitätsfeststellung in künftigen Strafverfahren gemäß § 81g StPO abgezielt hatte. Angesichts des minder schweren Tatvorwurfs wäre eine Anordnung nach § 81g StPO „zur Identitätsfeststellung in künftigen Strafverfahren" mangels Vorliegen der gesetzlich bestimmten Voraussetzungen auch nicht zulässig gewesen.

Die Polizei teilte mir mit, dass § 98c Satz 1 StPO die Rechtsgrundlage für den Abgleich des DNA-Identifizierungsmusters im jüngeren Verfahren gewesen sei, wonach zur Aufklärung einer Straftat personenbezogene Daten aus einem Strafverfahren mit anderen zur Strafverfolgung oder Strafvollstreckung oder zur Gefahrenabwehr gespeicherten Daten maschinell abgeglichen werden dürften. Auch nach §§ 81a, 81e und 81f StPO erhobene DNA-Identifizierungsmuster dürften einmalig mit den in der DNA-Analyse-Datei (DAD) des Bundeskriminalamtes gespeicherten offenen Spuren (Spurenmaterial ohne herstellbaren Bezug zum Verursacher) abgeglichen werden.

Diese Auskunft verwunderte, weil der Abgleich im zweiten Verfahren Monate nach der Erhebung des DNA-Identifizierungsmusters im ersten Verfahren erfolgte, die Erhebung des Musters aber gerade nicht für künftige Strafverfolgungszwecke erlaubt war.

Auf meine Nachfrage zum zeitlichen Ablauf der Untersuchungen und des Abgleichs teilte mir die Polizei bei einer Prüfung vor Ort und unter Vorlage der relevanten Unterlagen mit, dass die Analyse der beim Petenten im September 2020 auf Grundlage der richterlichen Anordnung entnommenen Körperzellen durch das beauftragte Institut erst im September 2021 – also etwa ein Jahr nach Entnahme der Körperzellen – erfolgte. Ende September 2021 wurde dann das nunmehr erstellte DNA-Identifizierungsmuster mit den in der DAD hinterlegten offenen Spuren abgeglichen, wobei

ein Treffer erzielt wurde, der sich auf eine DNA-Spur aus dem zweiten, jüngeren Verfahren bezog.

Es stellte sich heraus, dass zu diesem Zeitpunkt – Ende September 2021 – die Spuren aus der Straftat von Anfang Mai 2021, die zum zweiten, jüngeren Verfahren geführt hatten, bereits analysiert und – weil sie zur Zeit der Analyse keiner bekannten Person zugeordnet werden konnten – als offene Spur in die DAD eingestellt worden waren. Die Analyse der Tatortspur vom Mai 2021 war bereits Anfang Juli 2021 vorgenommen worden, ebenso die Einstellung in die DAD. Damit lag ein DNA-Identifizierungsmuster zur zweiten Tat ab Juli 2021 in der DAD als offene Spur vor und wurde bei dem Abgleich mit dem DNA-Identifizierungsmuster des Petenten, das im September 2021 erstellt wurde, als übereinstimmend erkannt. Obwohl also die zweite Straftat einige Monate nach der ersten Tat begangen wurde, wurde das im Zusammenhang mit der älteren Tat erhobene DNA-Identifizierungsmuster aufgrund der verzögerten Erstellung im September 2021 mit einer sogenannten offenen Spur aus einem seit Mai 2021 anhängigen Ermittlungsverfahren abgeglichen und führte zu einem Treffer. Die im Abgleich liegende Verwendung seines DNA-Identifizierungsmusters erfolgte damit nicht zur „Identitätsfeststellung in künftigen Strafverfahren", sondern in einem anderen anhängigen Strafverfahren. Maßgeblich ist insoweit der Zeitpunkt des Abgleichs, nicht aber derjenige der jeweiligen Straftat.

Dass nach §§ 81a, 81e und 81f StPO erstellte DNA-Identifizierungsmuster nach ihrer Erstellung einmalig mit offenen Tatspuren anhängiger Strafverfahren abgeglichen werden, ist datenschutzrechtlich nicht zu beanstanden und von § 81a Abs. 3 StPO gedeckt („…nur für Zwecke des der Entnahme zugrunde liegenden oder eines anderen anhängigen Strafverfahrens…"). Der Abgleich selbst erfolgt auf Grundlage von § 98c StPO.

Nach Auskunft der Polizei beruhten die deutlich voneinander abweichenden Bearbeitungszeiten für die Erstellung der beiden DNA-Identifizierungsmuster auf der unterschiedlichen Priorisierung der Ermittlungen. Während zur ersten minder

schweren Tat konkrete Beschuldigte bekannt gewesen seien, was keine besondere Dringlichkeit begründet habe, hätten bei der zweiten Straftat Anhaltspunkte dafür bestanden, dass sie mit weiteren, schweren Straftaten in Verbindung stand, weshalb eine zügige Analyse der Spuren geboten gewesen sei. Danach war das zunächst mit Blick auf den chronologischen Ablauf fragliche Vorgehen der Polizei nicht zu beanstanden. Die Polizei bestätigte mir, dass das im ersten Verfahren erhobene DNA-Identifizierungsmuster des Petenten nicht für Zwecke künftiger Strafverfolgung gespeichert werde.

Was ist zu beachten?
Die Vorschriften der §§ 81a ff. StPO regeln detailliert, in welchem Umfang und für welche Zwecke die aus körperlichen Untersuchungen und Analysen erlangten Daten in strafprozessualen Verfahren verwendet werden dürfen.

8.4 Erstellen von Listen mit personenbezogenen Daten von Beschuldigten/Tatverdächtigen und Übermittlung an die Bundespolizei

↗ §§ 79 Abs. 2 Satz 1 Nr. 2a, 80 Abs. 2 Nr. 2 und 3, 84 Abs. 1 SächsPVDG

Ein Petent wandte sich an mich mit dem Vortrag, eine Polizeidirektion (PD) würde regelmäßig eine Liste in Tabellenform zusammenstellen, welche Personen mit Namen, Geburtsdatum und Foto sowie aktuelle Ereignisse und Hinweise auf bisherige Vorkommnisse enthalte. Diese Liste würde regelmäßig behördenintern verteilt sowie an die Bundespolizei per E-Mail gesendet. Die von mir um Stellungnahme gebetene PD bestätigte den Sachverhalt. Bei der Liste handle es sich um die Schwerpunktlage (Darstellung von „nach sachgerechter Bewertung und Gefahrenprognose" ausgewählten Delikten der vorangegangenen Woche mit aktuellen Tatverdächtigen) im Zuständigkeitsbereich des verantwortlichen Polizeireviers, welche auch an die benachbarte Bundespolizeiinspektion übersandt werde. Als Zweck der wöchentlich erstellten und per E-Mail innerhalb der Dienststelle und an die Bundespolizeiinspektion versandten Liste gab die PD zum einen pauschal Gefahrenabwehr, zum anderen Gefahrenvorsorge an.

Erstellen der Liste und interne Weitergabe

Die in der Liste zusammengestellten personenbezogenen Daten der Beschuldigten hat die Polizeibehörde im Rahmen der Verfolgung von Straftaten gewonnen. Eine Weiterverarbeitung dieser Daten, hier in Form der Listenerstellung, ist gemäß § 80 Abs. 2 Nr. 2 Sächsisches Polizeivollzugsdienstgesetz (SächsPVDG) nur zulässig, soweit eine Gefahrenlage besteht. Nach § 4 Nr. 3a SächsPVDG liegt eine solche bei einer Sachlage vor, bei der im Einzelfall die hinreichende Wahrscheinlichkeit besteht, dass in absehbarer Zeit ein Schaden für die öffentliche Sicherheit oder Ordnung eintreten wird. Allgemeine kriminalpolizeiliche Erkenntnisse oder kriminalistische Erfahrung reichen hierfür nicht. Trotz mehrfacher Nachfragen war für mich nicht ersichtlich und wurde von der PD auch nicht plausibel dargelegt, wie die Zusammenstellung dieser personenbezogenen Daten von Beschuldigten Gefahren, zum Beispiel die konkrete zu befürchtende Begehung erneuter Straftaten durch die aufgelisteten Personen, verhindern könne.

Die Weiterverarbeitung von Daten von Personen, die einer Straftat verdächtig sind, zum Zweck der Gefahrenabwehr ist gemäß § 80 Abs. 2 Nr. 3 SächsPVDG zulässig, wenn dies erforderlich ist, weil wegen besonderer Erkenntnisse Grund zu der Annahme besteht, dass zukünftig Strafverfahren gegen sie zu führen sind. Zwar mag bei den aufgelisteten Personen eine gewisse Wahrscheinlichkeit der Begehung weiterer, gleichgelagerter Straftaten in absehbarer Zeit vorliegen, jedoch war für mich nicht ersichtlich, wie diese komprimierte Darstellung und Verteilung innerhalb der verantwortlichen Polizeibehörde weitere Straftaten verhindern kann, zumal die betroffenen Personen bereits polizeibekannt waren und es hierzu einschlägige Eintragungen im polizeilichen Auskunftssystem gab. Auch wäre eine Weitergabe dieser Informationen zur Verhütung weiterer Straftaten unter den oben genannten Voraussetzungen allenfalls – etwa, wenn diese Personen dort noch nicht bekannt sind – an den mit Gefahrenabwehraufgaben betrauten Streifendienst denkbar. Sollte Zweck dieser Übermittlung eine Art Überwachung dieser

Personen (im Sinne einer polizeilichen Beobachtung oder Observation) oder ein Ansprechen oder eine Kontrolle dieser bei Antreffen im Stadtgebiet sein, um die Person hierdurch an der Begehung der Straftat zu hindern, wäre dies nur unter den jeweiligen gesetzlichen Anforderungen zulässig (vgl. §§ 13, 15, 60 SächsPVDG).
Das Erstellen der wöchentlichen Liste (Schwerpunktlage) mit Aufnahme der aktuellen Tatverdächtigen halte ich daher für unzulässig und datenschutzwidrig.

Weiterleitung der Liste an die Bundespolizeiinspektion

Nach § 84 Abs. 1 SächsPVDG kann die Polizei unter Beachtung des § 79 Abs. 2 bis 4 SächsPVDG an die Polizeidienststellen anderer Länder oder des Bundes personenbezogene Daten übermitteln, soweit dies zur Erfüllung ihrer Aufgaben oder zur Erfüllung der Aufgaben des Empfängers erforderlich ist. Gemäß § 79 Ab. 2 Satz 1 Nr. 2a SächsPVDG ist eine Übermittlung nur im Einzelfall aufgrund konkreter Ermittlungsansätze zur Verhütung oder Verfolgung vergleichbarer Straftaten zulässig. Hierfür wären aber vor der Übermittlung jedes Einzelfalls Erkenntnisse notwendig, dass die übermittelte Person auch im Zuständigkeitsbereich des Empfängers, hier der Bundespolizeiinspektion, aktiv (Gefahrenabwehr) oder für dortige Ermittlungsverfahren relevant ist und die Übermittlung für deren Aufgabenerfüllung erforderlich ist. Nach der mir seitens des Petenten zur Verfügung gestellten Stellungnahme der Bundespolizeiinspektion prüft diese nach Erhalt der Liste zum einen, ob die darin erhaltenen Informationen für laufende Ermittlungsverfahren relevant sind. Sofern Zusammenhänge erkannt werden, wird Kontakt zu dem verantwortlichen Ermittlungsbeamten der PD aufgenommen. Zum anderen werde geprüft, ob die in der Schwerpunktlage mitgeteilten Erkenntnisse den eigenen Aufgabenbereich betreffen und sich hieraus Auswirkungen auf den Streifendienst und die Schwerpunktsetzung ergeben. Hieraus wird deutlich, dass bei der Übermittlung noch gar nicht feststeht, dass die Liste bzw. konkret die Angabe der aktuellen Tatverdächtigen für die Aufgaben der Bundespolizei erforderlich

ist. Eine Übermittlung „ins Blaue hinein" aber, auf Vorrat und ohne konkreten Anlass (für die eigene Aufgabenerfüllung oder auf Anforderung bei Bedarf der anderen Dienststelle) ist unzulässig.

Ein In-Kenntnis-Setzen anderer Dienststellen von aktuellen Tatverdächtigen wäre unter den Voraussetzungen einer Maßnahme nach § 60 SächsPVDG (Ausschreibung zur polizeilichen Beobachtung und zur gezielten Kontrolle) zulässig. Unterhalb der genannten Schwellen ist eine Übermittlung von personenbezogenen Daten von Tatverdächtigen unzulässig. Die Übermittlung der Schwerpunktlage mit den Daten der Tatverdächtigen entspricht nicht den gesetzlichen Anforderungen.

Ich habe die verantwortliche PD daher aufgefordert, die Praxis umgehend zu beenden, was mir vom Polizeipräsidenten zeitnah zugesichert wurde.

Was ist zu beachten?
Ein Zusammenstellen personenbezogener Daten, die die Polizei im Rahmen der Verfolgung von Straftaten gewonnen hat, außerhalb polizeilicher Datenbanken sowie deren interne Weitergabe und Übermittlung an Polizeidienststellen anderer Länder oder des Bundes ist nur unter den gesetzlichen Voraussetzungen des SächsPVDG zulässig, wobei die Erforderlichkeit der Daten für die Erfüllung einer konkreten Aufgabe maßgeblich ist.

8.5 Kontrolle besonderer polizeilicher Maßnahmen

↗ § 94 SächsPVDG, §§ 59 bis 69 SächsPVDG, § 74 Abs. 1 SächsPVDG in Verbindung mit § 12 Abs. 1 SächsDSUG, § 78 SächsPVDG

Zum 1. Januar 2020 trat das Sächsische Polizeivollzugsdienstgesetz (SächsPVDG) in Kraft und löste das bis dahin gültige Sächsische Polizeigesetz (SächsPolG) ab. Neben der Schaffung neuer Eingriffsbefugnisse für den Polizeivollzugsdienst insbesondere zur Abwehr erheblicher Gefahren und zur Verhütung schwerer/terroristischer Straftaten – etwa Maßnahmen zur Telekommunikationsüberwachung und zur elektronischen Aufenthaltsüberwachung („elektronische Fußfessel") – fand auch das Erfordernis von regelmäßigen datenschutzrechtlichen Kontrollen in Bezug auf besonders eingriffsintensive Maßnahmen Einzug in das SächsPVDG. Nach § 94 SächsPVDG obliegt mir seitdem die Durchführung von regelmäßigen Kontrollen in Bezug auf die Datenverarbeitung bei polizeilichen Maßnahmen nach den §§ 59 bis 69 SächsPVDG. Bei den besagten Maßnahmen handelt es sich hauptsächlich um verdeckte polizeiliche Maßnahmen, wie

die längerfristige Observation, den Einsatz technischer Mittel zur Videoüberwachung, die elektronische Aufenthaltsüberwachung oder die Telekommunikationsüberwachung. Datenschutzkontrollen gemäß § 94 SächsPVDG wurden im Berichtszeitraum erstmalig durchgeführt.

Auf meine Anfrage informierte mich das Sächsische Staatsministerium des Innern über die in den Jahren 2020 und 2021 von der Polizei gemeldeten polizeilichen Maßnahmen nach den §§ 59 bis 69 SächsPVDG. Daraus ergab sich, dass im Jahr 2020 insgesamt 23 und im Jahr 2021 insgesamt 29 Maßnahmen dieser Art durchgeführt wurden. Mit Blick auf die Intensität der Eingriffe wurden einige der Vorgänge ausgewählt und in Bezug auf die Rechtmäßigkeit der Datenverarbeitung überprüft. Dies erfolgte teils schriftlich, teils direkt in den Räumlichkeiten der Polizeidirektionen und des Landeskriminalamts. Der Schwerpunkt der Kontrollen lag auf der Überprüfung der ordnungsgemäßen Beantragung und Anordnung der Maßnahmen, deren Durchführung sowie auf der Benachrichtigung der Betroffenen und der Löschung von personenbezogenen Daten nach Abschluss der Maßnahmen. Die Ergebnisse der Kontrollen variierten dabei sehr stark: Während in vielen Fällen die Vorschriften des SächsPVDG korrekt angewendet wurden und den hohen gesetzlichen Anforderungen an die Rechtmäßigkeit der Datenverarbeitung Rechnung getragen wurde, musste ich auch einige, teilweise gravierende Defizite in der Vorbereitung, Umsetzung und Nachbereitung der Maßnahmen feststellen.

Anträge auf Anordnung bestimmter Maßnahmen

Ein wesentlicher Kritikpunkt bestand in der Beantragung der polizeilichen Maßnahmen. Die konkreten Anforderungen an den Antrag sind in den Einzelvorschriften der Maßnahmen nach §§ 59 bis 69 SächsPDVG festgehalten. In mehreren Fällen enthielten die Anträge keine oder nur unzureichende Angaben zu Art und Umfang der geplanten Maßnahme und zur Begründung. Auch habe ich festgestellt, dass Maßnahmen für Zeiträume beantragt wurden, welche die gesetzlich normierte Höchstdauer weit überschritten. Die Mängel in

den Anträgen wurden teilweise von den anordnenden Stellen übernommen und zogen sich in Einzelfällen bis in die gerichtlichen Anordnungen fort.

Um die Rechtmäßigkeit einer Maßnahme beurteilen zu können, ist eine ordnungsgemäße Beantragung jedoch unerlässlich. Der Antrag muss die anordnende Stelle gewissermaßen „auf einen Blick" in Kenntnis darüber setzen, ob bzw. dass die gesetzlichen Voraussetzungen für eine Anordnung vorliegen. Daneben dient er – in einem ersten Schritt – auch der Selbstkontrolle der beantragenden Stelle.

Durchführung der Maßnahmen

Erfreulicherweise konnte ich feststellen, dass die Durchführung der polizeilichen Maßnahmen in der ganz überwiegenden Zahl der geprüften Fälle den gesetzlichen Anforderungen entsprach. Hiervon auszunehmen ist eine Maßnahme, die als Überwachung eines Hotels beabsichtigt war. Die verantwortliche Polizeidirektion beantragte beim zuständigen Amtsgericht eine Anordnung des Einsatzes technischer Mittel zur Datenerhebung aus Wohnungen nach § 65 SächsPVDG, die so auch erlassen wurde. Tatsächlich wurden später aber der Eingangsbereich des Hotels (außerhalb des Gebäudes) sowie die sich daneben befindlichen Parkflächen vor dem Hotel überwacht. Dabei handelt es sich ohne Zweifel nicht um Wohnraum, sondern um öffentlich zugängliche Bereiche. Die tatsächlich vorgenommene Datenerhebung konnte daher nicht auf die Anordnung des zuständigen Amtsgerichts gestützt werden; eine andere Rechtsgrundlage ist nicht erkennbar und wurde auch im Rahmen der Datenschutzkontrolle nicht vorgetragen. Bei einer Überwachung öffentlichen Raums durch den Einsatz technischer Mittel handelt es sich um einen nicht unerheblichen Eingriff in die Grundrechte der Betroffenen. Eine hierfür fehlende Rechtsgrundlage kann auch nicht durch die richterliche Anordnung einer deutlich eingriffsintensiveren Maßnahme (Wohnraumüberwachung) ersetzt werden, wenn – wie hier – die tatsächlich durchgeführte Datenerhebung nicht mit den gesetzlichen Voraussetzungen der angeordneten Maßnahme

übereinstimmt und einen völlig anderen Lebenssachverhalt mit ganz anderen potenziell betroffenen Personen betrifft.

Benachrichtigung betroffener Personen

Ein weiterer Schwerpunkt der Kontrollen lag auf der Benachrichtigungspflicht der verarbeitenden Stelle. Gemäß § 74 Abs. 1 Satz 1 SächsPVDG sind die von den Maßnahmen nach §§ 59 bis 69 SächsPVDG betroffenen Personen nach Abschluss der Maßnahme über diese zu benachrichtigen. Die Anforderungen an die Benachrichtigung sind in § 74 Abs. 1 Satz 2 SächsPVDG geregelt. In mehreren Fällen stellte ich fest, dass die Benachrichtigungen nicht den gesetzlichen Anforderungen der genannten Vorschrift entsprachen. Insbesondere fehlten in den Benachrichtigungsschreiben die erforderlichen Angaben nach § 12 Abs. 1 Sächsisches Datenschutz-Umsetzungsgesetz (SächsDSUG), darunter zum Beispiel die Angabe der Rechtsgrundlage der Datenverarbeitung, der Speicherdauer sowie der Rechte der Betroffenen.

Die Bereitstellung der gesetzlich vorgeschriebenen Angaben im Rahmen der Benachrichtigung ist in jedem Fall zu beachten. Die Angaben sollen die betroffene Person in die Lage versetzen, bereits selbst die Rechtmäßigkeit der Maßnahme einschätzen und die Inanspruchnahme ihrer Rechte prüfen zu können.

Löschung der durch die Maßnahmen erlangten Daten

Sind die im Rahmen der Maßnahmen erhobenen Daten nicht mehr für die polizeiliche Arbeit und eine eventuelle gerichtliche Überprüfung erforderlich, sind sie gemäß § 78 Abs. 1 Satz 1 SächsPVDG unverzüglich zu löschen. Dieser Verpflichtung zur unverzüglichen Löschung wurde nicht in allen Fällen nachgekommen. So waren zum Beispiel im Fall einer Telekommunikationsüberwachung auch lange Zeit nach Abschluss der Maßnahme noch alle erhobenen Daten vollständig vorhanden, da man die Daten für den möglichen Fall zukünftiger neuer Erkenntnisse vorhalten wollte. Die Speicherung von Daten über einen für den konkreten erforderlichen Zweck hinausgehenden Zeitraum ist jedoch nicht mit

der Vorschrift des § 78 Abs. 1 Satz 1 SächsPVDG vereinbar und damit rechtswidrig.
In einigen Fällen war die Löschung entgegen der gesetzlichen Vorgabe in § 78 Abs. 1 Satz 2 SächsPVDG nicht dokumentiert. Teilweise wurde – ebenfalls entgegen der speziellen gesetzlichen Bestimmung der unverzüglichen Löschung – auf allgemeine Aufbewahrungsfristen verwiesen.
Im Ergebnis der Kontrollen habe ich die betroffenen Polizeistellen auf die von mir festgestellten Fehler in der Anwendung der Vorschriften des SächsPVDG hingewiesen und dringend um Beachtung der gesetzlichen Anforderungen gebeten. Über meine Feststellungen habe ich auch das Sächsische Staatsministerium des Innern als zuständige oberste Aufsichtsbehörde informiert. Gemeinsam mit dem Staatsministerium wurden Möglichkeiten und Wege erörtert, wie zukünftig die Beachtung der gesetzlichen Anforderungen und damit die Rechtmäßigkeit der Datenerhebung und -verarbeitung durch die Polizei sichergestellt werden können. Ich habe in diesem Zuge die Erstellung von einheitlichen Prüfschemata und Mustern für die Beantragung, Durchführung und Nachbereitung der Maßnahmen angeregt. Solche Muster werden derzeit durch das Staatsministerium erarbeitet und sollen nach Fertigstellung der Polizei zur Verfügung gestellt werden.

Was ist zu beachten?
Bei der Durchführung polizeilicher Maßnahmen ist die Einhaltung der gesetzlichen Anforderungen zwingend erforderlich. Die Beachtung gesetzlicher Vorgaben ist Grundlage rechtsstaatlichen Handelns und dient dem Schutz der Betroffenen und der Gewährleistung ihrer Rechte.

8.6 Polizeiliche Videoüberwachung an Straßen im Grenzgebiet

↗ §§ 57, 58, 59 SächsPVDG, §§ 100h, 163f StPO

Die Bekämpfung und Verhütung grenzüberschreitender Kriminalität ist im Freistaat Sachsen mit seinen Grenzen zur Republik Polen im Osten und zur Tschechischen Republik im Süden eine wichtige polizeiliche Aufgabe.
Im Grenzgebiet zu Polen nutzt die zuständige Polizeidirektion Görlitz zunehmend Technik zur Videoüberwachung von öffentlichen Straßen und Wegen. Immer wieder ist die

Videoüberwachung Gegenstand der Presseberichterstattung. Im Berichtszeitraum stand ich in intensivem Kontakt mit der Polizeidirektion, wobei wiederholt die rechtlichen Voraussetzungen und Rahmenbedingungen für den Einsatz von Videotechnik zur Überwachung des öffentlichen Raums diskutiert wurden.

Im Folgenden möchte ich die rechtlichen Möglichkeiten der Videoüberwachung zur Verhütung und Verfolgung grenzüberschreitender Kriminalität darstellen und die jeweiligen datenschutzrechtlichen Schwierigkeiten erläutern.

Automatisierte Kennzeichenerfassung und -auswertung

Zur vorbeugenden Bekämpfung der grenzüberschreitenden Kriminalität ist der Einsatz technischer Mittel zur automatisierten Kennzeichenerkennung (AKES) nach § 58 Abs. 1 Nr. 4 Sächsisches Polizeivollzugsdienstgesetz (SächsPVDG) und unter den Voraussetzungen des § 15 Abs. 1 Nummer 4 SächsPVDG (Grenzgürtel von 30 km Tiefe) zulässig. Dabei werden Kraftfahrzeugkennzeichen sowie Informationen über Ort, Zeit und Fahrtrichtung – nicht aber Bilder von Personen – erfasst und die Kraftfahrzeugkennzeichen sofort und unmittelbar mit polizeilichen Datenbeständen automatisiert abgeglichen.

Liegt für das vollständig erfasste Kraftfahrzeugkennzeichen keine Datenübereinstimmung vor, sind die erfassten Daten sofort, technisch spurenlos und automatisiert zu löschen.

Aus den jährlichen Berichten der Staatsregierung über besondere Ermittlungsmaßnahmen der Polizei an den Sächsischen Landtag – zuletzt zum Kalenderjahr 2020, LT-Drs. 7/7167 – geht hervor, dass die Trefferquote bei AKES sehr gering ist. Statistisch wurde bei einer Durchschnittsdauer von 4,5 Stunden pro Einsatz weniger als ein Treffer (Übereinstimmung von erfasstem Kennzeichen und Datenbestand) registriert.

Der Einsatz von AKES ist aus datenschutzrechtlicher Sicht wenig problematisch, da erfasste Daten nicht länger als für einen sofortigen automatisierten Abgleich technisch notwendig gespeichert und im Fall fehlender Übereinstimmung

sofort und spurenlos gelöscht werden. Die große Streubreite der Maßnahme, die sich in einer Vielzahl zunächst erfasster Kennzeichen zeigt, wird durch diese gesetzlich bestimmten Verarbeitungsschritte in ihrer Eingriffswirkung abgemildert. Im Trefferfall ergänzen die erfassten Daten, die gespeichert werden dürfen, bereits bei der Polizei vorhandene Angaben.

Videoüberwachung zur Verhütung schwerer grenzüberschreitender Kriminalität unter Einsatz von Gesichtserkennungssoftware

Nach § 59 SächsPVDG darf die Polizei zur Verhütung bestimmter (schwerer) Formen grenzüberschreitender Kriminalität personenbezogene Daten durch den offenen Einsatz technischer Mittel zur Anfertigung von Bildaufzeichnungen des Verkehrs auf öffentlichen Straßen erheben sowie Informationen über Ort, Zeit und Verkehrsrichtung der Nutzung erfassen, um Bilder automatisiert mit bereits vorhandenen personenbezogenen Daten abzugleichen. Die erfassten Bilddaten dürfen einer biometrischen Verarbeitung zugeführt und – einmalig und ausschließlich – mit zuvor bestimmten Daten (Lichtbildern) von polizeilich zur Beobachtung ausgeschriebenen Personen abgeglichen werden.
Es handelt sich bei dieser Maßnahme gewissermaßen um eine Erweiterung des automatisierten Kennzeichenabgleichs um den Abgleich der Gesichtsbilder sämtlicher von den Kameras im überwachten Straßenabschnitt erfasster Personen. Der Eingriff in die Rechte der betroffenen Personen ist allerdings weitaus intensiver als bei der Erfassung lediglich eines Kfz-Kennzeichens. Die besondere Schwere des Eingriffs ergibt sich zudem aus der im Gesetz vorgesehenen Frist von 96 Stunden, innerhalb derer der automatisierte Abgleich erfolgen muss. Dass die erfassten Daten in dieser Frist nur einmal abgeglichen, bis dahin nicht anderweitig verwendet werden dürfen und im Fall fehlender Übereinstimmung automatisiert gelöscht werden müssen, kann den erheblichen Eingriff in das Recht einer großen Zahl allergrößtenteils unbeteiligter betroffener Personen, die keinerlei Anlass für eine polizeiliche Erfassung gegeben haben, nur unwesentlich abmildern.

Die seit dem 1. Januar 2020 in Kraft befindliche gesetzliche Vorschrift, die in der Praxis kaum zur Anwendung kommt, wird derzeit in einem am Sächsischen Verfassungsgerichtshof anhängigen Normenkontrollverfahren überprüft.
Von ungleich höherer praktischer Relevanz für die Arbeit der Polizei ist der Betrieb von Kameratechnik zur Überwachung auf Grundlage von § 57 Abs. 3 Nr. 2 SächsPVDG sowie – in laufenden strafprozessualen Ermittlungsverfahren – nach §§ 163f, 100h Strafprozessordnung (StPO), siehe dazu unten.

Überwachung von Kriminalitätsschwerpunkten

Auf der Grundlage von § 57 Abs. 3 Nr. 2 SächsPVDG kann die Polizei auf öffentlichen Straßen, Wegen oder Plätzen, wenn nach polizeilich dokumentierten Tatsachen die Kriminalitätsbelastung dort gegenüber der des Gemeindegebiets deutlich erhöht ist (Kriminalitätsschwerpunkte), personenbezogene Daten durch den offenen Einsatz technischer Mittel zur Anfertigung von Bild- und Tonaufnahmen oder -aufzeichnungen von Personen erheben, soweit Tatsachen die Annahme rechtfertigen, dass an diesen Orten künftig Straftaten begangen werden, durch die Personen, Sach- oder Vermögenswerte gefährdet werden.
Solch eine punktuelle Überwachung eines begrenzten öffentlichen Raums bedarf einer eingehenden Analyse des Kriminalitätsaufkommens und seiner Verteilung im gesamten Gemeindegebiet sowie einer auf Tatsachen gestützten polizeilichen Prognose.
Rechtfertigen vorliegende Fallzahlen und Erkenntnisse eine Videoüberwachung des als Kriminalitätsschwerpunkt identifizierten Ortes, darf die Polizei die erhobenen Daten speichern und muss sie gemäß § 57 Abs. 10 SächsPVDG spätestens nach einem Monat löschen oder vernichten, soweit sie nicht zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Geltendmachung von öffentlich-rechtlichen Ansprüchen oder zum Schutz privater Rechte, insbesondere zur Behebung einer bestehenden Beweisnot, erforderlich sind.
Eine Maßnahme nach § 57 Abs. 3 Nr. 2 SächsPVDG greift angesichts dessen, dass eine Vielzahl von Personen erfasst wird

und die gefertigten Bilder eine Identifizierung ermöglichen, tief in das Recht auf informationelle Selbstbestimmung der Betroffenen ein. Die im Bereich der Polizeidirektion Görlitz eingesetzte Technik liefert hochauflösende Aufnahmen, die eine biometrische Auswertung der Bilder im Nachgang – nicht aber direkt nach § 57 Abs. 3 Nr. 2 SächsPVDG – technisch zulassen und einen automatisierten Abgleich etwa für Zwecke der Strafverfolgung ermöglichen. Erfasst werden zudem Kfz-Kennzeichen, die über einen unkomplizierten Abruf der Halterdaten weitere personenbezogene Informationen liefern.

Umso dringender ist die Notwendigkeit, grundrechtsschonende Begleitmaßnahmen zu ergreifen. Ich habe dazu konkrete Vorschläge unterbreitet, wobei die Polizeidirektion bereits in ausdrücklich zu begrüßender Eigeninitiative bestimmte Maßnahmen ergriffen oder vorgesehen hat.

Die Schwere des Rechtseingriffs soll durch

- eine Deaktivierung der Aufnahmetechnik in bestimmten Zeiträumen (zum Beispiel Tageszeiten, an denen nach kriminalistischer Erfahrung kaum Straftaten begangen werden),
- sehr kurze Speicherfristen (Art und Umfang der geplanten Überwachung erfordern eine erhebliche Verkürzung der Monatsfrist des § 57 Abs. 10 SächsPVDG, die bereits nach dem Wortlaut – „spätestens" – eine Höchstfrist darstellt und damit die Erforderlichkeit einer Verhältnismäßigkeitsprüfung im Einzelfall und bezogen auf die konkrete Maßnahme unterstreicht) und
- eine deutlich sichtbare Abdeckung der Kameras in den Zeiträumen, in denen die Aufnahmetechnik inaktiv ist,

verringert werden. Darüber hinaus ist eine jährliche Prüfung des weiteren Vorliegens der Voraussetzungen für eine Maßnahme nach § 57 Abs. 3 Nr. 2 SächsPVDG einschließlich einer nachvollziehbaren Dokumentation des Ergebnisses der Prüfung vorzunehmen. Sollten die gesetzlich geforderten Voraussetzungen nicht mehr vorliegen, muss die Überwachung beendet werden.

Überwachung von Straßenabschnitten in konkreten strafprozessualen Verfahren

In laufenden Ermittlungsverfahren – also im Bereich der Strafverfolgung, in dem das SächsPVDG nicht zur Anwendung kommt – setzt die Polizeidirektion Kameratechnik zur Überwachung von Straßenabschnitten auf strafprozessualer Grundlage ein. Rechtsgrundlage sind dabei jeweils richterliche Anordnungen nach §§ 100h Abs. 1 Nr. 1, 163f StPO. Die Polizeidirektion teilte mir mit, dass lediglich nachweislich verdachtsrelevante Recherchebestandteile (Aufzeichnungssequenzen) zur Ermittlungsakte genommen würden. Der weitaus größere Anteil von Bilddaten unbeteiligter Dritter werde dagegen schon nach wenigen Tagen gelöscht. Ein biometrischer Abgleich von Aufnahmen mit Referenzbildern werde äußerst selten und ausschließlich auf richterliche Anordnung nach § 98a StPO vorgenommen.

Aus datenschutzrechtlicher Sicht bestehen erhebliche Bedenken gegen die unter Umständen mehrwöchige oder mehrmonatige Überwachung einer öffentlichen Straße mit hohem Verkehrsaufkommen auf strafprozessualer Grundlage. Anders als bei einer gezielten Beobachtung bzw. Observation einer bzw. eines Beschuldigten, einer anderen konkreten Person oder eines einzelnen baulichen Objekts mit einem überschaubaren Kreis betroffener Personen – auf diese Konstellationen zielen die Vorschriften in §§ 100h und 163f StPO ab –, bei der eine vergleichsweise geringe Zahl unbeteiligter Dritter erfasst wird und bei „unvermeidbarer Betroffenheit" auch ausdrücklich erfasst werden darf, wird bei der Fertigung hochauflösender Bildaufnahmen des gesamten fließenden Verkehrs inklusive Fahrzeugkennzeichen und -insassen auf einer (Bundes-) Straße von vornherein nahezu ausschließlich in die Rechte unbeteiligter Dritter eingegriffen.

Meine Bedenken beruhen auch auf den Ausführungen des Bundesverfassungsgerichts zur Verhältnismäßigkeit des Einsatzes von automatisierten Kennzeichenlesesystemen zu präventiv-polizeilichen Zwecken (Beschlüsse vom 18.12.2018 – 1 BvR 142/15, 1 BvR 2795/09, 1 BvR 3187/10; BVerfGE 150, 244) und werden durch die klare Position des Bundesgesetz-

gebers, die dieser im Rahmen des Gesetzgebungsverfahrens zur strafprozessualen Befugnis zum Einsatz von automatisierten Kennzeichenlesesystemen zur Strafverfolgung nach § 163g StPO formuliert hat, verstärkt (BT-Drs 19/27654, Seite 84ff.).

Soweit polizeiliche Maßnahmen auf richterliche Anordnung erfolgen, sind meine datenschutzaufsichtsbehördlichen Befugnisse begrenzt, da ich für die Aufsicht über die von den Gerichten im Rahmen ihrer justiziellen Tätigkeit vorgenommenen Verarbeitungen nicht zuständig bin, § 37 Abs. 2 Sächsisches Datenschutz-Umsetzungsgesetz. Danach steht mir auch eine datenschutzrechtliche Prüfung der Entscheidungen unabhängiger Gerichte nicht zu.

Dieser Umstand ändert nichts daran, dass ich gegenüber der letztlich handelnden Polizei dringende Empfehlungen zur Ergreifung grundrechtsschützender Maßnahmen aussprechen kann. Darüber hinaus ist für die (Weiter-)Verarbeitung der Daten nach der richterlich angeordneten Erhebung meine Aufsichtszuständigkeit nicht beschränkt. Auch im Fall des Einsatzes der Kameratechnik auf strafprozessualer Grundlage verfolgen meine Empfehlungen und die polizeiseitig bereits ergriffenen oder vorgesehenen Maßnahmen dasselbe Ziel. Durch ganz ähnliche Maßnahmen wie beim präventiven Kameraeinsatz (Deaktivierung der Aufnahmetechnik in bestimmten Zeiträumen; schnellstmögliche Löschung der Bilddaten für das Ermittlungsverfahren irrelevanter Personen, Abdeckung der Kamerafenster in Phasen der Inaktivität) soll die Schwere des Eingriffs in das Grundrecht einer großen Zahl betroffener und für die Strafverfolgung irrelevanter Personen abgemildert werden.

Eine schnellstmögliche Löschung des für das Ermittlungsverfahren irrelevanten Bildmaterials ist dabei weniger Kulanz als verfassungsrechtlich erforderlich und gesetzlich geboten. Die gesetzlichen Speicherbefugnisse knüpfen ausnahmslos an die Erforderlichkeit der Daten für die Aufgabenerfüllung an. Nicht verfahrensrelevante Daten sind für die Erfüllung polizeilicher Aufgaben selbstverständlich nicht erforderlich. Besondere Bedeutung und Relevanz gewinnen diese Vor-

Was ist zu tun?
Bei der polizeilichen Videoüberwachung des öffentlichen Raums werden ganz überwiegend personenbezogene Daten von Betroffenen erhoben und verarbeitet, die für die Aufgabenerfüllung der Polizei ohne Bedeutung sind. Je nach Art der Überwachung sind Maßnahmen vorzusehen, um den Eingriff in die Rechte dieser Personen so gering wie möglich zu halten.

schriften dann, wenn Daten unbeteiligter Dritter und ohne Verfahrensrelevanz in großem Umfang erhoben und – zunächst – gespeichert werden. In diesen Fällen begründet schon die Art der Erhebung einen besonderen Einzelfall, der eine unmittelbar anschließende Prüfung der Erforderlichkeit der Speicherung im Einzelfall gebietet (vgl. § 91 Abs. 2 SächsPVDG).
Im Hinblick auf die fortlaufende Überprüfung der Erforderlichkeit der Überwachungsmaßnahmen und die Umsetzung der erwähnten grundrechtsschonenden Begleitmaßnahmen werde ich mit der Polizeidirektion Görlitz in engem Austausch bleiben.

8.7 Übermittlungen personenbezogener Daten durch die Sächsische Polizei an eine nichtöffentliche Stelle

↗ § 84 Abs. 4 Nr. 1 SächsPVDG

Im Rahmen der Petitionsbearbeitung habe ich mich auch mit der Frage der Rechtmäßigkeit der Übermittlung personenbezogener Daten durch die Sächsische Polizei an eine nichtöffentliche Stelle gemäß § 84 Abs. 4 Nr. 1 Sächsisches Polizeivollzugsdienstgesetz (SächsPVDG) beschäftigt.
Nach § 84 Abs. 4 Nr. 1 SächsPVDG kann die Polizei auf Ersuchen einer nichtöffentlichen Stelle (zum Beispiel Privatperson) personenbezogene Daten übermitteln, soweit diese ein rechtliches Interesse an der Kenntnisnahme der zu übermittelnden Daten glaubhaft macht und kein Grund zu der Annahme besteht, dass schutzwürdige Interessen des Betroffenen überwiegen. Ein rechtliches Interesse der Ersuchenden ist zu bejahen, wenn die Daten für die Feststellung, Durchsetzung oder Verteidigung von Rechten oder Ansprüchen, sprich für die Rechtswahrung benötigt werden. Zur Glaubhaftmachung muss der Antragsteller – auch im Hinblick auf die vorzunehmende Abwägung mit den schutzwürdigen Interessen der betroffenen Person – jedenfalls eine gewisse

Schlüssigkeit dafür dartun, dass die angeforderten Daten für die Rechtsverfolgung benötigt werden. Der Polizeibehörde ist demgegenüber nicht abzuverlangen, eine bis ins Letzte gehende Vorprüfung der geltend gemachten rechtlichen Belange des um die Übermittlung der Daten Nachsuchenden vorzunehmen (Verwaltungsgericht Gelsenkirchen, Urteil vom 23.03.2020 – 17 K 3482/16; Oberverwaltungsgericht Sachsen, Urteil vom 10.11.2016 – 3 A 318/16). Zwei Fälle sollen beispielhaft skizzieren, welche Abwägungen vorzunehmen sind, bevor personenbezogene Informationen aus dem Datenbestand der Polizei an nichtöffentliche Stellen übermittelt werden und damit aus dem Bereich staatlicher Kontrolle fallen.

Daten über einen Fahrzeughalter

In einer Beschwerde hatte eine Rechtsanwaltskanzlei in Vertretung ihrer Mandantschaft einen Antrag zur Halterabfrage zum Kfz-Kennzeichen des Fahrzeugs des Petenten bei der Sächsischen Polizei gestellt. Die Kanzlei stützte ihren Antrag zuvorderst auf die Geltendmachung von Unterlassungsansprüchen gemäß §§ 1004 Abs. 1 Satz 2, 823 Abs. 1 Bürgerliches Gesetzbuch (BGB) gegen die Veröffentlichung einer Abbildung des Hauses ihrer Mandantschaft. Zudem seien mögliche Rechtsverletzungen nach § 201a Strafgesetzbuch (StGB) und § 33 in Verbindung mit §§ 22, 23 Kunsturhebergesetz (KunstUrhG) denkbar. Der Petent, ein Fotojournalist, habe von der Straße aus Lichtbilder vom Haus der Mandantschaft gemacht und sei dabei von der Hauseigentümerin beobachtet worden, die das Kfz-Kennzeichen notiert habe. Bei Veröffentlichung der Fotos des Hauses in Verbindung mit der Adresse/dem Namen der Mandantschaft sei eine besondere Gefährdung der Familie zu befürchten, welche sich aus der beruflichen Position des Hauseigentümers ergebe. Die Polizeibehörde gab dem Antrag statt und übermittelte den vollständigen Namen sowie die Adresse des Petenten an die Kanzlei. Der Petent bat um datenschutzrechtliche Überprüfung dieses Vorgehens.

Nach meiner Sicht ist das rechtliche Interesse der Kanzlei an der Kenntnis der übermittelten personenbezogenen Daten des Petenten als grenzwertig einzuordnen. Außenaufnahmen eines Gebäudes sind nach ständiger Rechtsprechung zulässig und keine Beeinträchtigung der Persönlichkeitsrechte, sofern die Abbildung von allgemein zugänglichen Orten, wie hier einer öffentlichen Straße, außerhalb des fremden Grundstücks bzw. Gebäudes und nicht unter Überwindung bestehender Hindernisse oder mit geeigneten Hilfsmitteln (zum Beispiel Leiter, Drohne) angefertigt wird. Daher scheidet eine strafbare Handlung des Petenten gemäß § 201a Strafgesetzbuch (StGB) durch Verletzung des höchstpersönlichen Lebensbereichs und von Persönlichkeitsrechten durch Bildaufnahmen aus. Der Unterlassungsanspruch gemäß §§ 1004 Abs. 1 Satz 2, 823 Abs. 1 Bürgerliches Gesetzbuch (BGB) sowie eine Rechtsverletzung nach dem Kunsturhebergesetz beziehen sich auf eine eventuelle Veröffentlichung der Fotografien, die die Kanzlei der Polizeibehörde glaubhaft gemacht haben müsste. Die Polizeibehörde ist indes gemäß § 84 Abs. 4 Nr. 1 SächsPVDG verpflichtet, eine ermessensfehlerfreie Entscheidung zu treffen und dabei die rechtlichen Interessen des Antragstellers gegenüber dem Recht des Betroffenen auf informationelle Selbstbestimmung abzuwägen. Das Recht auf informationelle Selbstbestimmung darf im überwiegenden Interesse der Allgemeinheit und unter Beachtung des Grundsatzes der Verhältnismäßigkeit durch Gesetz oder aufgrund eines Gesetzes eingeschränkt werden; die Einschränkung darf nicht weiter gehen als es zum Schutz des öffentlichen Interesses unerlässlich ist (BVerfG, Beschluss vom 29.09.2013 – 2 BvR 939/13). Das Grundrecht auf informationelle Selbstbestimmung gebietet dabei insbesondere eine Auslegung des einfachen Rechts, bei der abschreckende Effekte auf den Gebrauch des Grundrechts möglichst gering gehalten werden. Hiergegen verstieße es, wenn das Anfertigen von Lichtbildern oder Videoaufnahmen eines Wohngebäudes unter Verweis auf die bloße Möglichkeit einer nachfolgenden strafbaren Verletzung des Rechts am eigenen Bild (nach § 22 Satz 1, § 33 Abs. 1 KunstUrhG)

genügen sollten, um einen Anspruch nach § 84 Abs. 4 Nr. 1 SächsPVDG geltend machen zu können.

Da eine Übermittlung personenbezogener Daten durch eine Polizeibehörde gemäß § 84 Abs. 4 Nr. 1 SächsPVDG grundsätzlich ein Eingriff in das Recht auf informationelle Selbstbestimmung der bzw. des Betroffenen ist, bedarf es zumindest der Glaubhaftmachung einer konkreten Gefahr einer Rechtsverletzung. Dies ist eine Frage der tatsächlichen Umstände im Einzelfall. Dementsprechend geht die verwaltungsrechtliche Rechtsprechung grundsätzlich in verfassungskonformer Auslegung der §§ 22, 23 KunstUrhG davon aus, dass selbst unzulässige Lichtbilder nicht auch stets verbreitet werden (BVerwG, Urteil vom 14.07.1999 – 6 C 7.98). Es mussten daher konkrete Anhaltspunkte dafür bestehen, dass die durch den Petenten gefertigten Lichtbilder entgegen den Vorschriften des Kunsturhebergesetzes unter Missachtung des Rechts der Mandantschaft am eigenen Bild auch veröffentlicht werden.

Auf eine besondere Gefährdungslage hinsichtlich der Verbreitung des Bildmaterials ist gerade nicht aus der Tätigkeit des Petenten als Fotojournalist zu schließen. Es lagen hier keine Anhaltspunkte dafür vor, dass der Petent seine Bildaufnahmen widerrechtlich und in strafbarer Weise hat veröffentlichen wollen. Die Kanzlei hat konkrete Anhaltspunkte nicht benennen können, sondern lediglich vermutet, der Petent werde Bildnisse in unzulässiger Weise verbreiten. Zudem ist anzunehmen, dass Fotojournalisten die rechtlichen Grenzen bekannt sind, unter denen nach dem Kunsturheberrechtsgesetz Bildnisse zulässigerweise veröffentlicht werden dürfen, sodass gerade bei Angehörigen dieses Berufs besondere Umsicht im Umgang mit der Veröffentlichung von Fotomaterial angenommen und erwartet werden kann (Verwaltungsgericht Dresden, Urteil vom 11.11.2021 – 6 K 315/21).

Ich habe die betroffene Polizeibehörde gebeten, den Vorgang zum Anlass zu nehmen, Bedienstete insoweit zu sensibilisieren, den ihnen in § 84 Abs. 4 Nr. 1 SächsPVDG vom Gesetzgeber eingeräumten Beurteilungs- und Entschließungsfreiraum ermessensfehlerfrei dahingehend zu nutzen, eine fundierte, das

heißt anhand konkreter Anhaltspunkte für eine konkrete Gefährdungslage und nachvollziehbare Abwägung zwischen den vom Antragsteller dargelegten rechtlichen Interessen und dem Recht auf informationelle Selbstbestimmung des Betroffenen zu treffen. Letzteres darf keinesfalls lediglich aufgrund allgemeiner Erwägungen, wie beispielsweise dass einmal an die Öffentlichkeit gelangte Informationen nur schwerlich und überhaupt nicht widerruflich seien, grundsätzlich zurückstehen.

Herausgabe personenbezogener Daten der Mitarbeiterin einer Bank

In einer anderen Petition beschwerte sich die Mitarbeiterin einer Bank, die dort für Meldungen über verdächtige Kontobewegungen nach § 43 Abs. 1 Geldwäschegesetz (GwG) zuständig war, über die Nennung ihres Namens und ihrer Telefondurchwahl durch die Polizei gegenüber der betroffenen Bankkundin und kontoführenden Person. Die Bankmitarbeiterin stand im Zuge der Meldung, zu der die Bank gesetzlich verpflichtet ist, im Austausch mit der Polizei, der ihre Kontaktdaten dadurch bekannt waren. Die Polizei wiederum war im Zuge ihrer Bearbeitung des Vorgangs auch mit der betroffenen Bankkundin in Kontakt und bat diese, sich mit ihrer Bank in Verbindung zu setzen. Die Bankkundin – die, wie sich herausstellte, selbst Geschädigte einer Straftat war – bat die Polizei um Kontaktdaten der Bank; ein Schreiben an die Bank sei unbeantwortet geblieben. In einem hierzu geführten Gespräch zwischen der Polizei und der Bankmitarbeiterin lehnte Letztere eine direkte Kontaktaufnahme mit der Kundin ausdrücklich ab und verwies auf die allgemeinen Kontaktdaten der Bank. Dessen ungeachtet teilte die Polizei der Bankkundin den Namen und die dienstliche Durchwahl der Bankmitarbeiterin telefonisch mit.

Auf meine Nachfrage gab die Polizei § 84 Abs. 4 Nr. 1 SächsPVDG als Grundlage für die Datenübermittlung an. Die Bankkundin habe die Kontaktdaten der Mitarbeiterin der Bank begehrt, um schnellstmöglich bestimmte Buchungen zu ermöglichen und die Geschäftsbeziehung zur weiteren Schadensvermeidung mit der Bank aufzulösen. Ein Grund

für das Vorliegen schutzwürdiger Interessen der Bankangestellten an der Nichtübermittlung der dienstlichen Telefonnummer und des Namens sei nicht ersichtlich gewesen. Im Übrigen habe die Datenübermittlung auch den Vorgaben von § 84 Abs. 3 Nr. 1 SächsPVDG entsprochen, da sie den Zweck gehabt habe, weitere Straftaten im Zusammenhang mit dem betreffenden Konto zu verhindern.

Die Voraussetzungen von § 84 Abs. 4 Nr. 1 SächsPVDG lagen tatsächlich jedoch nicht vor. Bereits die ausdrückliche Verweigerung der Zustimmung der Bankmitarbeiterin zu einer direkten Kontaktaufnahme mit der Kundin stand einer Übermittlung des Namens und der Kontaktdaten der Bankmitarbeiterin entgegen. Ein überwiegendes schutzwürdiges Interesse der Bankangestellten am Unterbleiben der Übermittlung ergab sich zudem aus der gesetzgeberischen Wertung des § 49 Geldwäschegesetz (GwG). Der Gesetzgeber hat darin bestimmt, dass die personenbezogenen Daten der Einzelperson, die die Meldung nach § 43 Abs. 1 GwG abgegeben hat, besonders zu schützen sind, um Bedrohungen und Anfeindungen zu verhindern. Auch wenn das Verbot der Offenlegung von Angaben zu diesen Personen anlässlich von Auskunftsersuchen Betroffener nicht die Strafverfolgungsbehörden bzw. Polizei unmittelbar adressiert, muss die gesetzgeberische Wertung bei der Ermessensausübung in der Anwendung anderer Übermittlungsvorschriften zwingend Berücksichtigung finden, denn die Gefährdung der nach § 43 Abs. 1 GwG meldenden Einzelpersonen knüpft an deren Aufgabe an und nicht an die Behörde, die ihre Daten Dritten gegenüber offenbart. Dieser Aspekt blieb bei der Entscheidung der Polizei zur Offenlegung der Kontaktdaten der Bankmitarbeiterin offenbar völlig unberücksichtigt. Des Weiteren wäre zu beachten gewesen, dass der Bankkundin ohne Weiteres die aus der Website der Bank ersichtlichen Kontaktmöglichkeiten hätten mitgeteilt werden können; im Kontakt für Privatkunden sind eine E-Mail-Adresse, eine Telefonnummer und eine Faxnummer angegeben, auch die Postanschrift ist aus der Website ersichtlich. Im Ergebnis hätten eine ordnungsgemäße polizeiliche Ermessensausübung und

Interessenabwägung zu keinem anderen Ergebnis führen können als zum Unterbleiben der Übermittlung des Namens und der Durchwahl der Bankmitarbeiterin an die Bankkundin.
Die Übermittlung konnte auch nicht auf § 84 Abs. 3 Nr. 1 SächsPVDG gestützt und mit der Verhütung weiterer Straftaten begründet werden. Zum einen ist die Vorschrift eine „Kann"-Bestimmung und erfordert die Ausübung pflichtgemäßen Ermessens, wobei auch hier die oben dargelegten Aspekte hätten berücksichtigt werden müssen. Zum anderen war auch nicht erkennbar, inwiefern die Offenlegung der individuellen Kontaktdaten der Bankmitarbeiterin zur Verhinderung von Straftaten im Zusammenhang mit dem betreffenden Konto hätte erforderlich sein können. Alle Beteiligten waren über die Vorgänge informiert; es war schlicht ausgeschlossen, dass das Konto gegen den Willen der Kontoinhaberin und der kontoführenden Bank für Straftaten hätte genutzt werden können.
Die Polizei nahm den Vorgang zum Anlass, die Bediensteten datenschutzrechtlich zu sensibilisieren. Ich habe angesichts des festgestellten Verstoßes gegen den Datenschutz die Polizei gebeten, das Vorliegen der gesetzlichen Voraussetzungen für die Übermittlung polizeilicher Daten an Privatpersonen besonders sorgfältig zu prüfen.

Was ist zu beachten?
Die Übermittlung personenbezogener Daten an nichtöffentliche Stellen sollte immer eine Ausnahme darstellen, die gesetzlichen Bestimmungen sind eng auszulegen. Polizeiliche personenbezogene Datensammlungen dienen der Erfüllung der Aufgaben auf dem Gebiet der Gefahrenabwehr und der Strafverfolgung, mithin der Wahrnehmung staatlicher, hoheitlicher Aufgaben; sie sind kein Informationspool für Private.

8.8 Übermittlung eines Strafbefehls trotz Tilgung des Eintrags im Bundeszentralregister

↗ § 51 BZRG, § 479 StPO

Ein Petent wandte sich an mich, nachdem er als Beteiligter in einem aktuellen familiengerichtlichen Verfahren feststellen musste, dass ein ihn betreffender und über zehn Jahre alter Strafbefehl thematisiert wurde.
Auf Hinweis des Petenten wandte ich mich an die Staatsanwaltschaft, die das seinerzeitige Verfahren wegen des Verdachts einer Straftat aus dem Dreizehnten Abschnitt des Besonderen Teils des Strafgesetzbuches gegen ihn geführt

hatte. Diese teilte mit, dass der Strafbefehl vom Juli 2011, der im August 2011 rechtskräftig geworden und in dem eine Geldstrafe von 90 Tagessätzen verhängt worden war, auf Ersuchen des Familiengerichts im Juni 2022 dorthin übersandt worden sei. Bis auf den Strafbefehl sei die Akte bereits vernichtet worden.

Daraufhin bat ich um Auskunft zur Rechtsgrundlage, auf der die Staatsanwaltschaft den Strafbefehl an das Amtsgericht, Familiengericht, übersandt hatte, und wies zur Begründung meiner Frage auf den Zeitablauf nach Rechtskraft des Strafbefehls und das gesetzliche Verwertungsverbot nach § 51 Bundeszentralregistergesetz (BZRG) hin.

Nach dieser Vorschrift dürfen die Tat und die Verurteilung der betroffenen Person im Rechtsverkehr nicht mehr vorgehalten und nicht zu ihrem Nachteil verwertet werden, wenn die Eintragung über eine Verurteilung im Bundeszentralregister getilgt worden ist oder sie zu tilgen ist. Strafbefehle, in denen eine Geldstrafe in Höhe von 90 Tagessätzen verhängt wird, gelten als Verurteilungen im Sinne des Bundeszentralregistergesetzes. Damit kamen auch die weiteren Vorschriften des BZRG zur Anwendung, insbesondere die Bestimmungen über die Tilgungsfrist (§§ 45, 46 BZRG) und das Verwertungsverbot nach Fristablauf gemäß § 51 Abs. 1 BZRG. Mit Blick auf den Tatvorwurf und die Höhe der Geldstrafe war die Eintragung nach zehn Jahren, das heißt im Juli 2021 zu tilgen (§§ 5, 36, 46 Abs. 1 Nr. 1a Buchst. a BZRG). Damit unterlagen die Tat und die Verurteilung spätestens seit August 2021 dem gesetzlichen Verwertungsverbot nach § 51 Abs. 1 BZRG.

Die Staatsanwaltschaft teilte mit, dass die Übersendung an das Familiengericht am Amtsgericht auf Grundlage von § 474 Abs. 1 Strafprozessordnung (StPO) zur Ausübung der Rechtspflege erfolgt sei. Inwieweit ein Übermittlungsverbot nach den §§ 479 StPO in Verbindung mit § 51 Abs. 1 BZRG bestand, sei nur summarisch geprüft worden, weil nach § 479 Abs. 4 Satz 2 StPO grundsätzlich das anfordernde Familiengericht die Verantwortung für die Zulässigkeit der Anforderung trage und besondere Übersendungsverbote

nicht offensichtlich gewesen seien. Dass § 51 Abs. 1 BZRG (stets) eine gesetzliche Verwendungsbeschränkung im Sinne des § 479 Abs. 1 StPO bilde, sei keineswegs zwingend, sondern im Einzelfall zu prüfen. Nachdem eine Ausnahme vom Übersendungsverbot aufgrund eines familiären Bezugs nach § 51 Abs. 2 BZRG habe nicht gänzlich ausgeschlossen werden können, sei der Strafbefehl zu übersenden gewesen.

Die Argumentation der Staatsanwaltschaft hielt einer datenschutzrechtlichen Prüfung nicht stand.

Der Begriff des Rechtsverkehrs im Sinne von § 51 Abs. 1 BZRG erfasst sämtliche Rechtsverhältnisse und Rechtsbeziehungen im privaten und öffentlichen Rechtsleben und lässt keinen Bereich des Rechts aus, unabhängig davon, ob es sich um materiell- oder verfahrensrechtliche Vorschriften oder um Bundes- oder Landesrecht handelt. Auch Übermittlungen auf Ersuchen von Familiengerichten zählen hierunter. Mit der Vorschrift bezweckte der Gesetzgeber, verurteilte Personen nach einer gewissen Zeit ohne erneute Straffälligkeit vollständig vom Strafmakel zu befreien und als nicht vorbestraft am gesellschaftlichen Leben teilnehmen zu lassen.

§ 479 Abs. 1 Alt. 2 StPO ist eine gesetzliche, Übermittlungen aus Strafverfahren regelnde Vorschrift, die keinen Ermessensspielraum lässt. Auskünfte aus Akten und Akteneinsicht sowie Datenübermittlungen sind danach zwingend zu versagen, wenn der Übermittlung besondere bundesgesetzliche oder entsprechende landesgesetzliche Verwendungsregelungen entgegenstehen. Die Vorschrift des § 51 Abs. 1 BZRG als eine solche besondere bundesgesetzliche Verwendungsregelung (Verwertungsverbot) lässt ebenso wenig Raum für Abwägungen oder eine Ermessensausübung der datenführenden Stelle.

Eine Übersendung des Strafbefehls wäre allenfalls in Betracht gekommen, wenn einer der abschließend in § 51 Abs. 2 BZRG und § 52 BZRG geregelten Ausnahmetatbestände vorgelegen hätte, der eine Übermittlung trotz des grundsätzlich bestehenden Verwertungsverbots nach § 51 Abs. 1 BZRG legitimiert hätte. Die Annahme, dass eine Ausnahme vom Übersendungsverbot aufgrund familiären Bezugs nach § 51

Abs. 2 BZRG habe „nicht gänzlich ausgeschlossen werden" können, wird von § 51 Abs. 2 BZRG nicht erfasst. Das Auskunftsersuchen eines (Familien-)Gerichts steht in keinem Zusammenhang mit den in § 51 Abs. 2 BZRG erwähnten Konstellationen. Weder waren „aus der Tat oder der Verurteilung entstandene Rechte Dritter" (wie etwa zivilrechtliche Ersatzansprüche aus der Tat) streitig, noch ergaben sich aus der Verurteilung im Jahr 2011 unmittelbar gesetzliche Rechtsfolgen, ebenso wenig stand die Gültigkeit gerichtlicher oder behördlicher Entscheidungen, die im Zusammenhang mit der Tat oder der Verurteilung ergangen sind, infrage. Ein möglicher familiärer Bezug einer strafprozessualen Information begründet ebenso wenig wie ein familiengerichtliches Übermittlungsersuchen eine Ausnahme nach § 51 Abs. 2 BZRG, die im Übrigen von der übermittelnden Stelle – hier der Staatsanwaltschaft – festzustellen wäre und nicht nur angenommen oder vermutet werden darf. Kann das Vorliegen der Voraussetzungen einer Ausnahme nach § 51 Abs. 2 BZRG nicht klar bejaht werden, bleibt es beim zwingenden Verwertungsverbot nach § 479 Abs. 1 Alt. 2 StPO in Verbindung mit § 51 Abs. 1 BZRG, und die Verwendung, hier: die Übermittlung, muss unterbleiben. Eine Ausnahme vom Verwertungsverbot nach § 52 BZRG kam im vorliegenden Fall von vornherein nicht in Betracht.

Die Prüfung besonderer Verwendungs- bzw. Übermittlungsverbote obliegt der übermittelnden Stelle, auch wenn die Übermittlung auf Ersuchen einer öffentlichen Stelle erfolgt. Insoweit wird gemäß § 479 Abs. 4 Satz 3 2. Halbsatz StPO die Verantwortungszuschreibung des § 479 Abs. 4 Satz 2 StPO aufgehoben. Das ist insofern zwingend und sachgerecht, als die ersuchende Stelle regelmäßig gar keine Kenntnis der tatsächlichen Umstände hat, die für ein Übermittlungsverbot ursächlich sein können (etwa eine Datenerhebung mittels besonders eingriffsintensiver Erhebungsmethoden, weitere, jüngere Eintragungen im Bundeszentralregister oder Ähnliches).

Vorliegend war ein besonderer Anlass zu einer weitergehenden Prüfung der Zulässigkeit der Übermittlung auch offensichtlich. Wenn eine Verurteilung elf Jahre zurückliegt und

Was ist zu tun?

Bei der beabsichtigten Übermittlung von Informationen über strafrechtliche Verurteilungen ist insbesondere bei länger zurückliegenden Entscheidungen stets zu prüfen, ob das Verwertungsverbot nach § 51 Abs. 1 BZRG einer Verwendung entgegensteht. Die Prüfung besonderer Verwendungs- und Übermittlungsverbote obliegt der übermittelnden Stelle. Das Verwertungsverbot gilt auch hinsichtlich solcher Aktenbestandteile, die nach Tilgung der Eintragung im Bundeszentralregister noch nicht vernichtet sind.

das Schriftgut zum Vorgang bereits vernichtet ist, ist kaum etwas näherliegend als die Notwendigkeit der Prüfung, ob das Verwertungsverbot nach § 51 Abs. 1 BZRG einschlägig ist und nach § 479 Abs. 1 StPO einer Übermittlung entgegensteht.

Angesichts der klaren Umstände hätte auch eine nur summarische Prüfung der Voraussetzungen von § 51 Abs. 1 BZRG zu dem Ergebnis führen müssen, dass eine Übermittlung unzulässig war.

Dem Petenten und der Staatsanwaltschaft habe ich das Ergebnis meiner Prüfung mitgeteilt.

Die Behandlung des alten Strafbefehls durch das Familiengericht konnte ich mangels Zuständigkeit nicht prüfen. Gerichte unterliegen der im Rahmen ihrer justiziellen Tätigkeit vorgenommenen Verarbeitungen personenbezogener Daten nicht der Kontrolle der Datenschutzaufsichtsbehörden, Art. 55 Abs. 3 DSGVO.

9 Rechtsprechung zum Datenschutz

9.1 Auslegung von Art. 9 Abs. 1 DSGVO

↗ Art. 5 Abs. 1 Buchst. c DSGVO, Art. 9 Abs. 1 DSGVO

Mit Urteil vom 1. August 2022 in der Rechtssache C-184/20 widmete sich der Europäische Gerichtshof der Auslegung des Anwendungsbereichs des Art. 9 Abs. 1 Datenschutz-Grundverordnung (DSGVO).

Ausgangspunkt des Verfahrens war der Vorlagebeschluss eines nationalen Gerichts im Hinblick auf eine nationale Antikorruptionsvorschrift, die regelte, dass die vollständigen Namen der oder des Ehegatten, der Partnerin bzw. des Partners oder der oder des Lebensgefährten erklärungspflichtiger Personen zu veröffentlichen sind. Gegenstand der rechtlichen Überlegungen war nun unter anderem, ob anhand der großen Namensinformationen Rückschlüsse in Bezug auf die sexuelle Orientierung der erklärungspflichtigen Personen getroffen werden konnten und es sich daher bei diesen Informationen schon um schützenswerte Daten im Sinne von Art. 9 Abs. 1 DSGVO handeln würde.

In seiner Entscheidung tendiert der Europäische Gerichtshof auch unter Rückgriff auf Überlegungen zur Wirksamkeit eines Schutzes zu einer weiten Auslegung des Wortlautes von Art. 9 Abs. 1. So seien die Namensangaben „zwar ihrer Natur nach keine sensiblen Daten im Sinne der Richtlinie 95/46 und der DS GVO", jedoch hielt es das Gericht für möglich, aus den namensbezogenen Daten bestimmte Informationen „über das Sexualleben oder die sexuelle Orientierung dieser Person, ihres Ehegatten, Lebensgefährten oder Partners abzuleiten"

und eine nicht nur am Wortlaut, sondern auch am Kontext und den Zielen zu berücksichtigende Auslegung vorzunehmen sei, vgl. Rdnr. 119 und 121 (zitiert nach curia.europa.eu).
In seinen Schlussfolgerungen kommt das Gericht zu der Überlegung, dass auch die Verarbeitung personenbezogener Daten, die „indirekt sensible Informationen über eine natürliche Person offenbaren können", eine Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne der Bestimmung des Art. 9 Abs. 1 DSGVO darstelle, vgl. Rdnr. 127.
Die Entscheidung wird in der Rechtsetzung, aber auch in der Datenverarbeitungs- und Verwaltungspraxis zu berücksichtigen sein, insbesondere auch im Hinblick auf die Angemessenheit und Notwendigkeit der Datenverarbeitung bzw. auf Datenminimierung, vgl. auch Art. 5 Abs. 1 Buchst. c DSGVO.

Was ist zu tun?
Die Anwendbarkeit von Art. 9 Abs. 1 DSGVO ist weit und kontextbezogen auszulegen. Auch bei mittelbaren Bezügen ist zu prüfen, ob besondere Kategorien personenbezogener Daten zu schützen sind.

9.2 Kündigungsschutz bei Datenschutzbeauftragten

Mit Urteil vom 22. Juni 2022 in der Rechtssache C-534/20 entschied der Europäische Gerichtshof (EuGH), dass Art. 38 Abs. 3 Satz 2 Datenschutz-Grundverordnung (DSGVO) einer nationalen Regelung, nach der einem Datenschutzbeauftragten aus wichtigem Grund gekündigt werden kann, nicht entgegensteht.
Im Ausgangsfall wandte sich eine Beschäftigte gegen ihre Kündigung. Der Rechtsstreit war zunächst beim zuständigen Arbeitsgericht und dem Landesarbeitsgericht Nürnberg anhängig, bei dem die Klägerin zunächst Erfolg hatte. Das Bundesarbeitsgericht legte den Fall – wegen Zweifeln – dem Europäischen Gerichtshof zur Klärung der Europarechtskonformität vor.
Die Entscheidung bezog sich sowohl auf § 38 Bundesdatenschutzgesetz (BDSG) und eine alte Fassung von § 6 Abs. 4 BDSG als auch auf die damit verbundene Vorschrift des § 626 Bürgerliches Gesetzbuch (BGB), vgl. Rdnr. 7 und 10 der Entscheidung (zitiert nach curia.europa.eu). § 6 Abs. 4 BDSG legt auch in der aktuellen Fassung fest, dass eine Abberufung des Datenschutzbeauftragten nur in entsprechender

Anwendung von § 626 BGB zulässig ist. Die Vorschrift bezieht sich zunächst auf öffentliche Stellen des Bundes, findet aber gemäß § 38 Abs. 2 BDSG bei der verpflichtenden Benennung eines Datenschutzbeauftragten auch bei nichtöffentlichen Stellen Anwendung. § 626 BGB ist bei beschäftigten Datenschutzbeauftragten unmittelbar – nicht nur entsprechend – anwendbar, vgl. den Wortlaut von § 6 Abs. 4 Satz 1 BDSG. Insofern ist die Entscheidung für in Deutschland ansässige Verantwortliche von allgemeinem Interesse gewesen. Hervorgehoben wird seitens des Europäischen Gerichtshofs die unabhängige Stellung des Datenschutzbeauftragten und dass Art. 38 Abs. 3 Satz 2 DSGVO diesen vor Entscheidungen im Zusammenhang mit der Erfüllung seiner Aufgaben schützen soll, vgl. Rdnr. 27f. der Entscheidung. Insbesondere soll der Datenschutzbeauftragte „keine Anweisungen bezüglich der Ausübung seiner Aufgaben" erhalten. Damit werde allerdings nicht bezweckt, das Arbeitsverhältnis zwischen dem Verantwortlichen und dessen Beschäftigten zu regeln, vgl. Rdnr. 27 der Entscheidung. Das Gericht erkannte in der nationalen Festlegung der Vorschrift zum Kündigungsschutz von beschäftigten Datenschutzbeauftragten nicht eine datenschutzrechtliche, sondern eine Regelung der Sozialpolitik. Damit bleiben Motive für Kündigungen zulässig, wenn sie nicht die Weisungsfreiheit und die Ausübung der Beauftragtenfunktion betreffen, so etwa wegen des allgemeinen Grundes der Zerrüttung des Beschäftigungsverhältnisses.

Was ist zu beachten?
Die Vorschriften des Bundesdatenschutzgesetzes zur Abberufung von Datenschutzbeauftragten, § 6 Abs. 4 Satz 1, § 38 Abs. 2 BDSG, sind europarechtskonform.

9.3 Verbandsklagerecht bei Verstößen gegen die Datenschutz-Grundverordnung

↗ Art. 80 Abs. 1, Abs. 2 DSGVO, UklaG, UWG

Mit Entscheidung vom 28. April 2022, C-319/20, entschied der Europäische Gerichtshof, dass ein Verbraucherschutzverband ohne Auftrag und unabhängig von der Verletzung konkreter Rechte betroffener Personen Klage erheben darf, soweit durch eine vermeintliche Datenschutzverletzung (auch) gegen

das Verbot gegen den unlauteren Wettbewerb, Verbraucherschutzgesetze oder das Verbot von allgemeinen Geschäftsbedingungen verstoßen wird.

Voraussetzung einer Klagebefugnis für den Verband sei, dass die jeweilige Datenverarbeitung die Rechte einzelner natürlicher Personen beeinträchtigen könne. Das Urteil kam aufgrund der Vorlage des Bundesgerichtshofs beim Europäischen Gerichtshof zur Vorabentscheidung zustande. Der in der Bundesrepublik angesiedelte Bundesverband der Verbraucherzentralen erhob eine Unterlassungsklage gegen das Unternehmen Meta Platforms Ireland Ltd. (umbenannt, früher Facebook Ireland Ltd.) wegen einer von diesem unterhaltenen Softwareplattform, die zunächst beim Landgericht und dann beim Kammergericht Berlin erfolgreich war. In dem Revisionsverfahren legte der Bundesgerichtshof, der in Bezug auf die Konformität mit Art. 80 Abs. 2 Datenschutz-Grundverordnung (DSGVO) Klärungsbedarf erkannte, den Rechtsstreit zur Vorabentscheidung vor. Der Verband berief sich auf Vorschriften des Gesetzes gegen den unlauteren Wettbewerb (UWG) sowie des Gesetzes über Unterlassungsklagen bei Verbraucherrechts- und anderen Verstößen (UklaG).

Der Europäische Gerichtshof ordnete den Verbraucherschutzverband als Organisation ein, die unter den Begriff des Art. 80 Abs. 2 DSGVO fallen könne, da ein „Verstoß gegen die Vorschriften zum Schutz der Verbraucher oder zur Bekämpfung unlauterer Geschäftspraktiken – den ein Verband zur Wahrung von Verbraucherinteressen wie der Bundesverband insbesondere durch die in der anwendbaren nationalen Regelung vorgesehene Unterlassungsklage verhindern und ahnden möchte – … nämlich, wie im vorliegenden Fall, mit einem Verstoß gegen die Vorschriften zum Schutz der personenbezogenen Daten dieser Verbraucher einhergehen" könne, vgl. Rdnr. 65f. der Entscheidung (zitiert nach curia.europa.eu). Allerdings könne eine Verbandsklage unter den Voraussetzungen der Datenschutz-Grundverordnung nur erhoben werden, wenn der Verbraucherverband die Rechte betroffener Personen gemäß der Verordnung infolge einer Verarbeitung als verletzt ansieht. Eine Person, „die von einer

Verarbeitung von Daten, die mutmaßlich gegen die Bestimmungen der DSGVO verstößt, konkret betroffen ist", muss hingegen im Voraus nicht ermittelt werden, vgl. Rdnr. 67f.
Der Entscheidung dürfte große praktische Bedeutung in der datenschutzrechtlichen Rechtsdurchsetzung zukommen. Insbesondere bei globalen, den Markt (mit)beherrschenden IT-Unternehmen stehen mit Informationsvorsprüngen und starken personellen und sachlichen Ressourcen ausgestattete Firmen den Verbraucherschutzvereinigungen gegenüber. Die deutschen Datenschutzaufsichtsbehörden wiederum sind zuständigkeitsbedingt nicht selten nur über die in anderen EU-Staaten verorteten und für ausländische Verantwortliche primär zuständigen Datenschutzaufsichtsbehörden auf den Verantwortlichen einzuwirken in der Lage. Softwarehersteller wiederum können von den Datenschutzaufsichtsbehörden nur dann pflichtig gemacht werden, soweit diese als Verantwortlicher oder Auftragsverarbeiter handeln.

Was ist zu beachten?
Auch Verbraucherschutzverbände sind bei datenschutzrechtlichem Bezug gemäß Art. 80 Abs. 2 DSGVO einzuordnende Vereinigungen.

9.4 Unionsrechtswidrigkeit der anlasslosen Vorratsdatenspeicherung von Verkehrs- und Standortdaten in der Telekommunikation

↗ § 113 a ff. TKG, Richtlinie 2002/58/EG

In seinem Urteil vom 20. September 2022, C-793/19 und C-794/19 entschied der Europäische Gerichtshof (EuGH), dass nationale Rechtsvorschriften, die präventiv zur Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit eine allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten im Telekommunikationsbereich vorsehen, mit der „Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation" (Datenschutzrichtlinie für elektronische Kommunikation) nicht im Einklang stehen, vgl.

den Wortlaut von Art. 15 Abs. 1 der genannten Richtlinie, die gewisse Beschränkungen der Kommunikation durch nationale Gesetzgebung erlaubt. Die Entscheidung bezieht sich auf bisherige telekommunikationsgesetzliche Vorschriften der Bundesrepublik Deutschland.

Das Urteil steht im Einklang mit der bisherigen Spruchpraxis des Europäischen Gerichtshofs. Die Regelungen der §§ 113 a ff. Telekommunikationsgesetz (TKG) wurden zuvor schon nicht weiter angewandt. Die Entscheidung ist dennoch für eine neue Rechtsetzung von Bedeutung, soweit der Gerichtshof unzulässige Datenverarbeitungen definiert und Ausnahmemöglichkeiten beschreibt. Insofern war das Urteil auch wegen der Breitenwirkung der gemeinhin als „Vorratsdatenspeicherung" bezeichneten Datenverarbeitungsbefugnisse von allgemeinem gesellschaftspolitischem Interesse. Durch die entsprechenden telekommunikationsgesetzlichen Festlegungen waren quasi alle betroffen. Nach der Entscheidung sind Rechtsvorschriften zur Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit zulässig, soweit sie „auf der Grundlage objektiver und nicht diskriminierender Kriterien anhand von Kategorien betroffener Personen oder mittels eines geografischen Kriteriums für einen auf das absolut Notwendige begrenzten, aber verlängerbaren Zeitraum eine gezielte Vorratsspeicherung von Verkehrs- und Standortdaten vorsehen; für einen auf das absolut Notwendige begrenzten Zeitraum eine allgemeine und unterschiedslose Vorratsspeicherung der IP-Adressen, die der Quelle einer Verbindung zugewiesen sind, vorsehen; eine allgemeine und unterschiedslose Vorratsspeicherung der die Identität der Nutzer elektronischer Kommunikationsmittel betreffenden Daten vorsehen; vorsehen, dass den Betreibern elektronischer Kommunikationsdienste mittels einer Entscheidung der zuständigen Behörde, die einer wirksamen gerichtlichen Kontrolle unterliegt, aufgegeben werden kann, während eines festgelegten Zeitraums die ihnen zur Verfügung stehenden Verkehrs- und Standortdaten umgehend zu sichern (quick freeze)", vgl. Rdnr. 75 der Entscheidung. Nunmehr ist ein erneutes Tätigwerden des Bundesgesetzgebers zu erwarten.

Was ist zu tun?
Die Zulässigkeit der Speicherung von Verkehrs- und Standortdaten durch Telekommunikationsdienstleister wird gemäß den Festlegungen des EuGH anzupassen sein.

Herausgeberin
Sächsische Datenschutz- und Transparenzbeauftragte
Dr. Juliane Hundert
Devrientstraße 5, 01067 Dresden

Kontakt
Postanschrift: Postfach 11 01 32, 01330 Dresden
Telefon 0351 85471-100
Telefax 0351 85471-109
post@sdtb.sachsen.de
www.datenschutz.sachsen.de

Fotos
Titel: © loveguli/istockphoto.com
Weitere Fotos: ronaldbonss.com (Seite 4), BfDI (Seite 193, 194)

Druck
siblog – Gesellschaft für Dialogmarketing, Fulfillment & Lettershop mbH

Auflage
1.500 Exemplare

Veröffentlichung
Mai 2023

Bezug
kostenlos
Zentraler Broschürenversand der Sächsischen Staatsregierung
Hammerweg 30, 01127 Dresden
Telefon: 0351 210-3671 / -3672
publikationen@sachsen.de
www.publikationen.sachsen.de

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