Tätigkeitsbericht der Sächsischen Datenschutzbeauftragten

Berichtszeitraum:
1. Januar bis 31. Dezember 2021

Freistaat
SACHSEN

Tätigkeitsbericht der Sächsischen Datenschutzbeauftragten 2021

Berichtszeitraum:
1. Januar bis 31. Dezember 2021

Rechtsstand: 31. Dezember 2021

Datenschutz ist Freiheitsschutz

Andreas Schurig, bis Ende 2021 Sachsens oberster Datenschützer, und Dr. Juliane Hundert, nun Sächsische Datenschutzbeauftragte, sprechen im Interview über die Aufgaben und Herausforderungen, die Macht der Tech-Konzerne und die Freude auf ein gutes Buch.

Herr Schurig, Sie sind nun als Sächsischer Datenschutzbeauftragter ausgeschieden. Gibt es einen Rat, den Sie Ihrer Nachfolgerin mitgeben wollen?

Schurig: Nein, denn jede Generation steht vor ihren eigenen Aufgaben und Herausforderungen, und ich bin überzeugt, dass Frau Dr. Hundert die ihrigen gut meistern wird. Schon vor meiner ersten Amtszeit als Sächsischer Datenschutzbeauftragter habe ich in der Behörde gearbeitet. Ich erinnere mich noch an meine Anfangszeit 1993. Damals gab es noch keinen Internetanschluss. Verglichen mit heute stand die elektronische Datenverarbeitung ganz am Anfang.

Frau Dr. Hundert, mit welchen Gefühlen haben Sie Ihr neues Amt angetreten?

Dr. Hundert: Mit einem guten! Ich kenne Herrn Schurig und einen Großteil der Mitarbeiterinnen und Mitarbeiter schon lange. Er hat den Datenschutz in Sachsen maßgeblich geprägt. Ich habe großen Respekt und Anerkennung für seine Leistung; nicht nur als neue Behördenleiterin, sondern zuallererst als Bürgerin. Gemeinsam mit meinen Mitarbeiterinnen und Mitarbeitern in der Behörde möchte ich diese Arbeit nun fortsetzen. Und ich freue mich auf neue Herausforderungen.

Was ist Datenschutz denn für Sie persönlich?

Dr. Hundert: Ich bin ein Kind der DDR. Ich habe von ihr noch so viel mitbekommen, dass ich weiß, wie es ist, wenn der Staat tief ins Private vordringt und systematisch die Bevölkerung ausspäht. Für mich ist Datenschutz deshalb in erster Linie ein Abwehrrecht gegen den Staat. Gleichwohl leben wir

heute in einer Zeit, in der die Bedrohung unserer Freiheit auch aus einer anderen Richtung kommt. Ich meine damit die Tech-Konzerne, die das Ausspähen ihrer Kunden zum Geschäftsmodell gemacht haben. Mein Händler um die Ecke wäre die längste Zeit mein Geschäftspartner gewesen, wenn er mich nach einem Besuch in seinem Geschäft auf meinem folgenden Weg in andere Geschäfte begleiten würde, damit er mir beim nächsten Mal Produkte anbieten kann, die besser zu meinen Bedürfnissen passen. Genau das jedoch lassen wir im Internet zu – und viele Menschen wissen nicht, dass es so ist. Es geht beim Datenschutz also auch um klare Regeln unter Privaten. Die EU und die Bundesrepublik haben mit der Datenschutz-Grundverordnung und dem nationalen Recht Regelungen geschaffen, die es uns ermöglichen sollen, unsere Freiheit und Privatsphäre auch gegenüber Unternehmen zu schützen. Die Bürgerinnen und Bürger dürfen dabei mit meiner Unterstützung rechnen.

Schurig: Das ist ein Aspekt, den ich nur unterstreichen kann. Es gibt eine überschaubare Zahl an Tech-Konzernen, die unglaublich mächtig geworden sind. Sie lassen sich kaum regulieren. Natürlich müssen wir trotzdem versuchen, diese Konzerne in die Schranken zu weisen. Auch sie müssen sich an die Spielregeln halten, die im Wesentlichen in der Datenschutz-Grundverordnung festgeschrieben sind. Jedoch ist viel wichtiger, dass wir – Verantwortliche und Nutzer – sorgfältig mit unseren bzw. den anvertrauten Daten umgehen. Wir müssen uns immer wieder bewusst machen: Datenschutz ist Freiheitsschutz!

Frau Dr. Hundert, seit dem 1. Januar 2022 sind Sie die Sächsische Datenschutzbeauftragte und legen nun gemäß der Datenschutz-Grundverordnung Ihren ersten Jahresbericht vor. Er dokumentiert jedoch die Arbeit Ihres Amtsvorgängers. Das war sicherlich keine ganz einfache Aufgabe, oder?

Dr. Hundert: Zuallererst bedanke ich mich bei Herrn Schurig für die hervorragende Amtsübergabe. Dadurch konnte ich mich schnell einarbeiten. Einige Aufsichtsvorgänge, die in

diesem Tätigkeitsbericht nachzulesen sind, haben mich bereits während meiner Zeit als Parlamentarische Beraterin und Justiziarin bei der Fraktion Bündnis 90/Die Grünen im Sächsischen Landtag beschäftigt. Dazu gehören unter anderem Datenschutzfragen im Zusammenhang mit den Pandemiemaßnahmen. Die eigentliche Herausforderung war eher, die wichtigen Vorgänge zu identifizieren, von denen ich vorher noch keine Kenntnis hatte, die aber für Datenschützer und Öffentlichkeit ebenso interessant und hilfreich sind.

Herr Schurig, wie war es 2021 um den Datenschutz in Sachsen bestellt?

Schurig: Es war das zweite Pandemiejahr. Das hat Datenschützern überall viel abverlangt. Denn mitunter sind die datenschutzfreundlichen Lösungen mit einigem Aufwand verbunden. Ich denke da beispielsweise an den richtigen Umgang mit Gesundheitsdaten; also bei der Kontaktdatenerfassung oder der Impf-, Genesungs- und Test-Abfrage durch den Arbeitgeber. Hier hat der Datenschutz aber wieder einmal bewiesen, dass er der Eindämmung der Pandemie nicht im Wege steht, sondern für Transparenz und damit für eine breite Akzeptanz der Maßnahmen sorgt. Die Corona-Warn-App ist ein Paradebeispiel dafür. Natürlich musste der Datenschutz auch 2021 wieder herhalten, um von eigenem Versagen und fehlender Regulierung abzulenken, beispielsweise bei den Abrechnungsskandalen in Corona-Testzentren. Dass die Verantwortlichen die Schuld am liebsten bei den anderen suchen, kommt offenbar nie aus der Mode. Die Corona-Maßnahmen waren aber nur ein Themenbereich, mit dem ich mich im Berichtszeitraum befasst habe. Auch beim Registermodernisierungsgesetz habe ich mich eingebracht, ebenso beschäftigten uns die Umsetzung des Schrems-II-Urteils, Cookies und Tracking im Netz sowie vieles mehr.

Frau Dr. Hundert, an Themen mangelt es offenbar nicht, oder wie schätzen Sie das ein?

Dr. Hundert: (lacht) Nein, ganz bestimmt nicht. Neu hinzukommen wird bald das Transparenzgesetz, so es der Sächsi-

sche Landtag beschließt. Dafür wurden im Berichtszeitraum die Weichen gestellt. Dann verfügt Sachsen wie fast alle Bundesländer auch über ein Gesetz, das die Informationsfreiheit regelt. Der Entwurf sieht vor, dass meine Behörde mögliche Beschwerden zu prüfen hat. Wenn Bürgerinnen und Bürger also der Auffassung sind, dass ihnen der Staat Informationen vorenthält, die er nach dem Transparenzgesetz bereitstellen muss, können sich die Betroffenen in Zukunft hoffentlich an meine Behörde wenden.

Braucht es für die neuen Herausforderungen auch neue Strukturen?

Schurig: Ich meine, dass es eine Verstärkung braucht, insbesondere personeller Natur. Datenschutzprobleme haben mit der Digitalisierung zugenommen. Es stehen schon neue Aufgaben am Horizont wie zum Beispiel die Überprüfung von Systemen, bei denen „Künstliche Intelligenz" eingesetzt wird. Das muss sich auch in der behördlichen Ausstattung nieder-

schlagen. Mit mehr Personal könnte die Behörde auch die Einhaltung des Datenschutzes besser überprüfen, zum Beispiel mit unangekündigten Kontrollen. Das war 2021 nur in sehr eingeschränktem Maße möglich.

Dr. Hundert: Mit den acht neuen Stellen, die uns der Landtag im letzten Jahr zur Verfügung gestellt hat, machen wir allerdings einen großen Schritt nach vorn. Aber Sie haben recht: Der Zuwachs an Aufgaben, der mit der Einführung der Datenschutz-Grundverordnung auf die Aufsichtsbehörden zugekommen ist, ist schon enorm. Allein die Abstimmung mit den anderen Aufsichtsbehörden erfordert sehr viel mehr Zeit als früher. Und da ist es gut, dass Sie, Herr Schurig, sich auch um die Weiterentwicklung der Datenschutzkonferenz bemüht haben. Unter der Führung Sachsens hat der Arbeitskreis DSK 2.0 im vergangenen Jahr eine Reihe von wichtigen Festlegungen vorbereitet. Im Kern geht es dabei um die Harmonisierung der Datenschutzaufsicht in Deutschland. Zu den Neuerungen gehört beispielsweise eine wöchentliche Videokonferenz auf Leitungsebene, in der sich die DSK-Mitglieder zu aktuellen Themen abstimmen. Ich werde mich dafür einsetzen, dass wir die Zusammenarbeit innerhalb der Datenschutzkonferenz fortentwickeln.

Herr Schurig, wie werden Sie Ihre freie Zeit nun nutzen?

Schurig: Wie ich meine Zeit verbringen werde? Das unterliegt dem Datenschutz! (lacht) Mehr Zeit für die Familie und öfter mal ein gutes Buch – darauf freue ich mich sehr.

Dr. Hundert: Dabei wünsche ich Ihnen viel Freude und hoffe, dass Sie dem Datenschutz weiterhin verbunden bleiben – und ich Sie bei Fragen immer mal wieder anrufen darf (lacht). Alles Gute!

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
AufenthG	Aufenthaltsgesetz
BArchG	Bundesarchivgesetz
BDSG	Bundesdatenschutzgesetz
BGB	Bürgerliches Gesetzbuch
BMG	Bundesmeldegesetz
BZRG	Bundeszentralregistergesetz
CoronaSchutzV	Coronavirus-Schutzverordnung
DSGVO	Datenschutz-Grundverordnung
eKFV	Elektrokleinstfahrzeugeverordnung
GG	Grundgesetz für die Bundesrepublik Deutschland
GKDZ-StV	Staatsvertrag über die Errichtung eines Gemeinsamen Kompetenz- und Dienstleistungszentrums der Polizeien der Länder Berlin, Brandenburg, Sachsen, Sachsen-Anhalt und Thüringen auf dem Gebiet der polizeilichen Telekommunikationsüberwachung als rechtsfähige Anstalt öffentlichen Rechts
GVO	Gerichtsvollzieherordnung
GVGA	Geschäftsanweisung für Gerichtsvollzieher
IfSG	Infektionsschutzgesetz
IfSGZuVO	Infektionsschutzgesetz-Zuständigkeitsverordnung
JI-RL	Richtlinie (EU) 2016/680 (Justiz und Inneres)
KunstUrhG	Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie
OWiG	Gesetz über Ordnungswidrigkeiten
SächsArchivG	Archivgesetz für den Freistaat Sachsen

SächsBRKG	Sächsisches Gesetz über den Brandschutz, Rettungsdienst und Katastrophenschutz
SächsCoronaNotVO	Sächsische Corona-Notfall-Verordnung
SächsCoronaSchVO	Sächsische Corona-Schutz-Verordnung
SächsDSG	Sächsisches Datenschutzgesetz
SächsDSDG	Sächsisches Datenschutzdurchführungsgesetz
SächsGemO	Sächsische Gemeindeordnung
SächsJAG	Sächsisches Juristenausbildungsgesetz
SächsJAPO	Sächsische Juristenausbildungs- und -prüfungsordnung
SächsISichG	Sächsisches Informationssicherheitsgesetz
SächsPetAG	Sächsisches Petitionsausschussgesetz
SächsPVDG	Sächsisches Polizeivollzugsdienstgesetz
SächsStVollzG	Sächsisches Strafvollzugsgesetz
SächsVwKG	Sächsisches Verwaltungskostengesetz
SächsVwOrgG	Sächsisches Verwaltungsorganisationsgesetz
SächsVwVG	Verwaltungsvollstreckungsgesetz für den Freistaat Sachsen
SchulKitaCoVO	Schul- und Kita-Coronaverordnung
SGB	Sozialgesetzbuch
StPO	Strafprozessordnung
StVZO	Straßenverkehrs-Zulassungs-Ordnung
TestV	Coronavirus-Testverordnung
TTDSG	Telekommunikation-Telemedien-Datenschutz-Gesetz
UWG	Gesetz gegen den unlauteren Wettbewerb
WEG	Wohnungseigentumsgesetz
WEMoG	Wohnungseigentumsmodernisierungsgesetz
ZPO	Zivilprozessordnung

Sonstiges

Abs.	Absatz
Art.	Artikel
Az.	Aktenzeichen
BAG	Bundesarbeitsgericht
BASt	Bundesanstalt für Straßenwesen
BGH	Bundesgerichtshof
BR-Drs.	Bundesrats-Drucksache
BSI	Bundesamt für Sicherheit in der Informationstechnik
BT-Drs.	Bundestags-Drucksache

Buchst.	Buchstabe
BVerfG	Bundesverfassungsgericht
BVerwG	Bundesverwaltungsgericht
DSK	Konferenz der unabhängigen Datenschutzbeauftragten des Bundes und der Länder – Datenschutzkonferenz
EGMR	Europäischer Gerichtshof für Menschenrechte
eKF	Elektrokleinstfahrzeug
EU	Europäische Union
GKDZ	Gemeinsames Kompetenz- und Dienstleistungszentrum der Polizeien der Länder Berlin, Brandenburg, Sachsen, Sachsen-Anhalt und Thüringen auf dem Gebiet der polizeilichen Telekommunikationsüberwachung
K. d. ö. R.	Körperschaft des öffentlichen Rechts
LaSuB	Landesamt für Schule und Bildung
LDS	Landesdirektion Sachsen
LG	Landgericht
LJK	Landesjustizkasse
LJPA	Landesjustizprüfungsamt
MIDEM	Mercator Forum Migration und Demokratie
OLG	Oberlandesgericht
OVG	Oberverwaltungsgericht
Rdnr.	Randnummer
SMI	Sächsisches Staatsministerium des Innern
SMK	Sächsisches Staatsministerium für Kultus
SMS	Sächsisches Staatsministerium für Soziales und Gesellschaftlichen Zusammenhalt
StA	Staatsanwaltschaft
SVN	Sächsisches Verwaltungsnetz
TOA	Täter-Opfer-Ausgleich
VwV	Verwaltungsvorschrift

Sachgebietsregister

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

Handel, Dienstleistungen, Gewerbe, Industrie	
• Auskunfteien, Inkassodienstleister, Detekteien	
• Banken, Finanzwirtschaft	
• Handel, siehe auch Internet/E-Commerce	
• Handwerk, Gewerbe, Industrie	3.1.3
• Hotel und Gastronomie, Freizeit, Tourismus, Sport	2.3.2, 2.4.2
• Versicherungen; siehe ggf. Sozialwesen, Leistungsträger	9.3
• Werbung, Markt- und Meinungsforschung	
• Sonstiges, Allgemeines	3.2.2
Infrastruktureller Sektor	
• Energie-, Wasser- und Versorgungswirtschaft	
• Verkehrs- und Beförderungswesen	
• Wohnungswirtschaft, Immobilienverwaltung	2.2.7
• Rechenzentren	
• Sonstiges, Allgemeines	
Internet, Medien, Kommunikation	
• E-Mail, Telekommunikationsvorgänge, Post	vgl. 4.4.1
• E-Commerce	2.2.3
• Social Media, Telemedien	2.3.2, 4.1.1, vgl. 6.1.3,
• Sonstiges, Allgemeines	1.3, 4.1.5, 4.2.3, 7.7
Kammern, berufsständische Körperschaften d. ö. R.*	
Meldung von Datenschutzverletzungen, Artikel 33	4.4.1
Ordnungswidrigkeiten – Sächsische Datenschutzbeauf.	6.3.1, 6.4
Religionsgemeinschaften	
Sächsische Datenschutzbeauftragte	6

Videografie und Bildverarbeitung	
• Behördliche Überwachung/Verarbeitung*	
• Beschäftigte, vgl. ansonsten Beschäftigtendatenverarbeitung	
• Dashcam, Drohnen	6.4.2
• Handel, Gewerbe	
• Wohnbereiche	
• Sonstiges, Allgemeines	2.2.4, 2.2.5, 2.2.6, 2.4.2, 3.1.2
Wahlrecht*	vgl. 3.1.1
Zertifizierung, Akkreditierungen, Prüfsiegel	vgl. 6.2.8

Richtlinie (EU) 2016/680

Polizei*	vgl. 2.4.5 und 2.4.6, 6.4.1
Ordnungswidrigkeitenbehörden*	vgl. 2.1.1 und 6.1.3
Strafverfolgung*	vgl. 2.4.6, 8.1, 8.2
Straf- und Justizvollzug*	
Betrieblicher Datenschutzbeauftragter siehe Datenschutzbeauftragter	

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

Sächsischer Landtag als Parlament	
Verfassungsschutz	
Weitere datenverarbeitende Stellen	

Vorbemerkung zum Sprachgebrauch

In diesem Tätigkeitsbericht wird nachfolgend das generische Maskulinum verwendet, um den Lesefluss und das Verständnis zu erleichtern. Selbstverständlich sind jedoch alle Geschlechter gemeint. Aus Gründen der grammatikalischen Korrektheit und richtigen Anwendung des Partizips Präsens wird auf Ersatzformen wie Nutzende oder Anwendende verzichtet.

1 Datenschutz im Freistaat Sachsen

1.1 Verarbeitung von Gesundheitsdaten Beschäftigter in der Corona-Pandemie

↗ § 26 BDSG; Art. 7, 9 DSGVO; SächsCoronaSchVO

Im vergangenen Berichtszeitraum hatte sich meine Behörde in erheblichem Umfang mit den Pandemiebekämpfungsmaßnahmen und damit einhergehenden datenschutzrechtlichen Fragen auseinanderzusetzen, die auch den Beschäftigendatenschutz betrafen. Die vielfältigen Problemlagen werden nachstehend in einer Chronologie dargestellt.

Im Rahmen der Corona-Pandemie hat der Sächsische Verordnungsgeber Infektionsschutzmaßnahmen in der Sächsischen Corona-Schutz-Verordnung (SächsCoronaSchVO) geregelt, die auch Auswirkungen auf das Beschäftigungsverhältnis hatten und weiterhin haben. Diese Regelungen führten zu vielfältigen Fragestellungen im Bereich des Arbeitsrechts sowie des Datenschutzes und bewegten sich regelmäßig im Spannungsfeld zu einem wirksamen Infektionsschutz.

Auch auf Bundesebene hat der Gesetzgeber mit der mehrfachen Änderung des Infektionsschutzgesetzes versucht, die arbeits- und datenschutzrechtlichen Fragestellungen, welche sich aus den Maßnahmen zum Infektionsschutz ergeben haben, wie zum Beispiel das Fragerecht des Arbeitgebers zum Impfstatus der Beschäftigten, zu regeln.

Corona-Tests

Neu entwickelte Möglichkeiten zur Eindämmung der Corona-Pandemie, wie zum Beispiel Antigen-Selbsttests, haben es bereits zu Beginn des Jahres 2021 Arbeitgebern erlaubt, diese ihren Mitarbeitern anzubieten. Das zog eine Reihe von arbeits- und datenschutzrechtlichen Fragen nach sich.

Meine Behörde war daher bereits im Januar 2021 mit der Beratungsanfrage eines internationalen Unternehmens, welches auch Niederlassungen in Sachsen unterhält, zur datenschutzkonformen Umsetzung von Corona-Tests von Mitarbeitern einschließlich der damit verbundenen Datenverarbeitungen, insbesondere auch von Testergebnissen, konfrontiert. Da dieses Unternehmen weitere Niederlassungen in anderen Bundesländern unterhielt und somit die Zuständigkeit weiterer deutscher Aufsichtsbehörden gegeben war, wurde über den Arbeitskreis Beschäftigtendatenschutz eine Antwort der zuständigen Aufsichtsbehörden an das Unternehmen koordiniert.

Diese setzte nach meiner Auffassung erste Maßstäbe bezüglich der datenschutzrechtlichen Anforderungen an die Verarbeitung von Gesundheitsdaten von Beschäftigten im Rahmen der Corona-Pandemie, insbesondere auch in Bezug auf die Verarbeitung von Corona-Testergebnissen, der einschlägigen Rechtsgrundlage, auf die eine derartige Verarbeitung von Gesundheitsdaten überhaupt gestützt werden kann, sowie in Bezug auf technisch-organisatorische Maßnahmen, die vom Verantwortlichen umzusetzen sind.

Dem anfragenden Unternehmen wurde unter anderem mitgeteilt, dass die Verarbeitung personenbezogener Daten im Rahmen der Durchführung der Corona-Selbsttests nicht auf § 26 Abs. 3 Satz 1 Bundesdatenschutzgesetz (BDSG), Art. 9 Abs. 2 Buchst. b Datenschutz-Grundverordnung (DSGVO) gestützt werden könne. Nach diesen Vorschriften können Gesundheitsdaten von Beschäftigten verarbeitet werden, wenn die Verarbeitung für Zwecke des Beschäftigungsverhältnisses erfolgt, zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes erforderlich

ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt.

Zu welchen Zwecken dürfen die Test- und Gesundheitsdaten verarbeitet werden?

Es bestanden jedoch bereits erhebliche Zweifel, ob die im Zusammenhang mit dem Corona-Selbsttest auf eine Infektion mit dem Coronavirus SARS-CoV-2 erhobenen Gesundheitsdaten für Zwecke des Beschäftigungsverhältnisses oder aber zu dem Zweck Pandemiebekämpfung durch Verhinderung von Ansteckungen verarbeitet werden sollten. Auch unter dem Gesichtspunkt, dass eine Testung von Beschäftigten der Fürsorgepflicht von Arbeitgebern gegenüber ihren Beschäftigten und damit auch Zwecken des Beschäftigungsverhältnisses dienen könnte, dürfen Arbeitgeber Gesundheitsdaten eines Beschäftigten gemäß § 26 Abs. 3 BDSG nur dann verarbeiten, um ihre Fürsorgepflichten gegenüber dem von der Datenverarbeitung selbst betroffenen Beschäftigten zu erfüllen. Die Erfüllung rechtlicher Pflichten gegenüber Dritten berechtigt gerade nicht zu einer Verarbeitung des von der Verarbeitung seiner personenbezogenen Daten betroffenen Beschäftigten.

Fürsorgepflicht als Verarbeitungszweck?

Auch aus der allgemeinen arbeitsrechtlichen Fürsorgepflicht nach §§ 611 a, 242 Abs. 2 Bürgerliches Gesetzbuch (BGB) konnte keine Verpflichtung des Arbeitgebers abgeleitet werden, die Belegschaft auf Covid-19 testen zu lassen und somit die hierfür erforderlichen Beschäftigtendaten einschließlich Gesundheitsdaten zu verarbeiten. Gegen eine solche allgemeine Pflicht des Arbeitgebers sprach auch, dass der Gesetzgeber im Wege von besonderen Vorschriften eine Testpflicht für Beschäftigte nur in sehr wenigen Fällen anerkannt hatte. Selbst die Verordnung zum Anspruch auf Testung in Bezug auf einen direkten Erregernachweis des Coronavirus SARS-CoV-2 (Coronavirus-Testverordnung – TestV) vom 30. November 2020 regelte „lediglich" einen Anspruch be-

stimmter Personengruppen auf Testung unter den in § 2 bis § 4 der TestV genannten Voraussetzungen, nicht hingegen eine von der Inanspruchnahme dieses Rechts unabhängige Verpflichtung der entsprechenden Einrichtung, Tests durchzuführen. Im Januar 2021 existierten nur vereinzelt Rechtsvorschriften, die eine echte Pflicht zur Durchführung von Tests begründeten. Der Charakter als Spezialnormen dieser – sehr wenigen – gesetzlichen Regelungen, die eine Testpflicht vorsahen, würde unterlaufen, wenn aus der allgemeinen arbeitsrechtlichen Fürsorgepflicht des Arbeitgebers eine über die spezialgesetzlich normierten Beschäftigtengruppen hinausgehende Pflicht zur Durchführung von Tests von Beschäftigten abgeleitet werden würde.

Verantwortlichen wurde weiter mitgeteilt, dass eine solche Pflicht auch nicht aus § 3 Abs. 1 Arbeitsschutzgesetz abgeleitet werden könne. Aus den genannten allgemeinen Vorgaben des betrieblichen Gesundheitsschutzes lässt sich gerade keine konkrete rechtliche Pflicht ableiten. Vielmehr liefe die Annahme einer Rechtspflicht des Arbeitgebers der oben genannten gesetzgeberischen Entscheidung zuwider, gerade nur in den explizit geregelten Fällen eine Testpflicht vorzusehen. Es bestand damit keine entsprechende Pflicht des Unternehmens und auch kein Recht, von den Beschäftigten die Duldung solcher Tests zu fordern; dies wäre aber Voraussetzung für die Anwendung des Art. 9 Abs. 2 Buchst. b DSGVO, § 26 Abs. 3 Satz 1 BDSG.

Öffentliches Interesse im Bereich der öffentlichen Gesundheit als Zweck?

Ein Verantwortlicher führte als weiteren möglichen Rechtsgrund für die Verarbeitung der Gesundheitsdaten der Beschäftigten Art. 9 Abs. 2 Buchst. i DSGVO, § 22 Abs. 1 Nr. 1 Buchst. c, Abs. 2 BDSG (öffentliches Interesse im Bereich der öffentlichen Gesundheit) an. Allerdings begründet die Aufgabe der Gesundheitsvorsorge keine allgemeine Befugnis von Unternehmen zur Verarbeitung von Gesundheitsdaten. Die Vorschriften beziehen sich ihrem Wortlaut und ihrer Entstehungsgeschichte nach auf das öffentliche Gesundheits-

wesen und auf die Gesundheitsverwaltung, soweit sie durch öffentliche und nichtöffentliche Stellen wahrgenommen wird. Dies ergibt sich insbesondere auch aus dem Verweis auf die Einhaltung berufsrechtlicher und strafrechtlicher Vorgaben zur Wahrung des Berufsgeheimnisses. Zudem darf eine solche Verarbeitung von Gesundheitsdaten aus Gründen des öffentlichen Interesses nicht dazu führen, dass Dritte, unter anderem Arbeitgeber, solche personenbezogenen Daten zu anderen Zwecken verarbeiten; Erwägungsgrund 54 DSGVO.
Da das Unternehmen jedoch „nur" seine eigenen Beschäftigten sowie Beschäftigte Dritter, die dem Unternehmen zuarbeiten, testen wollte, wurden gerade nicht überwiegend öffentliche Interessen im Bereich der öffentlichen Gesundheit verfolgt, sondern es sollte die Produktivität der einzelnen Betriebsstätten durch Vermeidung größerer Infektionsgeschehen erhalten werden.

Einwilligung als Rechtsgrundlage der Verarbeitung

Dem Unternehmen wurde daher mitgeteilt, dass nach Ansicht der beteiligten Datenschutzaufsichtsbehörden allein Art. 9 Abs. 2 Buchst. a DSGVO, § 26 Abs. 2 in Verbindung mit Abs. 3 Satz 2 BDSG für die avisierte Datenverarbeitung in Betracht käme, das heißt, die Einwilligung der Beschäftigten. Datenverarbeitungen im Beschäftigtenverhältnis, die auf eine Einwilligung gestützt werden, sind aufgrund des bestehenden Abhängigkeitsverhältnisses stets äußerst kritisch zu hinterfragen. Vor allem das Kriterium der Freiwilligkeit der Einwilligung ist zumeist nicht erfüllt. Insbesondere Druck seitens des Arbeitgebers, der die freie Entscheidung des Beschäftigten beeinflussen könnte, Nachteile, direkter oder indirekter Art, die den Beschäftigten entstehen könnten, falls sie sich gegen die Durchführung der Tests entscheiden, führen zu Zweifeln an der Freiwilligkeit und letztlich zur Unwirksamkeit der Einwilligung.
Der Verantwortliche wurde weiter darauf hingewiesen, dass die Beschäftigten umfassend über alle wesentlichen Aspekte der Datenverarbeitung, wie zum Beispiel Speicherdauer, informiert werden müssen, um auf diese Weise die Infor-

miertheit der Einwilligung im Sinne von Art. 4 Nr. 11 DSGVO sicherzustellen.

Freiwilligkeit der Einwilligung

Das Unternehmen teilte mit, dass es plane, für dieses Projekt Selbsttests einzusetzen, die im Labor eines Tochterunternehmens ausgewertet werden sollten und dieses wiederum die Testergebnisse den jeweiligen Unternehmensniederlassungen mitteilen würde. Aus diesem Grund wurde das Unternehmen darauf hingewiesen, dass die Einwilligung auch die Übermittlung eines etwaigen positiven Testergebnisses an den Arbeitgeber umfasst und daher auch transparent darüber zu informieren sei, an welche Funktionsträger des Arbeitgebers diese Übermittlung erfolgen würde. Diesbezüglich wäre eine Freiwilligkeit der Einwilligung auch nur anzunehmen, wenn der Arbeitgeber keine Rückmeldung über die negativen Testergebnisse erhält und auch nicht, welcher Beschäftigte das Testangebot angenommen hat oder eben nicht. Denn ansonsten müssten Beschäftigte befürchten, dass ihnen für den Fall, dass sie das Testangebot nicht wahrnehmen, mittelbar eventuell doch irgendwelche Nachteile erwachsen könnten. Gerade solche Befürchtungen müssen aber vermieden werden, denn nur so kann angesichts des Ungleichgewichts zwischen Arbeitgeber und Beschäftigten der Zweifel an der Freiwilligkeit der Einwilligung ausgeräumt werden.

Der Verantwortliche wurde des Weiteren darauf hingewiesen, dass die Beschäftigten nach Art. 7 Abs. 3 Satz 1 DSGVO über die jederzeitige Widerrufbarkeit der Einwilligung zu informieren sind und dass im Falle eines Widerrufs die personenbezogenen Daten nicht weiterverarbeitet werden dürfen.

Technisch-organisatorische Maßnahmen, Einrichtung einer „Vertrauensstelle"

Aufgrund der im Beschäftigungsverhältnis bestehenden Abhängigkeiten und damit gegebenenfalls verbundener Auswirkungen (wie zum Beispiel einer Kündigung), die sich aus der Verarbeitung von Gesundheitsdaten ergeben können, sind

besondere Anforderungen an die datenschutzkonforme Datenverarbeitung zu stellen. Auch im Hinblick darauf, dass der Arbeitgeber bzw. die Personalverwaltung, abweichend von gesetzlichen Vorschriften und dem arbeitsrechtlich ausgeprägten Fragerecht, Kenntnisse über konkrete Gesundheitsverhältnisse von Beschäftigten erlangen, sind im Gegenzug technisch-organisatorische Maßnahmen zur Kompensation durchzuführen.

Dem verantwortlichen Unternehmen wurde daher mitgeteilt, dass es für die avisierte Datenverarbeitung innerhalb seiner Personalverwaltung eine informationell abgeschottete Vertrauensstelle zu bilden hat, bei der die Informationen zu Positivtestungen eingehen. Diese Organisationseinheit muss im Hinblick auf Datenverarbeitung und personelle Ausstattung transparent beschrieben sein und von dem gemäß Art. 37 DSGVO benannten Datenschutzbeauftragten überwacht werden.

Die Anzahl der Beschäftigten der Vertrauensstelle und deren Zugang zu den empfangenen Test-Gesundheitsinformationen müssen auf das erforderliche Maß minimiert werden. Die Verarbeitung der erhobenen Gesundheitsdaten müsse autonom von der Verarbeitung der weiteren Beschäftigtendaten erfolgen. Das bedeutet, dass diese Gesundheitsdaten nicht in der Personalakte oder anderweitig verarbeitet werden dürfen. Bei der Weitergabe an Funktionseinheiten zur Personaleinsatzplanung hat der Verantwortliche daher ein Verfahren zu entwickeln, bei dem die Identitäten positiv getesteter Beschäftigter gegenüber Schichtleitern, Vorgesetzten usw. nicht aufgedeckt werden können.

Testpflicht

Nachdem zu Beginn des Jahres nur in speziellen Einrichtungen, wie zum Beispiel Pflegeheimen, die Beschäftigten auf das Vorliegen einer Infektion mit SARS-CoV-2 getestet wurden, legte der sächsische Verordnungsgeber in der SächsCoronaSchVO vom 5. März 2021 fest, dass alle Beschäftigten und Selbstständigen mit direktem Kundenkontakt ab 15. März 2021 einmal wöchentlich einen Test auf das Coronavi-

rus SARS-CoV-2 vorzunehmen haben oder verpflichtet sind, diesen vornehmen zu lassen.

Ab dem 22. März 2021 bestand für Arbeitgeber die Verpflichtung, ihren Beschäftigten, die an ihrem Arbeitsplatz präsent sind, ein Angebot zur Durchführung eines kostenlosen Selbsttests mindestens einmal pro Woche zu unterbreiten.

Auch dazu erreichte meine Behörde eine Vielzahl von Anfragen, die zumeist die Frage beinhalteten, ob diese Regelung den Arbeitgeber berechtige, die Testergebnisse zu erfassen. Ich konnte den Betroffenen mitteilen, dass der Arbeitgeber nicht berechtigt ist, das positive oder negative Testergebnis zu verarbeiten. Vielmehr wird der Arbeitgeber durch diese Regelung lediglich verpflichtet, den Nachweis zu führen, dass er seinen Beschäftigten den Test angeboten habe.

Testpflicht für Urlaubsrückkehrer

Mit Wirkung zum 26. Juli 2021 führte der Sächsische Verordnungsgeber sodann eine Testpflicht für sogenannte „Urlaubsrückkehrer" ein. Danach hatten Beschäftigte, die mindestens fünf Werktage nacheinander aufgrund von Urlaub und vergleichbaren Dienst- oder Arbeitsbefreiungen nicht gearbeitet haben, am ersten Arbeitstag nach dieser Arbeitsunterbrechung dem Arbeitgeber einen tagesaktuellen Test vorzulegen oder im Verlauf des ersten Arbeitstages einen dokumentierten beaufsichtigten Test durchzuführen.

Erfolgte die Arbeitsaufnahme im Homeoffice, galt diese Verpflichtung für den ersten Tag, an dem die Arbeit im Betrieb oder an sonstigen Einsatzorten außerhalb der eigenen Häuslichkeit stattfindet. Zur Nachweisführung sollte die Gewährung der Einsichtnahme in die Test- oder Impfnachweise gemeinsam mit einem amtlichen Ausweispapier im Original genügen.

Mehr Informationen:
↗ sdb.de/tb2101

Hierzu habe ich auf meiner Website ausgeführt, dass aus datenschutzrechtlicher Sicht die Kontrolle der Testnachweise durch Vorlage seitens der Beschäftigten, ohne dass diese Tests oder Kontrollen mit einem Personenbezug dokumentiert werden, das mildeste Mittel seien und dementsprechend

eine Verarbeitung dieser Daten nicht zulässig sei. Stattdessen können Arbeitgeber lediglich dokumentieren, dass sie einen Prozess zur Durchführung derartiger Kontrollen eingeführt haben. Die bloße Dokumentation eines entsprechenden Kontrollprozesses erschien insoweit ausreichend, da § 9 Abs. 1a der SächsCoronaSchVO vom 14. Juli 2021 lediglich eine Vorlagepflicht der Beschäftigten regelte, jedoch keine Festlegungen hinsichtlich einer Pflicht des Arbeitgebers zu einer weitergehenden Dokumentation und einer damit einhergehenden Verarbeitung personenbezogener Daten traf.
Soweit Beschäftigte über einen vollständigen Impfschutz gegen SARS-CoV-2 verfügten oder von einer SARS-CoV-2-Infektion genesen waren, regelte § 9 Abs. 7 der SächsCoronaSchVO in der Fassung vom 14. Juli 2021, dass für diese Beschäftigten keine Pflicht zur Vorlage eines Testnachweises besteht, soweit diese nachweisen, dass sie über einen vollständigen Impfschutz gegen SARS-CoV-2 verfügen oder von einer SARS-CoV-2-Infektion genesen sind.
Auch dies konnte in einem entsprechenden Kontrollsystem berücksichtigt werden. Allerdings war auch die Dokumentation des Impf- oder Genesenenstatus aus datenschutzrechtlicher Sicht nicht nach § 9 Abs. 1 a und Abs. 7 der SächsCoronaSchVO vom 14. Juli 2021 zulässig, insbesondere darf der Impf- oder Genesenennachweis nicht kopiert werden.

Frage des Arbeitgebers nach dem Impf- oder Genesenenstatus

Nachdem im Sommer 2021 die Impfstoffe gegen Covid-19 nicht mehr nur prioritär abgegeben wurden, sondern breiten Teilen der Bevölkerung zur Verfügung standen, und zu befürchten war, dass die Infektionszahlen im Spätsommer und Frühherbst wieder ansteigen könnten, stellte sich zunehmend die Frage, ob Arbeitgeber das Recht haben, ihre Beschäftigten nach dem jeweiligen Impf- oder Genesenenstatus zu fragen. Eine gesetzliche Regelung zur Verarbeitung des Impf- und Serostatus existierte bis dahin nur für Beschäftigte bestimmter Einrichtungen, wie zum Beispiel Krankenhäuser, gemäß § 23 a in Verbindung mit § 23 In-

fektionsschutzgesetz. Für alle anderen Bereiche galten die allgemeinen arbeits- und datenschutzrechtlichen Regelungen, die in der Praxis häufig zu rechtlichen Unsicherheiten führten, ob ein Fragerecht besteht oder nicht. Insbesondere wurde diskutiert, ob nicht mit einer Einwilligung des Beschäftigten der Impfstatus abgefragt werden könnte.
Bereits am 29. März 2021 hatte die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) im Hinblick auf diese zu erwartenden rechtlichen Unsicherheiten eine Entschließung veröffentlicht, die den Gesetzgeber aufforderte, entsprechende klare gesetzliche Regelungen zu schaffen.

Entschließung der DSK:
↗ sdb.de/tb2102

Verarbeitung des Impfstatus auf Einwilligungsbasis

Es erreichte meine Behörde dann auch die Anfrage einer Fluggesellschaft, die klären wollte, ob sie den Impfstatus der bei ihr beschäftigten Piloten im Rahmen einer Einwilligung verarbeiten darf. Die Fluggesellschaft teilte mir mit, dass Gesundheitsbehörden anderer Staaten die Impfausweise (auch internationale) der Piloten nicht anerkennen würden, sondern auf einer Bestätigung des Arbeitgebers bezüglich des Impfstatus bestehen würden. Teilweise wurden – nach Angaben der Fluggesellschaft – Einreisebestimmungen weiter verschärft, sodass Piloten, die Voraufenthalte in bestimmten Ländern hatten, nur einreisen durften, wenn sie geimpft sind und einen PCR-Test vornehmen ließen, oder, falls diese ungeimpft seien, eine dreiwöchige Quarantäne angeordnet werden würde. Der Verantwortliche wollte nun aufgrund dieser Umstände im Rahmen einer Einwilligung den Impfstatus der Piloten verarbeiten, um die Quarantäne und längere Wartefristen im Flughafenbereich für die Piloten zu vermeiden.
Der verantwortlichen Stelle habe ich zunächst mitgeteilt, dass es sich bei den Daten zum Impfstatus um Gesundheitsdaten im Sinne des Art. 4 Nr. 15 DSGVO und damit besondere Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 DSGVO handelt. Die Verarbeitung besonderer Kategorien personenbezogener Daten ist nach Art. 9 Abs. 1 DSGVO grundsätzlich untersagt, sofern die in Art. 9 Abs. 2 und 3

DSGVO aufgezählten Ausnahmetatbestände nicht einschlägig sind. Der Zugang des Arbeitgebers zu Gesundheitsdaten der Beschäftigten aus Gründen des Schutzes der Persönlichkeitssphäre ist nur sehr begrenzt möglich. Grundsätzlich besteht kein Anspruch auf Kenntnis von Gesundheitsdaten. So dürfen zum Beispiel die Arbeitsunfähigkeitsbescheinigungen für den Arbeitgeber keine Diagnosen enthalten, vgl. § 69 Abs. 4 SGB X.

Im Übrigen existierte in Deutschland zu diesem Zeitpunkt keine Impfpflicht. Lediglich die Verarbeitung von Impfdaten durch den Arbeitgeber aus besonderen Gründen der Pandemiebekämpfung ist in § 23 a Infektionsschutzgesetz (IfSG) vorgesehen (für Einrichtungen nach § 23 Abs. 3 IfSG, wie zum Beispiel Krankenhäuser). Diese ausdrückliche gesetzgeberische Wertentscheidung, nur im Einzelfall ein Fragerecht zu bejahen und zu regeln, macht ebenfalls deutlich, dass eine allgemeine Verarbeitungsbefugnis der Angaben zum „Impfstatus" gerade nicht anzunehmen ist.

Als Rechtsgrundlage für die avisierte Datenverarbeitung kam daher auch in diesem Fall wieder nur eine Einwilligung nach Art. 9 Abs. 2 Buchst. a DSGVO, § 26 Abs. 2 in Verbindung mit Abs. 3 Satz 2 BDSG in Betracht, da weder die SächsCoronaSchVO noch andere Rechtsvorschriften, von gesetzlich ausdrücklich benannten Berufsgruppen (vgl. § 23 a, § 23 Abs. 3 IfSG) abgesehen, eine Verarbeitungsbefugnis und damit einhergehende Dokumentationspflicht des Arbeitgebers im Hinblick auf den Impfstatus vorsehen. Dementsprechend hat meine Behörde der verantwortlichen Stelle mitgeteilt, dass bei einer Verarbeitung der Angaben zum „Impfstatus" durch den Arbeitgeber auf der Grundlage einer ausdrücklichen Einwilligung nach Art. 9 Abs. 2 Buchst. a DSGVO die spezifischen Anforderungen an die Wirksamkeit der Einwilligung im Beschäftigungsverhältnis zu beachten wären, insbesondere in Bezug auf die Freiwilligkeit (Art. 4 Nr. 11 DSGVO). Ferner müssten die Anforderungen gemäß Art. 7 DSGVO und § 26 Abs. 2 BDSG erfüllt werden. Trotz der hohen Anforderungen, die an die Einwilligung und insbesondere das Kriterium der Freiwilligkeit im Beschäftigungsverhältnis zu stellen sind, ist diese

im Beschäftigungsverhältnis dennoch nicht ausgeschlossen. Gemäß § 26 Abs. 2 Satz 2 BDSG kann Freiwilligkeit insbesondere vorliegen, wenn für Beschäftigte ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeber und Beschäftigte gleichgelagerte Interessen verfolgen. Nach meiner Einschätzung war in dem mir vorliegenden Fall die Verarbeitung des Impfstatus durch den Arbeitgeber auf Basis einer Einwilligung zur Vermeidung der „Ableistung" einer behördlich angeordneten Quarantäne oder von längeren Aufenthalten im Flughafengebäude gleichermaßen für Arbeitgeber und Piloten vorteilhaft. Entsprechend den mir vorgetragenen Sachverhaltsschilderungen stellte sich dies nicht nur für den Arbeitgeber, insbesondere in Bezug auf seine wirtschaftlichen Interessen, quarantänebedingte Ausfälle zu verhindern, als vorteilhaft dar. Auch für die Piloten war es von Vorteil, die Anordnung der Quarantäne bzw. längerfristige Aufenthalte im Flughafengebäude, die ihre Ruhezeiten verkürzen würden, zu vermeiden.

Die datenschutzkonforme Abfrage des Impfstatus durch den Arbeitgeber, gestützt auf eine Einwilligung, war daher ein absoluter Ausnahmefall. Neben den hohen Anforderungen, die an eine datenschutzrechtlich wirksame Einwilligung gestellt werden, ist die Rechtsgrundlage der Einwilligung für den Arbeitgeber zusätzlich durch den jederzeit möglichen Widerruf der Einwilligung eine mit erheblichen Risiken verbundene Variante. Es sollte daher vorrangig geprüft werden, ob nicht andere Rechtsgrundlagen in Betracht kommen.

Die verantwortliche Stelle habe ich im Übrigen auf die weiteren Voraussetzungen einer datenschutzkonformen Einwilligung, die bereits im Tätigkeitsbericht von 2019 veröffentlicht wurden, hingewiesen. Auch in diesem Fall habe ich mitgeteilt, dass die verantwortliche Stelle innerhalb ihres Unternehmens eine informationell abgeschottete Vertrauensstelle – die von der personalverwaltenden Stelle abgesetzt ist – zu bilden habe, bei der Informationen zum Impfstatus eingehen. Die erhobenen Gesundheitsdaten müssen autonom von der Verarbeitung der weiteren Beschäftigtendaten erfolgen. Zu gewährleisten wäre mithin, dass die per-

Tätigkeitsbericht 2019:
↗ sdb.de/tb2103

sonalverwaltende Stelle keine Kenntnis/Information erhält, wer seinen Impfstatus gegenüber der informationell abgeschotteten Vertrauensstelle offenbart hat und wer nicht und selbstverständlich auch nicht über den tatsächlichen Impfstatus. Das bedeutete weiterhin, dass diese Gesundheitsdaten nicht in der Personalakte oder anderweitig verarbeitet werden dürfen. Insbesondere dürfen diese Daten nicht gegenüber Vorgesetzten etc. offengelegt werden.
Ich habe die verantwortliche Stelle darüber informiert, dass diese Verarbeitung von Gesundheitsdaten von Beschäftigten einer Datenschutz-Folgenabschätzung gemäß Art. 35 DSGVO bedarf und die Verarbeitung dieser Gesundheitsdaten in das Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 DSGVO aufzunehmen sei. Es wurde empfohlen, mit dem Betriebsrat eine entsprechende Vereinbarung zu treffen, die auch normative Wirkung hat und die die zuvor dargestellten datenschutzrechtlichen Anforderungen berücksichtigt (vgl. § 26 Abs. 4 BDSG).

§ 36 Abs. 3 Infektionsschutzgesetz

Mit § 36 Abs. 3 IfSG hat der Bundesgesetzgeber am 10. September 2021 für bestimmte Einrichtungen, wie zum Beispiel Schulen und Kindertageseinrichtungen, geregelt, dass bei einer vom Deutschen Bundestag festgestellten epidemischen Lage von nationaler Tragweite, der Arbeitgeber – soweit dies zur Verhinderung der Verbreitung von COVID-19 erforderlich ist – personenbezogene Daten eines Beschäftigten über dessen Impf- und Serostatus in Bezug auf die Coronavirus-Krankheit-2019 (COVID-19) verarbeiten darf, um über die Begründung eines Beschäftigungsverhältnisses oder über die Art und Weise einer Beschäftigung zu entscheiden.
Für alle anderen Beschäftigten, für die die gesetzlichen Ausnahmeregelungen des §§ 23a, 23 und 36 Abs. 3 IfSG nicht gelten, blieb es daher bei den allgemeinen arbeits- und datenschutzrechtlichen Regelungen.

2G-Optionsmodell

Daher stellte sich für viele Arbeitgeber mit Aufnahme eines 2G-Optionsmodells in die Sächsische Corona-Schutz-Verordnung vom 21. September 2021 erneut die Frage, ob sie den Impf- und Serostatus ihrer Beschäftigten erfragen dürfen. Meine Behörde hat dazu wiederum umfassend Stellung genommen.

Mehr Informationen:
↗ sdb.de/tb2104

Das sogenannte 2G-Optionsmodell ermöglichte in bestimmten Bereichen ausschließlich für Geimpfte und Genesene Angebote, in denen keine Pflicht zum Tragen eines Mund-Nasen-Schutzes und keine Pflicht zur Einhaltung des Abstandsgebotes sowie keine Beschränkung hinsichtlich der Auslastung der Höchstkapazität bestehen. Voraussetzung des 2G-Optionsmodells war, dass alle anwesenden Personen über einen Impf- oder Genesenennachweis verfügten. Gemäß § 6 a Abs. 1 Satz 2 SächsCoronaSchVO vom 21. September 2021 galt dies nicht für Beschäftigte, die über einen Testnachweis verfügen und einen medizinischen Mund-Nasen-Schutz während der Dauer der Veranstaltung oder des Angebots tragen. Soweit ein Arbeitgeber das 2G-Optionsmodell einführen wollte, stellte sich in der Praxis daher die Frage, ob der Arbeitgeber die Offenbarung des Impf- und Genesenenstatus oder die Offenbarung des Ergebnisses eines Tests auf das Nichtvorliegen einer Infektion mit SARS-CoV-2 von seinen Beschäftigten verlangen darf.

Meine Behörde vertritt die Auffassung, dass die Einführung des 2G-Optionsmodells für seinen Betrieb den Arbeitgeber regelmäßig nicht berechtigt, den Impf- oder Genesenenstatus des einzelnen Beschäftigten zu verarbeiten. Vielmehr bedarf es dazu einer eindeutigen gesetzlichen Rechtsgrundlage. Einen spezialgesetzlichen Erlaubnistatbestand im Sinne des Art. 9 Abs. 2 Buchst. b, h und i DSGVO für die Verarbeitung von Daten über den Impf- und Serostatus sieht wie bereits zuvor ausgeführt § 23a Satz 1 IfSG für die in § 23 Abs. 3 IfSG aufgezählten Arbeitgeber des Gesundheitsbereichs (unter anderem Krankenhäuser, Reha-Einrichtungen, Tageskliniken, Arzt- und Zahnarztpraxen, ambulante Pflegedienste, Rettungsdienste) vor. Die Verarbeitung des Impfstatus der

Beschäftigten ist somit nur durch die in § 23 Abs. 3 IfSG genannten Arbeitgeber zulässig. Durch die Änderung des IfSG vom 10. September 2021 wurde für die Dauer der epidemischen Lage von nationaler Tragweite und soweit dies zur Verhinderung der Verbreitung der Coronavirus-Krankheit-2019 erforderlich ist, geregelt, dass auch Arbeitgeber von in § 36 Abs. 1 und 2 IfSG benannten Einrichtungen (unter anderem Kindertageseinrichtungen, Kinderhorte, Schulen, Obdachlosenunterkünfte) ebenso den Impf- und Serostatus in Bezug auf die Coronavirus-Krankheit-2019 verarbeiten dürfen, um über die Begründung eines Beschäftigungsverhältnisses oder über die Art und Weise einer Beschäftigung zu entscheiden, vgl. § 36 Abs. 3 IfSG.

Auch im Rahmen des sogenannten 2G-Optionsmodells, welches überwiegend von Restaurants, Bars und Clubs genutzt wurde, haben daher die Arbeitgeber grundsätzlich anhand der allgemeinen datenschutzrechtlichen Grundlagen zu prüfen, ob ein Fragerecht bezüglich des Impf- und Serostatus besteht und darauf eine Datenverarbeitung gestützt werden kann.

In der vorgenannten Stellungnahme wies meine Behörde dementsprechend darauf hin, dass in diesem Fall regelmäßig die Verarbeitung dieser Gesundheitsdaten von Beschäftigten nicht auf eine Einwilligung gestützt werden könne. Auch § 26 Abs. 3 Satz 1 BDSG kommt in aller Regel als Rechtsgrundlage nicht in Betracht, da für die Verarbeitung des Impfstatus der Beschäftigten durch den Arbeitgeber keine rechtliche Pflicht aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und dem Sozialschutz erkennbar ist, da die Voraussetzungen an die qualifizierte Erforderlichkeit der Verarbeitung des Impfstatus nach § 26 Abs. 3 Satz 1 BDSG nicht gegeben sind.

Auch der vom sächsischen Verordnungsgeber neu geschaffene § 6a SächsCoronaSchVO in der Fassung vom 21. September 2021 konnte aus meiner Sicht nicht als Rechtsgrundlage für die Verarbeitung des Impf- oder Genesenenstatus oder Testergebnisses durch den Arbeitgeber im Rahmen des 2G-Optionsmodells herangezogen werden, da § 32 Satz 1 in Verbindung mit § 28 Abs. 1 Satz 1 und 2, § 28a Abs. 1, Abs. 2 Satz 1, Abs. 3 und Abs. 6 IfSG in der Fassung vom 23. Juli 2021 keine

entsprechende Regelungskompetenz zu dieser Datenverarbeitung für den sächsischen Verordnungsgeber vorsah.
Im Übrigen sah auch der Wortlaut des § 6a SächsCoronaSchVO keine Pflicht zur Vorlage des Impf- oder Genesenennachweises vor. Der Arbeitgeber war auch nicht berechtigt, das Ergebnis eines Corona-Tests auf das Nichtvorliegen einer Infektion mit SARS-CoV-2 vom Beschäftigten zu verarbeiten. Wie bereits zuvor ausgeführt, handelt es sich bei den Ergebnissen von Corona-Tests um Gesundheitsdaten im Sinne des Artikels 4 Ziffer 15 DSGVO. Für die Verarbeitung dieser Daten von Beschäftigten gelten die obigen Ausführungen zur Verarbeitung des Impf- und Serostatus entsprechend.
Auch auf § 6a SächsCoronaSchVO konnte die Verarbeitung dieser Gesundheitsdaten nicht gestützt werden, da dieser lediglich vorsah, dass Beschäftigte über einen Testnachweis verfügen müssen, eine Pflicht zur Vorlage wurde, abweichend zu § 5 Abs. 3 SächsCoronaVO in der Fassung vom 21. September 2021 (Testpflicht für Urlaubsrückkehrer), gerade nicht geregelt.
Aus diesem Grunde war regelmäßig ein Fragerecht des Arbeitgebers bezüglich des Impf- und Genesenenstatus im Rahmen des sogenannten 2G-Optionsmodells zu verneinen. Des Weiteren bestand regelmäßig kein Fragerecht des Arbeitgebers bezüglich des Ergebnisses eines Tests auf das Nichtvorliegen einer Infektion mit SARS-CoV-2. Es oblag daher den zuständigen Gesundheitsbehörden, die Einhaltung der Voraussetzungen des § 6a SächsCoronaSchVO zu prüfen.

Anwendungshilfe der DSK

Da im Zusammenhang mit der Corona-Pandemie regelmäßig eine Vielzahl von Fragen zur Verarbeitung von Beschäftigtendaten zu beantworten sind, hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder eine Anwendungshilfe veröffentlicht.

Anwendungshilfe der DSK:
↗ sdb.de/tb2105

Darin enthalten sind unter anderem auch Ausführungen zu der Thematik, ob Arbeitgeber den Impfstatus der Beschäftigten im Zusammenhang mit der Entschädigung nach § 56 Abs. 1 IfSG (sogenannte Quarantäneentschädigung) ver-

arbeiten dürfen und welche datenschutzrechtlichen Fragen beziehungsweise Anforderungen sich aus § 28b IfSG in der Fassung vom 22. November 2021 aus der sogenannten 3G-Regelung am Arbeitsplatz ergeben.

Einführung einer Überprüfungspflicht des Arbeitgebers zum Pandemie-Gesundheitsstatus

Nach § 28b IfSG sind Arbeitgeber nunmehr verpflichtet zu prüfen, ob Beschäftigte, die ihre Arbeitsstätte betreten, geimpft, genesen oder getestet sind (Überprüfungspflicht). Aus Gründen der Datenminimierung und Datensparsamkeit entsprechend Art. 5 DSGVO genügt dazu eine Sichtung des Impf-, Genesenen- oder Testnachweises durch den Arbeitgeber bzw. von diesem beauftragte Beschäftigte oder Dritte. Die Nachweiserbringung kann digital zum Beispiel mittels der CovPassCheck-App des Robert-Koch-Instituts erfolgen. Sollten Dritte mit der Erfüllung dieser Aufgaben betraut werden, ist gegebenenfalls ein Auftragsverarbeitungsvertrag abzuschließen. Dieser sollte insbesondere Regelungen zur Verschwiegenheitsverpflichtung des Dritten enthalten. Auch eingesetzte Beschäftigte sind durch den Arbeitgeber für die Verschwiegenheitspflicht zu sensibilisieren.
Es besteht für Arbeitgeber ebenso die Möglichkeit, für den Status „geimpft" oder „genesen" vereinfachte Kontrollprozesse zu implementieren. Mittels einer wirksamen Einwilligung kann der Arbeitgeber erfassen, ob der Beschäftigte geimpft oder genesen ist sowie gegebenenfalls das Enddatum des jeweiligen Status. Eine Kopie des Impf- oder Genesenennachweises ist dazu jedoch nicht erforderlich. Soweit Beschäftigte den 3G-Nachweis durch eine Testbescheinigung erbringen, gelten die vorherigen Ausführungen. Sollte der Nachweis im Rahmen einer betrieblichen Testung oder mittels Selbsttests unter Aufsicht erbracht werden, ist zu beachten, dass lediglich erfasst wird, dass ein Nachweis erbracht wurde; das negative Testergebnis darf nicht verarbeitet werden. Im Falle eines positiven Tests kann vermerkt werden, dass der Beschäftigte die Arbeitsstätte nicht betreten darf. Darüber hinausgehende Meldepflichten, wie etwa

an das zuständige Gesundheitsamt, können sich aus weiteren Regelungen ergeben.

Dokumentationspflicht der Arbeitgeber

Arbeitgeber müssen die Einhaltung der zuvor genannten Verpflichtungen dokumentieren, § 28b Abs. 3 Satz 1 IfSG. Dem Gesetzeswortlaut ist nicht zu entnehmen, in welcher Form – insbesondere welchem Differenzierungsgrad – die Dokumentation zu erfolgen hat. Arbeitgeber haben zur Überprüfung der Zutrittsvoraussetzungen Prozesse etabliert. Für die Erfüllung der Dokumentationspflicht wird daher ausreichend sein, diese Prozesse regelmäßig zu dokumentieren.
Auch im Jahr 2022 erwarte ich eine Vielzahl von arbeits- und datenschutzrechtlichen Fragestellungen im Beschäftigtenkontext im Zusammenhang mit der Corona-Pandemie.

1.2 Erleichterte Datenweitergabe innerhalb von Stadtverwaltungen unter Geltung der DSGVO?

↗ Art. 6 Abs. 4 DSGVO; §§ 3, 4 SächsDSDG

Der Datenschutzbeauftragte einer großen Stadtverwaltung fragte an, ob sich nach dem 25. Mai 2018, also nach der Anwendbarkeit der Datenschutz-Grundverordnung (DSGVO), Wesentliches im Hinblick auf Datenweitergaben innerhalb einer Kommunalverwaltung geändert habe. Ferner interessierte ihn auch die Fortgeltung der Grundsätze der Erforderlichkeit zur Aufgabenerfüllung, des Verbots mit Erlaubnisvorbehalt sowie der informationellen Gewaltenteilung. Der Datenschutzbeauftragte erhielt von meiner Behörde folgende Antwort:
Art. 6 Abs. 4 DSGVO eröffnet grundsätzlich auch öffentlichen Stellen die Möglichkeit einer zweckkompatiblen Weiterverarbeitung, das heißt einer Verarbeitung, die nahe am ursprünglichen Erhebungszweck liegt, aber eben nicht deckungsgleich ist. Unterschiedliche Ansichten bestehen darüber, ob sich Art. 6 Abs. 4 DSGVO in seiner Funktion auf eine Art Kompatibilitätstest beschränkt oder darüber hinaus

auch als Erlaubnistatbestand für eine zweckändernde Weiterverarbeitung einzuordnen ist. Für einen bloßen Kompatibilitätstest sprechen für mich überzeugend die Entstehungsgeschichte sowie die Regelungssystematik und der Wortlaut der Vorschrift, sodass ich im Ergebnis feststelle, dass zumindest für den öffentlichen Bereich, der an den Vorbehalt des Gesetzes gebunden ist, die Kompatibilität alleine keine zweckändernde Weiterverarbeitung erlaubt.

Nach meiner Auffassung kann eine zweckändernde Verarbeitung, insbesondere Datenübermittlung, im öffentlichen Bereich nur auf eine, meines Erachtens nur selten zulässige Einwilligung oder auf eine Rechtsvorschrift nach Art. 6 Abs. 1 Buchst. c oder e DSGVO gestützt werden. Als solche Rechtsvorschriften kommen die §§ 3 und 4 Sächsisches Datenschutzdurchführungsgesetz (SächsDSDG) in Betracht. Art. 6 Abs. 4 DSGVO spielt – abgesehen von Fällen der Einwilligung und der gesetzlich erlaubten Weiterverarbeitung für andere Zwecke (vgl. § 4 SächsDSDG) – für öffentliche Stellen meines Erachtens zum Beispiel in folgenden Fällen eine Rolle:

- Verwendung personenbezogener Daten für andere, vom Erhebungszweck abweichende Zwecke im eigenen Aufgabenbereich (Beispiel Landesjustizkasse: Kontodaten werden bei der Einzahlung durch den Justizkostenschuldner für Buchhaltung und evtl. Zahlungsrückabwicklung erhoben und in einem anderen, späteren Vollstreckungsverfahren gegen den Kostenschuldner – beides Aufgaben der Landesjustizkasse – weiter verwendet; der Erhebungszweck ist ein anderer als der spätere Verwendungszweck. Aber beides ist Eingriffsverwaltung, und die Befugnisgrundlage ist dieselbe.)
- Übermittlung an andere Behörden zum Zweck der eigenen Aufgabenerfüllung (Daten werden zum Beispiel mit der Bitte um Mitteilung, ob beim Empfänger dazu Informationen vorliegen, die die verantwortliche anfragende Behörde zur Aufgabenerfüllung benötigt, übermittelt. Ein anderer Fall ist die Vollstreckungshilfe.)

Im Ergebnis halte ich eine auf die „Zweckvereinbarkeit" gestützte Übermittlung durch öffentliche Stellen an andere Stellen zu dem Zweck, dass der Empfänger mit den übermittelten Daten seine Aufgaben erfüllen kann, für unzulässig beziehungsweise für nicht vereinbar mit den Kriterien von Art. 6 Abs. 4 DSGVO. Des Weiteren ist eine Weiterverarbeitung, insbesondere Übermittlung, selbstverständlich auf der Grundlage und im Rahmen spezieller gesetzlicher Weiterverarbeitungsvorschriften, insbesondere spezieller Übermittlungsvorschriften, zulässig. Die Voraussetzungen vorhandener spezieller Übermittlungsvorschriften sind also auch innerhalb der Stadtverwaltung weiterhin zu beachten.

Ausdrücklich keiner besonderen Befugnis soll nach dem Erwägungsgrund 50 Satz 4 DSGVO die „Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke" bedürfen.

Schließlich habe ich dem anfragenden behördlichen Datenschutzbeauftragten mitgeteilt, dass der Grundsatz der Erforderlichkeit – insbesondere auch für öffentliche Stellen – weiterhin gilt, wie sich aus Art. 6 Abs. 1 Buchst. b bis f DSGVO ergibt (wobei Buchstabe f nicht für die durch Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung anwendbar ist). Auch der Grundsatz des Verbots mit Erlaubnisvorbehalt gilt im öffentlichen Bereich weiterhin für jede Phase der Verarbeitung, also auch das Übermitteln, das heißt, es bedarf weiterhin einer Erlaubnisnorm auf der Grundlage von Art. 6 Abs. 1 DSGVO. Das Gleiche gilt auch für den Grundsatz der informationellen Gewaltenteilung.

Was ist zu tun?
Öffentliche Stellen müssen bei jeder Übermittlung an eine andere Stelle die Zulässigkeit dieser Übermittlung prüfen, auch wenn die andere Stelle Teil derselben Stadtverwaltung ist. Vgl. auch 2.2.9.

1.3 Erstellung der dynamischen Lehrmitteldatenbank Sachsen

Das Landesamt für Schule und Bildung kam im Frühjahr auf meine Behörde zu, mit der Bitte, bei der Erstellung einer dynamischen Lehrmitteldatenbank zu beraten. Ziel des Vorhabens ist es, digitale Angebote für alle Lehrerinnen und Lehrer in Sachsen nach pädagogischen Gesichtspunkten zu bewerten

und Einsatzmöglichkeiten im Unterricht aufzuzeigen. Natürlich spielt auch der Datenschutz dabei eine wichtige Rolle. Denn bei einer Vielzahl sicherlich interessanter und prinzipiell für schulische Zwecke gut geeigneter Angebote haperte es, nach einer groben Durchsicht der in Auswahl befindlichen Produkte und Websites, vor allem eben dort. Mein Amtsvorgänger hat das Angebot einer Mitwirkung daher dankbar aufgegriffen. Ich halte es ebenso für sinnvoll, eine Hilfestellung für Pädagoginnen und Pädagogen von zentraler Stelle aus vorzuhalten, anstatt jeder einzelnen Lehrkraft die Aufgabe der Prüfung der fachlichen Eignung und der rechtlichen Zulässigkeit aufzubürden.

Mit den beschränkten Personalressourcen meiner Behörde ist klar, dass meine Mitarbeiterinnen und Mitarbeiter nicht jedes einzelne Angebot einer solchen Datenbank überprüfen können. In mehreren Workshops wurden daher Kriterien erarbeitet, mit denen die Mitarbeiter der medienpädagogischen Fachbereiche des Landesamtes für Schule und Bildung eine zumindest kursorische Überprüfung von möglichen Angeboten vornehmen können, ohne selbst zu Experten für Datenschutz werden zu müssen.

Keine Datentransfers in das nichteuropäische Ausland

Eine solche Bewertung ist insbesondere vor dem Hintergrund eines möglichen Einsatzes in der Schule nicht ganz einfach. Die Verwaltungsvorschrift (VwV) Schuldatenschutz formuliert die Anforderungen erfreulich deutlich: „Es sind nur solche Cloud-Computing-Dienste zulässig, auf die das Recht der EU Anwendung findet." Das bedeutet, dass Datentransfers in das nichteuropäische Ausland zu unterbleiben haben. Das betrifft nicht nur den Standort des eigentlichen Anbieters der App oder der Website, sondern auch in das Angebot integrierte Dienste. Und dort liegt dann oft das Problem, dass viele Angebote zu Analysezwecken und aus Gründen der Vereinfachung auf Angebote meist US-amerikanischer Unternehmen zurückgreifen und dann eben Nutzungsdaten auch dort landen. Solche Angebote sind für schulische Zwecke klar ungeeignet und schlicht rechtswidrig.

Einwilligungen und Tracking

Ein weiteres Problem betrifft Einwilligungen in Datenverarbeitungen. Auch wenn es beim privaten Surfen oder bei der Installation einer App mittlerweile Usus ist, dass man in allerlei Dinge einwilligen soll, gelten für solche Einwilligung im schulischen Kontext besondere Regeln. Wenn ein Lernmittel zur Verfügung gestellt wird (oder im Fall der Lehrkräfte ein dienstlich genutztes Unterrichtsmittel) ist eine Einwilligung in aller Regel nicht möglich. Zum einen fehlt es an einer Freiwilligkeit, zum anderen sind viele Schülerinnen und Schüler gar nicht einwilligungsfähig, weil diese nicht das erforderliche Alter haben und somit die Eltern gefragt wären. Websites und Apps, die eine Einwilligung („Wir brauchen deine Zustimmung" oder Ähnliches) fordern, sind daher für den schulischen Einsatz nicht geeignet.

Auch beim Thema Tracking oder Werbung, welche das Verhalten von Nutzerinnen und Nutzern im Internet nachverfolgt, gelten enge Regeln. Eine solche Beobachtung des Verhaltens ist in aller Regel nicht mit dem Bildungsauftrag oder dem Beschäftigtendatenschutz vereinbar.

Prüfwerkzeuge für Apps und Websites

Wie können nun pädagogisch geschulte Mitarbeiter eine App oder eine Website in überschaubarer Zeit auf datenschutzrechtliche Probleme überprüfen? Im ersten Schritt wird die Datenschutzerklärung auf eventuelle Probleme (Einwilligungen, Übermittlung in Drittländer, Verständlichkeit und Transparenz) unter die Lupe genommen. Allerdings reicht dies leider nicht aus. In der Praxis wurde häufig festgestellt, dass Datenverarbeitungen, welche in der Datenschutzerklärung auftauchen, gar nicht stattfinden oder, weitaus schlimmer, Datenverarbeitungen stattfanden, die in der Datenschutzerklärung wiederum nicht erwähnt wurden. Insgesamt muss leider festgehalten werden, dass in vielen Fällen bereits die Datenschutzerklärung nicht das beste Licht auf die Anbieter wirft. Es muss also auch eine technische Analyse erfolgen. Einfach kann dies mit öffentlich verfügbaren Prüfwerkzeugen wie Privacy Score (privacyscore.org) oder Webkoll

Anwendungshilfe der DSK:
↗ sdb.de/tb2105

Was ist zu tun?
Bildungseinrichtungen müssen bei Einsatz von digitalen Lehr- und Lernmitteln sicherstellen, dass neben den Anforderungen der DSGVO auch bereichsspezifische Vorgaben sowie eine strikte Ausrichtung aller Datenverarbeitungen am Bildungsauftrag gewährleistet werden. Den Anforderungen an den Schutz der Daten von Minderjährigen sowie von Lehrkräften ist dabei in besonderer Weise gerecht zu werden.

(webbkoll.dataskydd.net) bzw. für Apps Exodus Privacy (exodus-privacy.eu.org) erfolgen. Mit diesen Instrumenten können die Mitarbeiter eine Entscheidung treffen und diese dokumentieren.

Insgesamt hat sich der Einsatz gelohnt. Die Mitarbeiter haben die Hintergründe der Entscheidungsfindung verinnerlicht, und in Zweifelsfällen hat sich auch ein kurzer Dienstweg etabliert, um in heiklen Fällen bei meiner Behörde nach Rat zu suchen. Die Zusammenarbeit mit dem Landesamt für Schule und Bildung kann daher als gelungener Weg betrachtet werden, Synergieeffekte auch für größere Vorhaben zu nutzen und schnell praxisorientierte Ergebnisse zu erzielen.

2 Grundsätze der Datenverarbeitung

2.1 Datenverarbeitungsgrundsätze, Begriffsbestimmungen

2.1.1 Fahrtenbuchauflage für ein Unternehmen – Datenminimierung

↗ § 31a Abs. 1 Satz 1 StVZO, Art. 5 Abs. 1 Buchst. c DSGVO

In einer Beratungsanfrage eines größeren handwerklichen Betriebes ist meine Dienststelle mit den datenschutzrechtlichen Auswirkungen der sogenannten Fahrtenbuchauflage nach § 31a Abs. 1 Satz 1 Straßenverkehrs-Zulassungs-Ordnung (StVZO) konfrontiert worden.

Eine Ordnungswidrigkeitenbehörde hatte das Unternehmen mit der (vorübergehenden) Führung eines Fahrtenbuches beauflagt und festgelegt, dass jeder Fahrzeugführer neben seinem Namen auch die Wohnanschrift einzutragen habe. Dies wiederum hatte der Geschäftsführer des Betriebs als unverhältnismäßige Verarbeitung ausgemacht, weil so eine Anschriftensammlung entstehen würde, in die eine Vielzahl von Beschäftigten Einblick erhalten würde. Er wandte sich daher ratsuchend an meine Dienststelle.

Letztendlich konnte meine Behörde die Bußgeldstelle davon überzeugen, dass es als (ladungsfähige) Anschrift ausreicht, wenn die Firmenanschrift eingetragen wird, gegebenenfalls ergänzt um die Abteilung, eine Personalnummer oder dergleichen, um Zuordnungsfehler auszuschließen. Entsprechendes ist ausreichend zur behördlichen Aufgabenerfüllung. Und seitens der Behörde ist auch nachzuvollziehen, dass der Verantwortliche – das Unternehmen – sich in Bezug auf eine

Datenverarbeitung zu beschränken hat, Art. 5 Abs. 1 Buchst. c DSGVO.

Um einer zureichenden und lückenlosen Buchführung gerecht zu werden, haben davon betroffene Unternehmen zusätzlich aber auch einzubeziehen, dass etwaige Fahrten durch Firmenfremde – zum Beispiel bei Probefahrten in einer Reparaturwerkstatt – einzutragen sind.

Praxishinweis

In dem meist vom Platz her beengten Fahrtenbuch muss dabei nicht bei jeder Fahrt die typischerweise zutreffende Firmenanschrift vollständig eingetragen werden. Es genügt für das korrekte Ausfüllen des Anschriftenfeldes ebenso ein simpler Binnenverweis („gemäß Seite …"). Auf dieser Seite könnte der Firmenstempel eingetragen sein. Mit seiner Unterschrift legitimiert der die Bucheintragung vornehmende Fahrzeugführer auch den Arbeitgeber und Verantwortlichen in einem zweiten Schritt zur Offenlegung seiner Wohnanschrift gegenüber Polizei, Ordnungswidrigkeitenbehörde, Finanzbehörden und Staatsanwaltschaft, falls ausreichende Verdachtsmomente dazu Anlass geben. Verständlicherweise haben Verwaltungsbehörden darauf zu achten, dass Vereinfachungen sich nicht zu Schlupflöchern entwickeln. Aber es soll auch keine unnötige Datenpreisgabe und zu viel Datenverarbeitung stattfinden. Insoweit gilt der Albert Einstein zugeschriebene Satz, dass etwas durchaus so einfach wie möglich gemacht werden darf – aber auch nicht einfacher!

Was ist zu tun?
In einem Unternehmen sind gegenseitige nicht erforderliche Offenbarungen von Beschäftigtendaten zu vermeiden. Zu den zu schützenden Informationen zählen insoweit auch die Privatanschriften der Beschäftigten. Auch öffentliche Stellen haben allgemeine datenschutzrechtliche Anforderungen, denen Unternehmen unterliegen, zu berücksichtigen.

2.1.2 Künstliche Intelligenz in der Schule: Area9 Rhapsode

↗ Art. 4 Nr. 1, 6 DSGVO

Im Februar 2021 informierte das Sächsische Staatsministerium für Kultus (SMK) meine Behörde, dass es beabsichtige, an sächsischen Schulen den Einsatz des „Intelligente Tutorielle System Area9 Rhapsode" zu testen. Das Besondere an dieser Lernplattform: Sie vermittelt nicht nur Inhalte und fragt Wissen ab, sondern erkennt auch die unterschiedlichen Wis-

sensstände der Schüler. Dementsprechend soll sie ihnen auf individuellen Lernwegen helfen, bis sie ein Thema wirklich verstanden haben. Neben inhaltlichen Antworten geben die Nutzer Auskunft über ihre Selbstsicherheit von „Das habe ich verstanden" über „Da bin ich unsicher" bis zu „Ich habe keine Ahnung". Gibt jemand eine falsche Antwort, kreuzt aber an, er sei sich sicher, erkennt das System eine unbewusste Inkompetenz – und umgekehrt. Das System kann mit Inhalten für alle Fächer, Schulformen und Altersstufen gefüttert werden. Diese können zwar auch selbst erstellt werden, werden aber wohl hauptsächlich – sofern diese „mitspielen" – von den Schulbuchverlagen kommen und in das System eingepflegt werden. Es liegt auf der Hand, dass dies insbesondere in Zeiten von Homeschooling ein vielversprechender Weg sein kann, Wissensstände selbstständig zu erweitern.

Entscheidend waren für meine Behörde zunächst die dabei entstehenden Datenflüsse. Der Hersteller, an den das SMK verwies, ging dabei davon aus, dass außer Benutzernamen, E-Mail und Passwort keine anderen persönlichen Daten der Benutzer verarbeitet würden. Alle anderen gesammelten Daten seien „Lerndaten" aus den Interaktionen des Benutzers mit dem System oder nicht personenbezogene „technische Informationen", bei denen Daten lediglich erhoben und verarbeitet würden, um die Geräte zu erkennen und zu registrieren, die für den Zugriff auf Rhapsode verwendet werden.

Meine Behörde wies den Hersteller und das SMK darauf hin, dass alle vorgenannten Daten einem Schüler zuzuordnen und somit personenbezogene Daten gemäß Art. 4 Nr. 1, 6 DSGVO sein dürften. Deren Verarbeitung bedarf daher – auch zu Testzwecken – einer Rechtsgrundlage. Dies auch, um sicherzustellen, dass Daten sächsischer Schüler nicht außerhalb des schulischen Kontextes beispielsweise zur Produktverbesserung genutzt werden. Ausdrücklich hinterfragte meine Behörde die Nutzung von „AWS-Diensten", also dem Cloud-Angebot von Amazon, da nicht vollumfänglich sichergestellt werden kann, dass alle Daten in Deutschland verbleiben. Die Fragen meiner Behörde blieben unbeantwortet.

Stattdessen war einer Pressemitteilung des SMK vom 8. Juli 2021 zu entnehmen, dass der Test des „Intelligente Tutorielle System (ITS) Area9 Rhapsode" gestartet wurde. Auf Nachfrage erfuhr meine Behörde, dass hierfür das Cloud-Angebot von Amazon genutzt wurde. Trotz dieses gravierenden Datenschutzverstoßes wurde von einer Anweisung nach Art. 58 Abs. 2 Buchst. f) DSGVO – den Testbetrieb sofort einzustellen – angesichts des bevorstehenden Schuljahresendes abgesehen. Der Staatsminister teilte meiner Behörde in einem Schreiben mit, dass die geäußerten Bedenken aufgrund mangelnder Abstimmung unterschiedlicher Beteiligter im SMK nicht berücksichtigt worden seien, und versicherte, dass für den künftigen Einsatz des Systems „Area9 Rhapsode" datenschutzrechtliche Belange in enger Abstimmung mit mir geprüft und gewährleistet werden. Dies ist auch mein Eindruck aus den Gesprächen, die es dazu mit dem SMK gab.

2.2 Rechtmäßigkeitsvoraussetzungen der Datenverarbeitung

2.2.1 Art. 6 Abs. 1 Buchst. e DSGVO in Verbindung mit einer Zuständigkeitsregelung keine Rechtsgrundlage für öffentliche Stellen

Gelegentlich erhalte ich auch im vierten Jahr der unmittelbaren Geltung der Datenschutz-Grundverordnung (DSGVO) auf die an eine Behörde oder sonstige öffentliche Stelle gerichtete Frage nach der Rechtsgrundlage für die dort vorgenommene Verarbeitung personenbezogener Daten die Antwort, die Verarbeitung werde auf Art. 6 Abs. 1 Buchst. e DSGVO in Verbindung mit der für die angefragte Stelle einschlägige gesetzliche Zuständigkeitsregelung gestützt.
Diese Auffassung ist jedenfalls hinsichtlich öffentlicher Stellen des Freistaates Sachsen unzutreffend.

Weil die Kenntnis der zutreffenden Rechtsgrundlage für die Rechtmäßigkeit behördlicher Verarbeitungen personenbezogener Daten unabdingbar und die Angabe gegenüber betroffenen Personen nach Art. 13 Abs. 1 Buchst. c DSGVO verpflichtend sind, sind Ungenauigkeiten in dieser Frage inakzeptabel.

Art. 6 Abs. 1 Buchst. e DSGVO bildet auch in Verbindung mit einer gesetzlichen Aufgabenzuweisung keine Rechtsgrundlage für die Verarbeitung personenbezogener Daten durch öffentliche Stellen. Erforderlich ist vielmehr eine Rechtsvorschrift im Sinne von Art. 6 Abs. 3 Satz 1 DSGVO, die explizit die Verarbeitung personenbezogener Daten erlaubt. Dass diese Verarbeitung für die Aufgabenerfüllung der öffentlichen Stelle erforderlich sein muss, ist selbstverständlich (Art. 6 Abs. 3 Satz 2 DSGVO, vgl. auch Erwägungsgrund 45 Satz 1 und 3 der DSGVO). Mitgliedsstaatliche Verarbeitungsvorschriften als Rechtsgrundlage für Eingriffe in das Grundrecht auf informationelle Selbstbestimmung nach Art. 6 Abs. 1 Buchst. e DSGVO müssen den verfassungsrechtlichen Anforderungen an Eingriffsnormen für staatliche Stellen genügen (Erwägungsgrund 41 der DSGVO). Reine Aufgabenzuweisungen verfehlen auch in Verbindung mit Art. 6 Abs. 1 Buchst. e DSGVO die Anforderungen des Europäischen Gerichtshofs (EuGH) und des Europäischen Gerichtshofs für Menschenrechte (EGMR) an die Bestimmtheit und „Vorhersehbarkeit" einer grundrechtsbeeinträchtigenden Norm, die nach dem Willen des EU-Verordnungsgebers bei „Rechtsgrundlagen" im Sinne der DSGVO zu berücksichtigen sind (Erwägungsgrund 41 der DSGVO). Nationales Verfassungsrecht, das hier zum selben Befund führt, bleibt im Rahmen von Art. 6 Abs. 1 Buchst. c und e DSGVO – hinsichtlich dieser Bestimmungen weist die DSGVO, wie auch an einzelnen anderen Punkten, Richtliniencharakter auf und lässt den Mitgliedsstaaten Gestaltungsspielraum – in Verbindung mit Art. 6 Abs. 2 und 3 DSGVO nach dem Willen des Verordnungsgebers unberührt (Erwägungsgrund 41 der DSGVO), sodass auch die vom Bundesverfassungsgericht formulierten Anforderungen an die Bestimmtheit von Eingriffsnormen zu erfüllen sind. Das ist

bei ausdrücklichen Verarbeitungsbefugnissen der Fall, nicht aber bei reinen Aufgabenzuweisungsnormen.

Hinsichtlich der Verarbeitung personenbezogener Daten durch sächsische öffentliche Stellen im Sinne von § 2 Abs. 1 Sächsisches Datenschutzdurchführungsgesetz (SächsDSDG) hat der Gesetzgeber in § 3 Abs. 1 SächsDSDG bestimmt, dass – sofern die Verarbeitung nicht auf vorrangige Vorschriften im speziellen Fachrecht gestützt werden kann – eine Verarbeitung zulässig ist, wenn sie zur Erfüllung der in der Zuständigkeit des Verantwortlichen liegenden Aufgabe oder in Ausübung öffentlicher Gewalt, die dem Verantwortlichen übertragen wurde, erforderlich ist. Kommt keine bereichsspezifische Datenverarbeitungsvorschrift zur Anwendung, greift § 3 SächsDSDG gewissermaßen als Auffangnorm für die Datenverarbeitung öffentlicher Stellen des Freistaates.

Der „Rückgriff" einer öffentlichen Stelle des Freistaates bei der Bestimmung der für ihre Verarbeitung personenbezogener Daten einschlägigen Rechtsgrundlage auf Art. 6 Abs. 1 Buchst. e DSGVO in Verbindung mit einer Zuständigkeitsregelung ist damit – ganz gleich, ob ein solcher Rückgriff aus Unkenntnis der einschlägigen nationalen Rechtsvorschrift(en) oder aus Unwillen erfolgte, diese anzuwenden – weder zulässig (siehe oben) noch notwendig. Es steht sächsischen öffentlichen Stellen nicht zu, geltendes Recht außer Acht zu lassen und wirksame, sie adressierende Rechtsvorschriften nicht zur Anwendung zu bringen. Selbstverständlich liegt hier auch kein Fall eines möglichen Anwendungsvorrangs von EU-Recht vor.

Was ist zu tun?
Öffentliche sächsische Stellen müssen die Rechtsgrundlage für ihre Verarbeitung personenbezogener Daten kennen, bezeichnen und betroffene Personen hierüber informieren. Ein Rückgriff auf Art. 6 Abs. 1 Buchst. e DSGVO in Verbindung mit einer gesetzlichen Zuständigkeitszuweisung ist ausgeschlossen.

2.2.2 E-Mail-Aushang im Lehrerzimmer

↗ Art. 6 DSGVO

Eine Praxisberaterin, die Berufsorientierung an Oberschulen durchführt, informierte meine Behörde, dass sie von ihrem privaten E-Mail-Account eine Nachricht an die private E-Mail-Adresse der Schulleiterin geschickt hatte. In der Nachricht hatte sie unter anderem die Erkrankung ihres Kindes als Grund für ihre Fehlzeiten angeführt. Die Praxisberaterin

erfuhr später, dass diese E-Mail im Lehrerzimmer aushing und somit sowohl ihre private E-Mail-Adresse als auch deren Inhalt für die gesamte Lehrerschaft einsehbar war.
Die von meiner Behörde um Stellungnahme gebetene Schulleiterin teilte mit, dass die Fehlzeiten der Petentin zu Erklärungsnot gegenüber Schülern und Eltern geführt hätten. Deshalb habe sie den Träger der Praxisberatung kontaktiert, der eine E-Mail der Petentin ankündigte. Die Schule konnte bei dieser daher ungeachtet der verwendeten privaten E-Mail-Adresse von einem dienstlichen Bezug ausgehen.
Nicht erforderlich war jedoch, dass diese E-Mail vollständig im Lehrerzimmer aushing. Meine Behörde teilte der Schulleiterin daher mit, dass auch eine Information über „persönliche Gründe" bzw. eine Schwärzung der jeweiligen Passagen ausreichend gewesen wäre. Alternativ hätte auch die Petentin um eine entsprechende Einwilligung gebeten werden können.

2.2.3 Datenübermittlung einer Mobilfunknummer durch den Händler an einen Versanddienstleister

↗ § 242 BGB, Art. 6 Abs. 1 Buchst. b DSGVO, Art. 13 Abs. 1 Buchst. e DSGVO, Art. 14 DSGVO

Ein Kunde eines Online-Händlers beschwerte sich, dass seine nur für den Händler bestimmte Mobilfunknummer durch diesen an den Versanddienstleister übermittelt und dieser ihm vor Eintreffen der bestellten Ware beim Kunden hierüber eine SMS zugesandt hätte. Beschwerden dieser Art, was Datenweitergaben anbelangt, hat meine Behörde nicht selten zu verzeichnen.
Verkompliziert wurde der Sachverhalt dadurch, dass der Kunde aufgrund einer saisonalen Bonusaktion und regionaler Verfügbarkeit in den Genuss einer aufpreislosen Expresslieferung gelangt war. Das bei Bestellung bereits vorbelegte Feld („Express") dürfte der Kunde entweder übersehen oder in seiner Wirkungsweise verkannt haben.

Als Rechtsgrundlage für die Übermittlung der Rufnummer an den Versanddienstleister kam vorliegend Art. 6 Abs. 1 Buchst. b Datenschutz-Grundverordnung (DSGVO) wegen der bestimmungsgemäßen Vertragserfüllung in Betracht. Auf eine Einwilligung kam es im streitigen Fall nicht an. Die Versendung war mit Vertragsinhalt gewesen, die Gratis-Express-Lieferung vom Kunden gewählt worden. Es gehört auch zur Obliegenheit des E-Commerce-Kunden, sich über die Lieferbedingungen vor dem Vertragsschluss zu informieren, was im vorliegenden Fall nach meinen Feststellungen mühelos mit einem Blick auf den Auswahlbereich auf der Internetpräsenz möglich und abänderbar gewesen war. Die Bestellseite war insoweit verständlich und keinesfalls irreführend.

Bei Beauftragung der Versandart „Express" ist nach meiner Überzeugung eine Benachrichtigung des Kunden auf eine Weise, die dieser sofort zur Kenntnis zu nehmen in der Lage ist, kundenseitig gewünscht und unternehmensseitig erforderlich. Sie entspricht insoweit auch § 242 Bürgerliches Gesetzbuch (BGB). Andere Kommunikation, zum Beispiel E-Mail-Benachrichtigungen, würde nach allgemeiner Lebenserfahrung in zu vielen Fällen nicht eine für den geschuldeten Express-Sendeweg rechtzeitige Kenntnisnahme des Empfängers mit sich bringen. In Anbetracht der Interessenlage bin ich dem Grunde nach von einer Zulässigkeit der Übermittlung der von dem Kunden im Bestellvorgang einzutragenden Telefonnummer an den Postdienstleister ausgegangen.

Als Rechtsmangel hatte das Unternehmen indes zu verantworten, dass es auf die Übermittlung der Telefonnummer an den bei Beauftragung der Versandart „Express" nicht explizit in seinen Datenschutzhinweisen eingegangen ist, Art. 13 Abs. 1 Buchst. e DSGVO. Daran schloss sich die Frage an, ob sich dies gegebenenfalls auf die Zulässigkeit der Datenübermittlung auswirkt. Im Ergebnis habe ich dies wiederum verneint. Ausschlaggebend waren für mich dabei folgende Überlegungen:

Sogar anzunehmendes berechtigtes Interesse ist nach Erwägungsgrund 47 der Datenschutz-Grundverordnung daran zu messen, ob eine betroffene Person in der gegebenen Situation vernünftigerweise mit einer Verarbeitung rechnen muss. Dies gilt erst recht in Vertragsverhältnissen.

Eine im Vorfeld nicht ausreichend klar kommunizierte Vorgehensweise wäre zwar generell geeignet, die Erwartungshaltung in Richtung Ausschluss der Verarbeitung zu beeinflussen; dies gilt jedoch nicht pauschal, sondern es ist der Einzelfall zu betrachten. Dafür spricht letztendlich auch die Tatsache, dass Art. 13 DSGVO selbst keine Aussage zur etwaigen Rechtsfolge der Verletzung der Informationspflicht trifft.

Besondere Umstände waren dem zu prüfenden Einzelfall nicht zu entnehmen. Damit verbleibt die Prüfung auf die (insbesondere für die Warengruppe) typische Erwartungshaltung aufseiten des Kunden. Hier bin ich zu dem Ergebnis gelangt, dass eine mithilfe aller zur Verfügung stehenden Kommunikationswege erfolgreiche Belieferung jedenfalls bei Expresssendungen als gemeinhin üblich betrachtet werden kann und muss. Die Weitergabe von über die Namen und Anschrift hinausgehenden Kontaktdaten an den Postdienstleister ist für den Kunden bei Eillieferungen letztendlich auch subjektiv erwartbar. Aus dem Mangel in den Datenschutzinformationen konnte für den beschriebenen Sachverhalt kein Ausschluss einer Datenweitergabe abgeleitet werden.

Meine Behörde hat das Unternehmen allerdings auf die – auf die konkreten Umstände bezogen – missverständliche Abfassung der Datenschutzhinweise hingewiesen und eine klarstellende Formulierung angeregt. Die entsprechende Datenschutzerklärung ist daraufhin angepasst worden.

Es wäre lebensfremd, flächendeckend lückenlose und völlig korrekte Datenschutzinformationen gemäß Art. 13 und 14 DSGVO der datenverarbeitenden Unternehmen und anderen Stellen zu erwarten. Die Rechtsfortbildung ist, was die Datenschutz-Grundverordnung und die Auslegung der Normen betrifft, noch längst nicht abgeschlossen; von einer kohärenten europaweiten Anwendung der Bestimmungen ganz zu schweigen. Soweit die Verantwortlichen an der Abstellung von Infor-

Was ist zu tun?

Gerade im Bereich des Handels, insbesondere beim E-Commerce, sollten Verantwortliche schon aus Eigeninteresse die Informationspflichten gemäß Art. 13 und 14 DSGVO vollständig erfüllen. Gegebenenfalls ist fachkundiger Rat einzuholen. Streitige Datenweitergaben sind im Rahmen von Vertragsverhältnissen auch unter Einbeziehung der Generalklausel des § 242 BGB, nach Treu und Glauben mit Rücksicht auf die Verkehrssitte im Hinblick auf deren Zulässigkeit zu beurteilen.

mationsmängeln kooperativ mitwirken, erkenne ich aber auch meine Arbeit als fruchtbringend. Ich werbe aber ebenso dafür, dass sich Verantwortliche bei Bedarf und in Zweifelsfällen frühzeitig an sachkundige Datenschutzberater wenden.
Schwerer als Unsicherheiten und Fehler wiegen strukturelle Wiederholungsfälle und Versuche, Fehlverhalten zu verschleiern. Entsprechendes gilt es gegebenenfalls auch zu sanktionieren.

2.2.4 Videoüberwachung zur Analyse des Fahrverhaltens von E-Scootern

↗ § 15 Abs. 4 eKFV; Art. 6 Abs. 1 Buchst. f DSGVO; Art. 9 Abs. 1, 2 DSGVO; § 27 Abs. 1 BDSG; Art. 25 und 32 DSGVO

Seit der Freigabe der Elektrokleinstfahrzeuge (eKF) – besser bekannt als E-Scooter – im öffentlichen Straßenverkehr ist die Anzahl von Unfällen mit diesen Fahrzeugen stark angestiegen. Bereits mit deren Zulassung wurde eine wissenschaftliche Begleitung der Teilnahme von eKF am Straßenverkehr angeregt (§ 15 Abs. 4 Elektrokleinstfahrzeugeverordnung – eKFV), welche durch die Bundesanstalt für Straßenwesen (BASt) mit dem Forschungsvorhaben „Wissenschaftliche Begleitung der Teilnahme von Elektrokleinstfahrzeugen am Straßenverkehr" auf den Weg gebracht wurde. Mit der Durchführung des Forschungsvorhabens hat die BASt die Verkehrsunfallforschung an der TU Dresden GmbH (VUFO) gemeinsam mit unterschiedlichen Partnern beauftragt, um letztlich mit korrekter Argumentation die Diskussion um die Fahrzeuge zukünftig auf sachlicher Grundlage zu gestalten.

Forschungsziel und -konzeption

Vor diesem Hintergrund wandte sich die VUFO mit einem die datenschutzrechtlichen Aspekte des Forschungsvorhabens umfassenden Datenschutzkonzept an meine Dienststelle. Ein wesentlicher Forschungsbestandteil lag in der Analyse des Fahrverhaltens von E-Scootern, welches die VUFO mittels Videobeobachtung in realen Verkehrssituationen (begrenzter Streckenabschnitt) genauer erforschen wollte. Als Orte

für die Verkehrsbeobachtung waren Straßenzüge sowohl in Dresden als auch in Berlin vorgesehen, wobei sich die Standortwahl nach der Frequenz an eKF-Durchfahrten, infrastrukturellen Aspekten und einer möglichen hohen Anzahl an Konflikten orientierte.

Hierzu sollte auf einer Höhe von 4 Metern eine Kamerabox (Mobile Beobachtungsbox) mit einem Aufnahmegerät angebracht werden, in dem die Videosequenzen zum Schutz vor unberechtigtem Zugriff verschlüsselt gespeichert werden. Die Auswertung des Videomaterials sollte bei einem dafür spezialisierten Unternehmen in Wien stattfinden, da eine automatisierte Verarbeitung vor Ort sowohl aus Platz- als auch aus Sicherheitsgründen nicht möglich war. Der Zugriff auf die Videoaufnahmen sowie die Selektion für das Forschungsvorhaben relevanter Sequenzen sollte ausschließlich automatisch erfolgen und das übrige Videomaterial – nach Auswertung und Pseudonymisierung – im unmittelbaren Anschluss gelöscht werden. Bereits durch die Herabsetzung der Bildqualität sollten die Identifikation natürlicher Personen erschwert und auch durch einen wöchentlichen Standortwechsel längere, durchgehende Aufnahmezeiten vermieden werden.

Von der Videoüberwachung potenziell betroffen waren sowohl die Nutzer von eKF als auch die beteiligten Konfliktpersonen sowie unbeteiligte, zufällig anwesende und beobachtete Personen. Die Datenverarbeitung erfolgte auf Basis von Algorithmen, die automatisiert eKF im Straßenverkehr auf der Basis ihres speziellen Erscheinungsbildes erkennen und daraus eine Fahrlinie (Trajektorie) erstellen. Weder war somit ein „Erkennen" von Nutzern noch eine manuelle Durchsicht des Videomaterials vorgesehen. Ziel der Videobeobachtung war es, mithilfe der zeitlichen Abfolge der Bildsequenzen Fahrbewegungen und Geschwindigkeiten nachzuvollziehen und darzustellen, um Erkenntnisse zu gefahrenen Geschwindigkeiten, gehaltenen Abständen sowie den genutzten Verkehrsflächen zu gewinnen. Zusätzlich sollte eine unfallanalytische Bewertung von eventuell entstandenen Konflikt- bzw. Unfallsituationen erfolgen. Auch wenn im Gegensatz

zu einem Laborversuch eine Beeinflussung des Verkehrsverhaltens möglichst vermieden werden sollte, sah das Datenschutzkonzept – gezwungenermaßen – eine entsprechende Hinweisbeschilderung vor.

Verarbeitung von Gesundheitsdaten

Unerlässlich für den Erfolg des Forschungsvorhabens war insbesondere die Kenntnis über Art und Schwere von Verletzungen bei einem Unfallgeschehen unter Beteiligung von Elektrokleinstfahrzeugen. Damit ließen sich anhand des beobachteten (Unfall-)Geschehens mittelbar Rückschlüsse auf den Gesundheitszustand der am Unfall beteiligten Personen ziehen. Letztlich handelt es sich dabei um Gesundheitsdaten (besondere Kategorien personenbezogener Daten, Art. 4 Nr. 15 DSGVO), für die ein gesetzliches Verarbeitungsverbot besteht (Art. 9 Abs. 1 DSGVO). Der nationale Gesetzgeber hat mit dem Bundesdatenschutzgesetz (BDSG) von der in Art. 9 Abs. 1 Buchst. j DSGVO enthaltenen Öffnungsklausel Gebrauch gemacht und dort in § 27 für Zwecke der Wissenschaft und Forschung konkretisiert, unter welchen Voraussetzungen das grundsätzliche Verarbeitungsverbot des Art. 9 Abs. 1 DSGVO ausnahmsweise keine Geltung hat. Voraussetzung hierfür ist nach § 27 Abs. 1 BDSG, dass

- die Verarbeitung besonderer Kategorien personenbezogener Daten für die genannten Zwecke erforderlich ist und
- verschärfend zur allgemeinen Interessenabwägung des Art. 6 Abs. 1 Buchst. f DSGVO die Interessen des Verantwortlichen an der Verarbeitung zu den privilegierten Zwecken die Interessen der betroffenen Person erheblich überwiegen.

Dabei bilden Art. 9 DSGVO bzw. § 27 BDSG allein keine eigenständige Rechtsgrundlage für die Verarbeitung personenbezogener Daten. Denn die Beurteilung der rechtlichen Zulässigkeit für die Verarbeitung von Gesundheitsdaten kann nur gemeinsam mit einer Vorschrift des Art. 6 Abs. 1 DSGVO erfolgen. Die datenschutzrechtliche Zulässigkeit der Verkehrsbeobachtung sowie der damit einhergehenden Verarbeitung personenbezo-

gener Daten sah ich mit den berechtigten Interessen des Art. 6 Abs. 1 Buchst. f DSGVO in Verbindung mit Art. 9 Abs. 2 Buchst. j DSGVO (in Verbindung mit § 27 Abs. 1 BDSG) begründet. Meine Behörde konnte sich der von der VUFO vorgenommenen Risikobewertung anschließen und kam zu dem Ergebnis, dass mit den zahlreichen Vorkehrungen und Maßnahmen der VUFO letzten Endes ein nur minimaler Rechtseingriff verbunden war. Jedenfalls ergab sich vorliegend kein Ansatz für ein das Forschungsinteresse überwiegendes Interesse der im Beobachtungsbereich agierenden Verkehrsteilnehmer.

Datenschutzkonforme Umsetzung

Gegenstand der Befassung war die Prüfung der datenschutzrechtlichen Schwerpunkte des Forschungskonzepts. In dieser Hinsicht hat meine Behörde der VUFO ihre Anmerkungen zum vorgestellten Konzept mitgeteilt, die entsprechend umgesetzt wurden. Im bilateralen Austausch wurden die durch das Forschungsvorhaben implizierten datenschutzrechtlichen Grundsätze erörtert und übereinstimmende Festlegungen hierzu getroffen sowie eine Verständigung über grundsätzliche Positionen erzielt. Wichtig war dabei, auch die Öffentlichkeit im Vorfeld darüber zu informieren. Sowohl in der Presse als auch auf den Webseiten der VUFO und meiner Behörde erschienen dazu Informationen. Die VUFO hat an den betroffenen Straßenabschnitten vor Eintritt in den videoüberwachten Bereich außerdem ein den Datenschutzvorgaben entsprechendes vollständiges Informationsblatt angebracht. Zusätzlich habe ich die VUFO noch zur Sicherstellung der technischen und organisatorischen Maßnahmen gemäß der Art. 25 und 32 DSGVO angehalten.

Ob es letztlich an der groß angelegten Öffentlichkeitsarbeit lag oder an der professionellen Umsetzung seitens der VUFO, lässt sich nicht genau sagen, jedoch erreichte meine Behörde keine einzige Anfrage oder Eingabe zur Verkehrsbeobachtung. Im Ergebnis leisteten die unter Beteiligung der Dresdner Verkehrsteilnehmer gewonnenen Daten als Grundlage für eine darauf aufbauende Evaluierung des E-Scooter-Fahrverhaltens einen wichtigen Beitrag, die künftige Beteiligung der

Was ist zu tun?
Videoüberwachung in allgemein zugänglichen Bereichen ist – orientiert am Zweck – zu minimieren, zu pseudonymisieren und zeitnah zu anonymisieren. Diese sind in der Praxis nur in Ausnahmefällen nach umfassender Interessenabwägung vertretbar. Automatisierten Verfahren hingegen, die die augenblickliche Umrechnung der erhobenen Videoaufnahmedaten in Informationen gewährleisten, die nicht mehr einzelnen Individuen zugeordnet werden können, ist der Vorzug zu geben.

E-Scooter am Straßenverkehr sicherer zu machen. Man darf gespannt sein, wie und in welcher Form die gewonnenen Erkenntnisse in den durch das Bundesministerium für Verkehr und digitale Infrastruktur erarbeiteten Vorschlag für die Änderung der eKFV Eingang finden.

2.2.5 Grenzen der Videoüberwachung von privaten Grundstücken

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

Oftmals wähnen sich private Kamerabetreiber im Einklang mit dem Datenschutzrecht, wenn sie ihre Videokameras ausschließlich auf ihre eigenen privaten Grundstücksflächen ausrichten. In den meisten Fällen habe ich hiergegen auch nichts einzuwenden. Denn das Datenschutzrecht findet bei der Videoüberwachung dann keine Anwendung, wenn sie von einer natürlichen Person zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten und somit ohne Bezug zu einer beruflichen oder wirtschaftlichen Tätigkeit vorgenommen wird, vgl. die sogenannte Haushaltsausnahme in Art. 2 Abs. 2 Buchst. c Datenschutz-Grundverordnung (DSGVO). Eine Videoüberwachung lässt sich damit jedoch dann nicht rechtfertigen, wenn auf dem Privatgrundstück (auch) ein Gewerbebetrieb mit Kundenverkehr eingerichtet ist oder ein Mietswohnhaus steht. Der Rückgriff auf die Haushaltsausnahme greift auch in den privaten Grundstücksbereichen nicht, in denen andere Personen ein Betretungs-, Nutzungs- oder Aufenthaltsrecht haben.

So wenden sich gelegentlich Anwohner eines Hinterliegergrundstücks an mich. Denn wer ein Grundstück kauft, welches über keinen eigenen Straßenanschluss verfügt, kann hierzu nur den Weg über das benachbarte Grundstück nehmen. Erfahrungsgemäß ist dies oft der Ausgangspunkt für einen Nachbarschaftsstreit, etwa darüber, wer bei einer Abnutzung oder Beschädigung für die Reparaturkosten des Weges aufkommt. So verhielt es sich in einem Fall, der meiner Behörde bekannt wurde. Hintergrund waren angebliche Schäden am Weg, die der Hinterlieger verursacht haben soll.

Zu deren Dokumentation brachte der Nachbar eine Videokamera an.

Aufgrund der Nichtanwendbarkeit der genannten Haushaltsausnahme könnte sich eine Zulässigkeit allenfalls aus den berechtigten Interessen ergeben, Art. 6 Abs. 1 Buchst. f DSGVO. Jedoch ist ein Rückgriff darauf zur Legitimation der Videoüberwachung des grundbuchrechtlich gesicherten Zufahrtsbereichs, auch wenn dieser auf dem eigenen Grundstück des Kamerabetreibers liegt, nicht möglich. Selbstverständlich darf der Grundstückseigentümer bei Vorliegen der Voraussetzungen des Art. 2 Abs. 2 Buchst. c DSGVO alle anderen vom Wegerecht nicht umfassten Bereiche zulässigerweise überwachen. Dies gilt jedoch auf dem vom Grundbucheintrag umfassten Wegebereich nicht mehr – dort überwiegen die schutzwürdigen Interessen der Nutzer des Wegerechts (Hinterlieger, Besucher, Handwerker, Postdienstleister etc.), bei der für sie unvermeidbaren Passage dieses Weges nicht vom Eigentümer per Video überwacht zu werden.

Zum gleichen Ergebnis gelange ich, wenn der Grundstückseigentümer seine Privatstraße überwacht. So geschehen bei einem weiteren an mich herangetragenen Fall, bei dem sich die Privatstraße im Eigentum mehrerer Anwohner befand. Zwar waren sich die Eigentümer der Privatstraße über die Videoüberwachung dort einig, jedoch änderte dies nichts an meiner rechtlichen Wertung. Auch in diesem Fall ist der Betroffenenkreis viel weiter gefasst, zumal sich der Kreis der Anwohner erweitert und diese keinen Anteil an der Privatstraße haben, jedoch zum Erreichen ihres Grundstücks diese Zuwegung nutzen müssen. Letztlich lässt sich eine Videoüberwachung bereits aus rein praktischen Gründen in kaum einem denkbaren Fall auf die Einwilligungslösung stützen, wäre hierfür doch die informierte und freiwillige Einwilligung aller davon betroffenen Personen notwendig, Art. 6 Abs. 1 Buchst. a DSGVO.

In einem anderen Fall wandte sich ein Bürger an meine Behörde, weil er an einem öffentlichen Wanderweg eine Videokamera erspähte. Wie sich bei meinen Untersuchungen herausstellte, lag dieser zwar auf einem Privatgrundstück, jedoch wurde der

Weg schon vor mehreren Jahrzehnten als beschränkt-öffentlicher Weg von der Kommune gewidmet. Insoweit ist der Grundstückseigentümer in der Nutzung seines Privateigentums eingeschränkt und darf nicht die den Weg nutzenden Wanderer und Spaziergänger permanent überwachen.

Was Wildkameras in privaten Waldflächen angeht, erreichen mich auch hierzu hin und wieder Eingaben und Anfragen. Hiermit befasste sich bereits mein Amtsvorgänger im 7. Tätigkeitsbericht (Nr. 8.1.2), allerdings damals unter Geltung des alten Bundesdatenschutzgesetzes und damit der Rechtslage vor Anwendung der Datenschutz-Grundverordnung. Jedoch hat sich auch nach aktueller Rechtslage nichts an der damaligen datenschutzrechtlichen Wertung geändert. An die Stelle des § 6b Abs. 1 Nr. 3 Bundesdatenschutzgesetz ist die Vorschrift des Art. 6 Abs. 1 Buchst. f DSGVO getreten, die in gleicher Weise beim Vorliegen berechtigter Interessen noch eine Abwägungsentscheidung verlangt, welche bei privaten Waldflächen im Regelfall zugunsten der Waldnutzer (Wanderer, Pilzsucher etc.) ausfällt.

Im Ergebnis lässt sich die Begründung des Bundesgerichtshofs vom 25. April 1995, Az. VI ZR 272/9, für die Rechtswidrigkeit einer durch Private vorgenommenen Videoüberwachung im öffentlichen Verkehrsraum auf die dargestellten Fälle übertragen. Auch bei öffentlich-zugänglichen im Privateigentum befindlichen Grundstücksbereichen überwiegen grundsätzlich die schutzwürdigen Betroffeneninteressen das Überwachungsinteresse des Kamerabetreibers.

Was ist zu tun?
Grundstückseigentümer und Kamerabetreiber sollten vor Inbetriebnahme von Videotechnik zunächst prüfen, ob Dritte durch den Erfassungsbereich der vorgesehenen Videokameras betroffen sein können. Ist dies der Fall und handelt es sich um einen für Dritte zugänglichen Bereich, sollte von der Maßnahme Abstand genommen werden, soweit auch wirksame Einwilligungen sämtlicher Betroffener – wie in diesen Fällen regelmäßig – nicht einholbar sein werden.

2.2.6 Kurioses und Merkwürdiges zur Videografie

↗ Art. 6 Abs. 1 Buchst. f DSGVO

Immer wieder erlebe ich bei meinen Untersuchungen, wie wenig Gedanken sich manche Kamerabetreiber über die Grenzen der Videoüberwachung machen und dass sie das informationelle Selbstbestimmungsrecht der beobachteten Personen verletzen, wenn sie unbescholtene Mitmenschen ständig unter Beobachtung haben. Umso mehr erstaunt es mich, welche

Argumente Verantwortliche zuweilen als Rechtfertigung für den Kameraeinsatz anführen; Begründungen, die auch offensichtlich nicht als Rechtfertigung einer Verarbeitung wegen eines berechtigten Interesses gemäß Art. 6 Abs. 1 Buchst. f Datenschutz-Grundverordnung (DSGVO) taugen.

Alternative zum TV-Programm

So wandte sich in einem Fall der kommunale Ordnungsdienst einer sächsischen Stadt an meine Behörde, weil er auf Fensterbänken im dritten Stock eines Wohngebäudes mehrere Videokameras ausmachte. Der Kamerabetreiber ließ die kommunalen Bediensteten ungeniert Einblick in die Videoüberwachung nehmen und gab diesen gegenüber auch bereitwillig Auskunft hierzu. Er hatte die Kameras so positioniert, dass sie auf die ansteigende Straße vor dem Wohnhaus gerichtet waren, konnte aufgrund der Kamerawinkel jedoch auch mehrere gegenüberliegende Wohngebäude beobachten. Die kommunalen Bediensteten staunten wohl nicht schlecht, als der Kamerabetreiber die von ihm angebrachten Kameras mit Unterhaltungszwecken begründete, vor allem im Winter, wenn frischer Schnee gefallen sei und die Kraftfahrzeuge Probleme an der Straßensteigung hätten. Zwar fand aufgrund der eingesetzten veralteten Technik keine Videoaufzeichnung statt, jedoch übertrug der Wohnungsinhaber die Live-Bilder der Kameras auf sein analoges TV-Gerät, um auf diese Art quasi das Sender-Angebot um einen (zusätzlichen) Live-Kanal zu ergänzen. Es bleibt hier nur zu vermuten, dass er wohl mit dem Programmangebot der herkömmlichen TV-Sender nicht vollumfänglich zufrieden war.

Kontrolle der öffentlichen Infrastruktur

In einem anderen Fall schilderte mir eine Bürgerpolizistin ihre Schwierigkeiten, die sie mit einem privaten Grundstückseigentümer hatte. Nachdem sie den Verdacht hatte, dieser beobachte mit der am Wohnhaus in Richtung Eingangspforte zeigenden Kamera auch den öffentlichen Verkehrsraum jenseits der Grundstückseinfriedung, sprach sie den Kamerabetreiber an. Dieser gab unumwunden zu, dass

er die Kamera aktiv betreibe und führte als Gründe für die Videoüberwachung an, dass permanent Radfahrer und gemeindliche Bauhofmitarbeiter bei Räum- und Streuarbeiten, aber auch Post- und Zeitungszusteller mit ihren Fahrzeugen den vor dem Wohngrundstück verlaufenden Gehweg befahren würden. Er habe darauf auch schon ein Pferdegespann fahren sehen. Außerdem würde der Rasen vor dem Grundstück nicht regelmäßig gepflegt. Deshalb meinte er, dies müsste kontrolliert werden und sah sich offensichtlich selbst hierzu berufen. Im Zuge der weiteren Ermittlungen wurde bekannt, dass er sich sogar einmal wegen der aus seiner Sicht mangelhaften Qualität des Winterdienstes an den zuständigen Bauhofleiter wandte und zum Beleg hierfür Videoaufzeichnungen seiner Kamera vorlegte.

Im ersten Fall konnte ich den Kamerabetreiber zum kompletten Abbau der Videokameras bewegen. Der Hauseigentümer wies mir im anderen Fall nach, dass er die Kameraausrichtung auf meine Aufforderung hin so verändert hat, dass nur sein privater Grundstückseingang noch davon erfasst war. Aufgrund der Schwere der Rechtsverstöße kam ich in beiden Fällen nicht umhin, gegenüber den Kamerabetreibern jeweils eine Verwarnung auszusprechen.

2.2.7 Bereitstellung von Abrechnungsunterlagen innerhalb einer Wohnungseigentümergemeinschaft

↗ § 18 Abs. 4 WEMoG, Art. 4 Nr. 1 und 2 DSGVO, Art. 6 Abs. 1 und 3 DSGVO, Art. 32 DSGVO

Durch die mit der Bekämpfung der Corona-Pandemie einhergehenden Kontaktbeschränkungen hat die Verlagerung von Dienstleistungen ins Internet einen Aufschwung erhalten. Dies stellt nicht zuletzt die Verantwortlichen, die gerade bei der digitalen Verarbeitung personenbezogener Daten gesteigerte Maßnahmen zu treffen haben, um dem Datenschutz gerecht zu werden, vor neue Herausforderungen. Weil er sein informationelles Selbstbestimmungsrecht durch die ihn be-

treuende Wohnungsverwaltung verletzt sah, wandte sich ein Wohnungseigentümer mit einer Eingabe an meine Behörde.
Die Hausverwaltung hatte allen Miteigentümern eine E-Mail geschickt, mit der diese über die Jahresabrechnung für das Jahr 2020 informiert wurden. Die E-Mail enthielt neben einem Link zu einem Internetportal auch direkt aufrufbare PDF-Dokumente, die jeweils mit einer fortlaufenden Nummer sowie dem jeweiligen Eigentümernamen bezeichnet waren. Diese waren nach Anmeldung in einem Internetportal für jeden der über 60 Eigentümer abrufbar und gewährten einen Zugriff auf sämtliche Abrechnungsunterlagen (Einzelabrechnungen nebst Heizungs- und Wasserabrechnung) aller Wohnungseigentümer des betreffenden Wohnobjekts.
Die Wohnungsverwaltung rechtfertigte dieses Vorgehen damit, dass die genaue Ausgestaltung des jedem Eigentümer zustehenden Einsichtsrechts in die Verwalter- und damit auch die Abrechnungsunterlagen allein ihr obliege. Sie war der Ansicht, die in den Einzelabrechnungen enthaltenen personenbezogenen Daten der Eigentümer als auch der Mieter unterlägen bereits nicht der Datenschutz-Grundverordnung. Nachdem sie dem Sachverhalt unter Verweis auf die zunehmende Bereitstellung von Unterlagen bei Eigentümergemeinschaften in digitaler Form eine grundsätzliche Bedeutung für eine Vielzahl von Verwaltungsunternehmen beimaß, hat meine Behörde die Fragestellung dem zuständigen Arbeitskreis der Datenschutzaufsichtsbehörden vorgestellt, um dort eine abgestimmte Rechtsauffassung zu erreichen.

Rechtsgrundlage gesucht

Doch zunächst zur Frage der Anwendbarkeit des Datenschutzrechts innerhalb einer Wohnungseigentümergemeinschaft, im Konkreten bezüglich der Offenlegung von Abrechnungsunterlagen. Diese enthalten neben Eigentümer- und Mieternamen auch individuelle Verbrauchswerte und damit unzweifelhaft personenbezogene Daten im Sinne des Art. 4 Nr. 1 Datenschutz-Grundverordnung (DSGVO). Damit ist die Verarbeitung – hier in Form der Offenlegung (Art. 4 Nr. 2 DSGVO) – nach den Datenschutzvorschriften zu beurteilen.

Dem Hausverwalter war es offensichtlich entgangen, dass auch der Bundesgesetzgeber in der Gesetzesbegründung ausdrücklich klargestellt hat, dass bei dem gesetzlich verankerten Einsichtsrecht im ab 1. Dezember 2020 geltenden § 18 Abs. 4 Wohnungseigentumsgesetz (WEG) „freilich zwingende datenschutzrechtliche Vorgaben einzuhalten sind" (Bundestagsdrucksache 19/18791 zu § 18 Abs. 4 Wohnungseigentumsmodernisierungsgesetz – WEMoG).

Für eine zulässige Datenoffenlegung hätte es dementsprechend einer Rechtsgrundlage gemäß Art. 6 Abs. 1 DSGVO bedurft. Mangels Vorliegens einer gesetzlichen Pflicht zur Datenweitergabe schied eine auf Art. 6 Abs. 1 Buchst. c DSGVO gestützte Verarbeitung aus. Die Verarbeitung personenbezogener Daten ist danach nur dann rechtmäßig, wenn sie zur Erfüllung einer rechtlichen Verpflichtung, welcher der Verantwortliche unterliegt, erforderlich ist. Dabei muss der Verarbeitungszweck in der Rechtsgrundlage als solcher ausdrücklich festgelegt sein, Art. 6 Abs. 3 Satz 2 DSGVO.

Die Vorschrift des § 18 Abs. 4 WEG (vormals abgeleitet aus § 24 Abs. 6 Satz 3 und Abs. 7 Satz 8 WEG in Verbindung mit §§ 675, 666 Bürgerliches Gesetzbuch in Verbindung mit dem Verwaltervertrag) enthält jedoch nur einen Individualanspruch eines Wohnungseigentümers auf Einsicht in die Verwaltungsunterlagen und damit auch die Aufzeichnungen und Abrechnungsbelege sowie die Einzelabrechnungen der übrigen Wohnungseigentümer. Das Einsichtsrecht soll dem Wohnungseigentümer eine Überprüfung der Verwaltertätigkeit und im Zusammenhang mit der Jahresrechnung eine Kontrolle der Richtigkeit der – ihn betreffenden – Abrechnung ermöglichen. Hierzu bedarf es lediglich eines Antrags ohne Ermächtigung der übrigen Wohnungseigentümer, ohne eine diesbezügliche vorherige Beschlussfassung der Eigentümerversammlung sowie ohne Darlegung eines (rechtlichen) Interesses (siehe hierzu Bundestagsdrucksache 19/18791 zu § 18 Abs. 4 WEMoG). Dem steht die Verpflichtung des Hausverwalters gegenüber, mit Ausnahme der rechtsmissbräuchlichen oder schikanösen Rechtsausübung, Einsicht in die Verwalterunterlagen zu gewähren.

„Die Öffentlichkeit hat eine unstillbare Neugier, alles zu wissen, nur nicht das Wissenswerte."

Oscar Wilde

Voraussetzung für die Offenlegung der Verwaltungsunterlagen ist damit zwingend ein diesbezüglicher Antrag des Eigentümers. Eine Befugnis zur vollständigen und antragsunabhängigen Offenlegung der Abrechnungsunterlagen (hier: Jahresabrechnungen einschließlich der Einzelabrechnungen sowie Unterlagen zu Betriebskostenabrechnungen, insbes. Heiz- und Warmwasserkostenabrechnungen) als Teil der Verwaltungsunterlagen gegenüber allen Eigentümern – im Vorgriff auf individuell geltend gemachte Einsichtsrechte – lässt sich daraus jedoch nicht ableiten.

Berechtigtes Interesse kein Grund

Der Hausverwalter konnte sich auch nicht auf die berechtigten Interessen berufen, vgl. Art. 6 Abs. 1 Buchst. f DSGVO. Danach ist die Verarbeitung nur rechtmäßig, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen. Diese Voraussetzungen waren vorliegend gleichfalls nicht erfüllt.

Meine Behörde erkannte bereits kein berechtigtes Interesse aufseiten des Hausverwalters. Bei einer wohlwollenden Betrachtung könnte dieses allenfalls in einem reduzierten Zeit- und Arbeitsaufwand zur Bearbeitung individueller Einsichtsansprüche bestehen. Wollte man darin ein berechtigtes Interesse sehen, so fehlte es jedenfalls für die antragsunabhängige unaufgeforderte Bereitstellung sämtlicher Abrechnungsunterlagen aller Objekteigentümer an der Erforderlichkeit. Die pandemiebedingte (vorzugsweise) elektronische Zurverfügungstellung von Unterlagen konnte hieran auch nichts ändern. Zwar stellt der Gesetzgeber dem Verwalter die Wahl der Form frei, mit der er die Abrechnungsunterlagen gegenüber einem sich mit einem Einsichtsbegehren an ihn wendenden Wohnungseigentümer bereitstellt, also ob in herkömmlicher Weise mit der physischen Bereitstellung in den Geschäftsräumen oder aber in digitaler Form. Jedoch sollte gerade Letztere eine Zeit- sowie Kostenersparnis er-

möglichen, indem zum Beispiel mit einer entsprechenden Rechtevergabe beim Zugriff auf ein Internetportal oder in Form einer verschlüsselten Übersendung von Abrechnungsunterlagen sich diese empfängerkonkret und ohne großen Aufwand übermitteln lassen. Auch bezüglich der zusätzlichen Offenlegung von Mieterdaten, und seien es nur die Namen, konnte ich keine Erforderlichkeit erkennen.

Weitergabe nicht rechtmäßig

Letztlich ergab auch die in der zweiten Stufe vorzunehmende Abwägung, dass Eigentümer die ungefragte und anlasslose Weitergabe der gesamten abrechnungsrelevanten Daten an andere Eigentümer nicht hinnehmen müssen. Ansonsten ließe sich das Datenschutzgrundrecht der betroffenen Eigentümer – gerade im Internetzeitalter – unter Verweis auf Kostenersparnisgründe und fortschreitende technische Möglichkeiten pauschal und quasi schrankenlos aushebeln. Allein die Tatsache, dass sich nicht zuletzt durch die Erfahrungen aus der Corona-Pandemie viele Dienstleistungen ins Internet verlagert haben, impliziert jedoch kein (automatisches) Zurücktreten des Datenschutzgrundrechts der betroffenen Personen.

DSK-Arbeitskreis teilt Auffassung

Im zuständigen Arbeitskreis der Datenschutzkonferenz (DSK) bestätigte sich meine Rechtsmeinung, und es bestand Einigkeit darüber, dass die unaufgeforderte Bekanntgabe der Einzelabrechnungen innerhalb einer Wohnungseigentümergemeinschaft gegen Art. 6 DSGVO verstößt, soweit nicht eine vorherige informierte Einwilligung der betroffenen Eigentümer vorliegt. Bei Geltendmachung des individuellen Rechts auf Einsichtnahme allerdings sind – mit Ausnahme eventueller Mieterdaten – alle Einzelabrechnungen und abrechnungsrelevanten Verbrauchswerte vollumfänglich gegenüber dem Antragsteller offenzulegen.

Im Übrigen bestehen aus Sicht des Datenschutzes grundsätzlich keine Bedenken gegen die Auslagerung von Abrechnungsdaten auf ein Internetportal, soweit die Sicherheit der Verarbeitung durch technisch-organisatorische Maßnahmen sichergestellt ist (Art. 32 DSGVO). Dies lässt sich mit einem gestuften Offenlegen der Abrechnungsunterlagen ermöglichen, zum Beispiel durch Beschränkung des Zugriffs (in Abhängigkeit eines Antrags auf Einsicht) je nach Inhalt und Art der dort hinterlegten Unterlagen. Letztlich bedarf es zur Einsicht nach der Intention des Gesetzgebers aber zwingend eines ausdrücklich formulierten Begehrens des Eigentümers („Jeder Wohnungseigentümer kann [...] Einsicht in die Verwaltungsunterlagen verlangen.", siehe § 18 Abs. 4 WEG). Das Recht auf Einsichtnahme in Belege impliziert damit keine Pflicht und auch keine Befugnis des Hausverwalters zur unaufgeforderten Übermittlung der gesamten Einzelabrechnungen an alle Wohnungseigentümer. Im Gegensatz dazu wäre eine vorauseilende Offenlegung eine aufgedrängte Informationsflut, die nicht jeder Wohnungseigentümer will.

Was ist zu tun?
Die Bereitstellung von Abrechnungsunterlagen innerhalb einer Wohnungseigentümergemeinschaft kann durch den Verwalter auch digital im Wege eines Abrufs erfolgen. Dabei sind den zur Einsichtnahme berechtigten Personen nur die datenschutzrechtlich zulässigen Unterlagen bereitzustellen. Seitens des Verantwortlichen ist gemäß Art. 32 DSGVO dafür Sorge zu tragen, dass die Daten informationssicherheitsgerecht bereitgehalten werden.

2.2.8 Kernbereich privater Lebensgestaltung auch im Visumverfahren geschützt

↗ § 86 AufenthG, Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG

Ein Petent hatte sich an mich gewandt, der als Ehemann seiner noch im Ausland lebenden Frau von einer sächsischen Ausländerbehörde per E-Mail aufgefordert wurde, im Rahmen des Visumsverfahrens seiner Ehefrau zur weiteren Prüfung der Kontaktnachweise den Chatverlauf bei WhatsApp oder des Mediums, welches der Petent mit seiner Ehefrau nutzt, einzureichen, wobei dies den Schriftverkehr ebenso einschließe wie versandte Bilddateien und die gemeinsame Anrufliste. Dieser E-Mail der Ausländerbehörde war ein förmliches Schreiben der Behörde vorausgegangen, in dem der Petent aufgefordert worden war, sämtliche Kontaktnachweise mit seiner Ehefrau (E-Mails, Chatverläufe, Anruflisten und Ähnliches) vorzulegen.

Unverletzlichkeit der Intimsphäre

Meine Dienststelle bat die zuständige Behörde um Stellungnahme und wies darauf hin, dass sie die behördliche Aufforderung zur Übermittlung „sämtlicher Kontaktnachweise" und kompletter privater Chatverläufe grundsätzlich für nicht zulässig erachte. Die Aufforderung zur Vorlage lückenloser privater Chatverläufe stellt einen schweren behördlichen Eingriff in Art. 2 Abs. 1 Grundgesetz (GG) in Verbindung mit Art. 1 Abs. 1 GG dar und bedarf einer verfassungsmäßigen gesetzlichen Grundlage, aus der sich die Voraussetzungen und der Umfang der Beschränkungen klar und für den Bürger erkennbar ergeben und die damit dem rechtsstaatlichen Gebot der Normenklarheit entspricht. Eine spezielle Ermächtigungsgrundlage für eine derart tiefgreifende Erhebungsmaßnahme enthält das Aufenthaltsgesetz (AufenthG) aber nicht. § 86 Satz 1 AufenthG stellt lediglich einen Grundtatbestand der Befugnis zur Datenerhebung dar, der besonders tiefgreifende Erhebungen sensibler Daten nicht umfasst. Zudem hat die Ausländerbehörde im Rahmen der Überprüfung zu jedem Zeitpunkt die Unverletzlichkeit der Intimsphäre der Ehegatten zu beachten (Verwaltungsgerichtshof Hessen, 21.3.2000, Az.: 12 TG 2545/99). Zumindest Teile privater Chatverläufe zwischen Ehepartnern einschließlich versandter Bilddateien werden regelmäßig in den Kernbereich privater Lebensgestaltung fallen.

Die Behörde teilte mit, dass ein behördliches Anordnungsrecht zur Vorlage bestimmter Unterlagen auch aus Sicht der Ausländerbehörde nicht besteht. Dies sei auch in den behördlichen Schreiben erkennbar gewesen. Außerdem informiere die Ausländerbehörde die Betroffenen bei ihren persönlichen Vorsprachen mündlich regelmäßig darüber, dass die Auswahlentscheidung zur Vorlage geeigneter Beweismittel bei den Betroffenen selbst liegt. Soweit die Beweismittel intimen oder verfänglichen Inhaltes seien, stehe es dem Betroffenen frei, die Daten nicht zur Vorlage zu bringen. Würden keine geeigneten Nachweise erbracht, könne die Ausländerbehörde nur nach Aktenlage entscheiden. Um

zukünftig Missverständnisse zu vermeiden – insbesondere mangels persönlicher Vorsprachen des Betroffenen aufgrund der Corona-Pandemie –, schlug die Ausländerbehörde vor, ein entsprechendes Informationsblatt für die Betroffenen zu entwerfen und diesen auszuhändigen. Gleichwohl vermöge aus Sicht der Ausländerbehörde die nachprüfbare Darstellung der organisatorischen, emotionalen und geistigen Verbundenheit von Eheleuten im Verdachtsfall nicht funktionieren, ohne den Kernbereich der Intimsphäre und das Recht auf informationelle Selbstbestimmung zu berühren.

Keine Pflicht zur Offenbarung höchstpersönlicher Umstände

Meine Dienststelle hat daraufhin die Ausländerbehörde darauf hingewiesen, dass die bislang versandten behördlichen Schreiben keinen klaren Hinweis auf den Umfang einzureichender Kontaktnachweise bzw. die Freiwilligkeit der Vorlage enthielten. Unter Angabe einer Abgabefrist war im behördlichen Schreiben nämlich nur darauf hingewiesen worden, dass die Unterlagen „benötigt" würden. Auch der Hinweis, dass nicht fristgerecht geltend gemachte Umstände bei der behördlichen Entscheidungsfindung unberücksichtigt bleiben, entsprach nicht dem allgemeinen Verständnis von freiwilliger Mitwirkung.

Dem Hinweis der Ausländerbehörde, dass die anhand nachprüfbarer Umstände vorzunehmende Prüfung der organisatorischen, emotionalen und geistigen Verbundenheit von Eheleuten im Verdachtsfall nicht in Gänze möglich sein könne, ohne den Kernbereich der Intimsphäre zu berühren, habe ich deutlich widersprochen.

Der Kernbereich privater Lebensgestaltung ist absolut geschützt und nach ständiger Rechtsprechung des Bundesverfassungsgerichts jedwedem staatlichen Zugriff ausnahmslos entzogen. Selbst überwiegende Interessen der Allgemeinheit können einen Eingriff in diesen absolut geschützten Kernbereich privater Lebensgestaltung nicht rechtfertigen (BVerfG, 3.3.2004, Az.: 1 BvR 2378/98, 1 BvR 1084/99). Zur Entfaltung der Persönlichkeit im Kernbereich privater Lebens-

gestaltung gehört die Möglichkeit, innere Vorgänge wie Empfindungen und Gefühle sowie Überlegungen, Ansichten und Erlebnisse höchstpersönlicher Art zum Ausdruck zu bringen, und zwar ohne Angst, dass staatliche Stellen dies überwachen und bewerten. Vom Schutz umfasst sind auch Gefühlsäußerungen, Äußerungen des unbewussten Erlebens sowie Ausdrucksformen der Sexualität (BVerfG, 3.3.2004, Az.: 1 BvR 2378/98, 1 BvR 1084/99). Vor diesem Hintergrund hat die Ausländerbehörde bei künftigen Anforderungen von Kontaktnachweisen zur ausländerbehördlichen Prüfung von Lebensverhältnissen darauf zu achten, dass bei der betroffenen Person der Eindruck vermieden wird, Kommunikationsinhalte einschließlich versandter Bilder seien lückenlos offenzulegen (Stichwort „Chatverläufe").

Klare Hinweise an betroffene Personen

Die Erstellung des von der Ausländerbehörde avisierten Hinweisblattes habe ich ausdrücklich begrüßt und angeregt, entsprechende Hinweise zur Freiwilligkeit und zum Schutz des Kernbereichs privater Lebensgestaltung aufzunehmen. Nach inhaltlicher Abstimmung zwischen der Ausländerbehörde, dem für sie zuständigen Datenschutzbeauftragten und meiner Behörde händigt die Ausländerbehörde seit einigen Monaten betroffenen Personen das meines Erachtens gelungene Informationsblatt aus.

Was ist zu tun?
Der Kernbereich privater Lebensgestaltung ist absolut geschützt und staatlichem Zugriff ausnahmslos entzogen. Behörden dürfen keine diesem Bereich entstammenden Daten erheben.

2.2.9 Nutzung von Kontoverbindungsdaten für künftige Verfahren durch die Landesjustizkasse

↗ Art. 6 Abs. 4 DSGVO, Art. 13 Abs. 3 DSGVO

Eine Petentin berichtete, dass die Landesjustizkasse (LJK) gegen ihre kontoführende Bank einen Pfändungs- und Überweisungsbeschluss erlassen habe. Sie fragte sich, woher die LJK ihre Bankverbindung kenne.
Auf die Anfrage meiner Behörde hin teilte die LJK, eine Abteilung des Oberlandesgerichts (OLG) Dresden, mit, dass die Bankverbindung aus einem vorangegangenen Kosteneinn-

ziehungsverfahren gegen die Petentin bekannt gewesen sei. Dies habe sich aus einer von der Betroffenen mittels Überweisung veranlassten Einzahlung ergeben. Die Erhebung und Verarbeitung der Zahlungsdaten diene der Erfüllung der Aufgaben der LJK als Vollstreckungsbehörde.
Die ursprüngliche, erste Nutzung der Kontodaten betreffe das konkrete Verfahren, für das die Daten ursprünglich erhoben worden waren bzw. in dem die Daten – hier durch die von der Kostenschuldnerin veranlasste Überweisung – bekannt wurden. Die Weiternutzung in eventuellen anderen, späteren Verfahren stelle eine Zweckänderung dar, die nach Art. 6 Abs. 4 Datenschutz-Grundverordnung (DSGVO) zulässig sei.

Zulässige zweckändernde Verwendung

Diese Praxis der Weiterverarbeitung der Kontoverbindungsdaten in einem anderen Verfahren erachte ich, nachdem mein Amtsvorgänger auch noch vor Inkrafttreten der DSGVO und unter der alten Rechtslage eine solche Verarbeitung für andere Zwecke für zulässig gehalten hatte, ebenso unter heutiger Maßgabe der DSGVO für zulässig. Die zweckändernde Weiterverarbeitung steht in Einklang mit den Vorgaben des Art. 6 Abs. 4 DSGVO. Die Vorschrift beschreibt die Voraussetzungen, unter denen eine Verarbeitung personenbezogener Daten zu einem anderen Zweck als zu demjenigen, zu dem die Daten ursprünglich erhoben wurden, zulässig ist. Zur Diskussion stand dabei auch die Frage, ob nach den in Art. 6 Abs. 4 DSGVO genannten Kriterien eine Bankverbindung, die der LJK – beiläufig – im Wege der Banküberweisung durch den Kostenschuldner offengelegt worden war, später zur Durchführung von Vollstreckungsmaßnahmen (in diesem oder einem anderen Verfahren) gegen diesen Schuldner verwendet werden kann. Erwägungsgrund 50 der DSGVO führt hierzu aus, dass – neben der Kategorie der betroffenen Daten und den Folgen der Weiterverarbeitung für die betroffene Person – auch zu prüfen ist, ob unter Berücksichtigung der Beziehung der betroffenen Person zum Verantwortlichen (LJK) diese vernünftigerweise erwarten muss oder kann, dass die Daten auch in anderer Weise verwendet werden. Es liegt meines Er-

achtens im Rahmen vernünftiger Erwartungen, dass Kontoverbindungsdaten, die der LJK offengelegt werden, durch die LJK, solange die Daten rechtmäßig gespeichert werden und der LJK vorliegen, auch im Rahmen der ihr obliegenden Aufgabe der Zwangsvollstreckung genutzt werden.

Geringerer Eingriff als neue Datenerhebung bei Dritten

Im Rahmen der gebotenen Abwägung ist dabei auch zu berücksichtigen, dass es datenschutzrechtlich einen geringeren Eingriff darstellt, wenn die LJK ihr bekannte Kontoverbindungsdaten in einem künftigen Fall erneut nutzt, als wenn sie eine Abfrage hinsichtlich bestehender Bankverbindungen des Schuldners an das Bundeszentralamt für Steuern (vgl. hierzu § 802l Abs. 1 Zivilprozessordnung) richten und in diesem Zusammenhang mehr Daten des Schuldners verarbeiten und sogar noch eine dritte Stelle einbeziehen würde.
Die LJK unterliegt allerdings nach Art. 13 Abs. 3 DSGVO der Verpflichtung, die betroffene Person vor einer Weiterverarbeitung umfassend über die Zweckänderung zu informieren. Bereits vor Inkrafttreten der DSGVO hatte die LJK nach Abstimmung mit meiner Behörde seit 2013 Kostenschuldner formularmäßig gemeinsam mit der Zahlungsaufforderung darauf hingewiesen, dass die übermittelten Überweisungsdaten gespeichert und gegebenenfalls in weiteren Verfahren genutzt werden. Bedauerlicherweise fehlte dieser Hinweis im aktuellen Fall der Petentin, sodass diese nicht gemäß Art. 13 Abs. 3 DSGVO über die Weiterverarbeitung zu einem anderen Zweck informiert wurde. Das OLG teilte mit, dass der Hinweis auf eine eventuelle Nutzung der Überweisungsdaten auch in weiteren Verfahren auf Zahlungsaufforderungen gefehlt habe, die in einem Zeitraum von einigen Monaten nach dem Juni 2018 versandt wurden. Mit Bemerken des Fehlers seien die Zahlungsaufforderungen umgehend wieder um den Hinweis ergänzt worden. Hinsichtlich der Schuldner, bei denen der Hinweis formularmäßig nicht erfolgt war, forderte das OLG Dresden die LJK auf, vor einer Nutzung der übermittelten Bankdaten zu anderen Zwecken, etwa zur Vollstreckung, eine Unterrichtung nach Art. 13 Abs. 3 DSGVO vorzunehmen.

Was ist zu tun?
Die Landesjustizkasse hat Kostenschuldner darauf hinzuweisen, dass nach Überweisungen die Kontoverbindungsdaten gespeichert und gegebenenfalls auch in weiteren Verfahren genutzt werden.

2.2.10 Impfwerbung des Sozialministeriums

Ein Petent wandte sich im Berichtszeitraum an meine Behörde, da er befürchtete, dass das Sächsische Staatsministerium für Soziales und Gesellschaftlichen Zusammenhalt (SMS) für die „Impfwerbung im Erzgebirgskreis" personenbezogene Daten missbräuchlich nutze, und bat, dies zu prüfen. Er bezog sich in seiner Beschwerde auf ein Interview der „Freien Presse" vom 24. August 2021. Darin habe Staatsministerin Petra Köpping geäußert, dass nach einer Studie der Technischen Universität Dresden vor allem jüngere AfD-Wähler mit geringem Einkommen die Impfung ablehnen. Diese sollen nun gezielt angesprochen werden.

Das SMS teilt zur „Impfwerbung im Erzgebirgskreis" mit, dass das Büro für strategische Beratung Hitschfeld in Leipzig beauftragt wurde, eine speziell auf die besonders impfskeptischen Bevölkerungsgruppen im Erzgebirgskreis zielende Informationskampagne zu entwickeln. Dem Unternehmen wurden dafür keine personenbezogenen Daten zur Verfügung gestellt. Die relevanten Bevölkerungsgruppen sind bereits zuvor in einer mikrogeografischen Analyse ermittelt worden. Grundlage war die Studie „Covid-19 in Sachsen" vom Mercator Forum Migration und Demokratie (MIDEM). Auf Basis der Auftragsergebnisse hat das SMS Informationsflyer über die Deutsche Post in kompletten Zustellbezirken konkreter Kommunen des Erzgebirgskreises zustellen lassen.

Eine Nutzung personenbezogener Daten fand somit nicht statt. Auf der Internetseite von MIDEM ist die oben genannte Studie eingestellt.

Mehr Informationen:
↗ www.forum-midem.de

2.2.11 Auskunft aus archivierten Melderegisterdaten

↗ SächsArchivG

Meine Behörde erhielt eine Anfrage, ob sich die Anforderungen an eine Auskunft zu Melderegisterdaten nach deren Archivierung (nach Ablauf der Aufbewahrungsfrist) nach

Archiv- oder weiter nach Melderecht bestimmen. Während Letzteres gemäß § 44 Bundesmeldegesetz (BMG) ohne weitere Voraussetzungen eine sogenannte einfache Melderegisterauskunft ermöglicht, sind bei Ersterem bis zum Ablauf von Schutzfristen (welche gemäß § 10 Abs. 1 Archivgesetz für den Freistaat Sachsen {SächsArchivG} zwischen 10 und 100 Jahren betragen können) keine Auskünfte möglich. Diese Schutzfrist kann zwar bei Einwilligung oder gemäß § 10 Abs. 5 SächsArchivG verkürzt werden, Letzteres setzt aber berechtigte Belange voraus, die die schutzwürdigen Belange der Person, auf die sich das Archivgut bezieht, überwiegen.
Das Bundesarchivgesetz enthält in § 11 Abs. 5 BArchG eine Regelung, nach der Schutzfristen auf Archivgut des Bundes nicht anzuwenden sind, soweit es aus Unterlagen besteht, die bereits vor Übergabe an das Bundesarchiv einem Informationszugang nach einem Informationszugangsgesetz offengestanden haben. Zum einen umfasst der Wortlaut „Informationszugangsgesetz" dabei schon nicht das Bundesmeldegesetz. Zum anderen ist das BArchG für sächsische Melderegister nicht anwendbar, und das SächsArchivG enthält keine mit § 11 Abs. 5 Nr. 2 BArchG vergleichbare Regelung.
Das um Stellungnahme gebetene Sächsische Staatsministerium des Innern teilte meiner Behörde mit, dass im Ergebnis tatsächlich mit der Archivierung von Meldedaten eine zusätzliche Schwelle für Auskünfte eingebaut wird, die ursprünglich nach § 44 BMG für Registraturgut nicht vorgesehen war.

2.3 Einwilligungsfragen

2.3.1 Datenschutz im Täter-Opfer-Ausgleich

↗ § 155 Abs. 2 StPO

Zu Beginn des letzten Jahres wandte sich eine Petentin an meine Behörde mit der Beschwerde, dass ihre im Rahmen eines Täter-Opfer-Ausgleichs (TOA) getätigten Aussagen durch den Sozialen Dienst der Justiz an den Sozialpsychiatrischen Dienst des örtlich für die Petentin zuständigen Gesundheitsamtes weitergegeben wurden, obwohl die Petentin

mehrfach gegenüber der zuständigen Mitarbeiterin erwähnte, dass sie keinen Kontakt zum Sozialpsychiatrischen Dienst wünscht. Gleichwohl hatte die Petentin nach dem Gespräch im Rahmen des TOA einen Telefonanruf vom Sozialpsychiatrischen Dienst des Gesundheitsamtes erhalten, in welchem auf ihre Aussagen im Rahmen des TOA eingegangen wurde.
Meine Behörde forderte den Sozialen Dienst der Justiz, der beim Landgericht (LG) eingerichtet ist und dessen Mitarbeiter der Dienstaufsicht des Präsidenten des LG unterliegen, zur Stellungnahme auf. Dabei wies ich darauf hin, dass gemäß § 155 b Abs. 2 Satz 2 Strafprozessordnung (StPO) die zur Durchführung des TOA beauftragte Stelle – bei erwachsenen Beschuldigten der Soziale Dienst der Justiz, beauftragt durch die Staatsanwaltschaft (StA) – personenbezogene Daten nur verarbeiten darf, soweit dies für die Durchführung des TOA oder der Schadenswiedergutmachung erforderlich ist und die betroffene Person eingewilligt hat.
Die Vorschrift soll sicherstellen, dass die für die Durchführung des TOA erforderliche Verarbeitung personenbezogener Daten nicht ohne den Willen der betroffenen Personen (Verletzte ebenso wie mutmaßliche Täter) erfolgt. Die Verarbeitung personenbezogener Daten umfasst auch die Übermittlung dieser Daten an Dritte. Die Einwilligung des Betroffenen ist somit nicht nur für die Datenerhebung, sondern auch für die Datenübermittlung erforderlich. Vorliegend hatte die Petentin sich ausdrücklich gegen eine Übermittlung sie betreffender Informationen an das Gesundheitsamt gewandt. Ohne Einwilligung des Betroffenen darf die zur Durchführung des TOA beauftragte Stelle – also der Soziale Dienst der Justiz – gemäß § 155 Abs. 2 Satz 3 StPO nach Abschluss der Tätigkeit ausschließlich der StA oder dem Gericht im erforderlichen Umfang berichten. Dass nur „im erforderlichen Umfang" zu berichten ist, bedeutet, dass der Soziale Dienst selbst der StA oder dem Gericht gegenüber lediglich verfahrenserhebliche, nicht aber sämtliche Informationen offenlegen darf, die mutmaßliche Täter oder Verletzte im Rahmen des TOA preisgegeben haben.

Diese strenge Zweckbindung der Datenverarbeitung soll die Bereitschaft zum TOA fördern, weil sie den Beteiligten die Entscheidung erleichtern wird, sich der mit seiner Durchführung befassten Stelle auch hinsichtlich solcher Umstände zu offenbaren, an deren Geheimhaltung grundsätzlich ein besonderes Interesse besteht.

Der Soziale Dienst der Justiz war vorliegend auch nicht durch die StA beauftragt worden, bestimmte Angaben über die Petentin (von denen die StA nicht einmal Kenntnis hatte) an den Sozialpsychiatrischen Dienst des Gesundheitsamtes zu übermitteln. Auch § 13 Abs. 2 in Verbindung mit § 17 Nr. 3 Einführungsgesetz zum Gerichtsverfassungsgesetz (EGGVG) konnte die Übermittlung durch den Sozialen Dienst nicht rechtfertigen. Die Übermittlung personenbezogener Daten von Amts wegen für andere Zwecke als die des Verfahrens, für die die Daten erhoben worden sind, steht nur den Gerichten und der StA zu. Sollten im Rahmen des TOA Aussagen getätigt werden, in denen nach Einschätzung des Sozialen Dienstes der Justiz eine (konkrete) Gefahr für die öffentliche Sicherheit gesehen wird, kann der Soziale Dienst der Justiz aufgrund einer akuten Gefahrenlage die Polizeibehörden informieren.

Im vorliegenden Fall gab es keine Rechtsgrundlage für die Übermittlung der die Petentin betreffenden Angaben aus dem TOA an den Sozialpsychiatrischen Dienst des Gesundheitsamtes; die Übermittlung verletzte datenschutzrechtliche Vorschriften. Der Präsident des hier zuständigen LG nahm den Vorgang zum Anlass, die Mitarbeiter des Sozialen Dienstes der Justiz beim LG über die Anwendung datenschutzrechtlicher Bestimmungen für die Bearbeitung von Aufträgen für den TOA zu belehren, und bat meine Behörde um entsprechende fachkundige Beratung.

Geltung der DSGVO für TOA-Stellen

Zunächst war zu klären, ob TOA-Stellen dem Anwendungsbereich der Datenschutz-Grundverordnung (DSGVO) unterliegen. Ich vertrete die Auffassung, dass TOA-Stellen im Anwendungsbereich der DSGVO agieren. Selbst wenn man die Ansicht vertritt, dass der TOA mit seiner Verankerung in der

Strafprozessordnung im weitesten Sinne der Strafverfolgung dient und damit in den Anwendungsbereich der Richtlinie (EU) 2016/680 (JI-Richtlinie) fällt, ist das Verfahren zum TOA von vorneherein auf die freiwillige Mitwirkung der Beteiligten angewiesen und weist insoweit eine Nähe zur DSGVO auf. Eine zwangsweise Durchsetzung dieser Maßnahme, wie sie der Richtliniengeber grundsätzlich bei der Wahrnehmung der Aufgaben im Rahmen der JI-Richtlinie sieht, kommt wegen der gesetzlich vorausgesetzten Freiwilligkeit des TOA nicht in Betracht. Hinzu tritt der Umstand, dass mit der Erteilung des Auftrags zur Durchführung des TOA das Ermittlungsverfahren gemäß § 153a Abs. 1 Satz 1, Satz 2 Nr. 5 StPO vorläufig eingestellt wird, dass also während des TOA gar keine Strafverfolgung stattfindet.

Aber auch im Anwendungsbereich der DSGVO nimmt die TOA-Stelle eine gewisse Sonderstellung ein, da sie weder klar als Auftragsverarbeiter noch als Verantwortlicher im datenschutzrechtlichen Sinn betrachtet werden kann.

Voraussetzung einer Auftragsverarbeitung im Sinne von Artikel 4 Nr. 8 DSGVO ist, dass der Auftragsverarbeiter im Auftrag und auf Weisung des Auftraggebers personenbezogene Daten verarbeitet. Der Soziale Dienst der Justiz wird zwar durch die StA oder das Gericht zur Durchführung des TOA-Verfahrens beauftragt, es fehlt allerdings an einer hinreichenden Weisungsgebundenheit der TOA-Stelle. Bei einer Auftragsverarbeitung bestimmt der Auftraggeber die Art und Weise der Verarbeitung. Der Auftragsverarbeiter erhält vom Verantwortlichen eine „Marschroute", das heißt Vorgaben oder eben Weisungen, was genau er zu tun hat. Die TOA-Stelle unterliegt aber hinsichtlich der Durchführung ihrer Aufgabe gerade nicht den Weisungen der StA oder des Gerichts. Der Gesetzgeber geht mit § 155 b Abs. 2 Satz 2 StPO davon aus, dass neben den von StA und Gericht übermittelten personenbezogenen Daten noch weitere personenbezogene Informationen erst im Rahmen der Durchführung des TOA von der damit beauftragten Stelle erhoben werden. Um ihrer Aufgabe gerecht werden zu können und mutmaßlichem Täter und Geschädigtem eine Verständigung, einen

Ausgleich zu ermöglichen, wird die TOA-Stelle regelmäßig weitere (Lebens-)Umstände der Beteiligten in Erfahrung bringen müssen, die bis dahin noch nicht ermittelt worden und Gericht oder StA unbekannt sind.

Ein weiteres Merkmal der Auftragsverarbeitung ist das Recht des Verantwortlichen gegenüber dem Auftragsverarbeiter, über die Löschung der im Auftrag verarbeiteten Daten oder deren Rückgabe zu bestimmen. Dem steht im TOA schon § 155 b Abs. 4 StPO entgegen, der Vorgaben ausschließlich für die TOA-Stelle, nicht aber für StA oder Gericht enthält. Außerdem kann der Betroffene seine Einwilligung nach § 155 b Abs. 2 Satz 2 StPO beschränken, sodass die Berichtspflicht der TOA-Stelle (selbst gegenüber StA oder Gericht) begrenzt wird. Die TOA-Stelle handelt somit zumindest zum Teil in eigener gesetzlicher Verantwortung.

Als eigener Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO handelt die TOA-Stelle aber auch nicht; sie entscheidet nicht allein über Mittel und Zwecke der Datenverarbeitung, sondern erhält den Auftrag, eine bestimmte Aufgabe gemäß den gesetzlichen Vorgaben zu erfüllen. Der TOA obliegt dem Sozialen Dienst der Justiz, der in die Verwaltungsstruktur am jeweiligen Landgericht eingegliedert und insoweit eine zwar eigenverantwortlich handelnde, aber unselbstständige Stelle des Landgerichts ist.

TOA-Stelle holt Einwilligung des Betroffenen ein

Demzufolge stellte sich die Frage, wer die Einwilligung des Betroffenen nach § 155 b Abs. 2 Satz 2 StPO einzuholen hat – die mit dem TOA beauftragte Stelle (die TOA-Stelle beim Sozialen Dienst der Justiz), das Landgericht, bei dem der Soziale Dienst eingerichtet ist, oder die beauftragende Stelle (StA oder Gericht)?

Tatsächlich ist die Einwilligung von der TOA-Stelle einzuholen. Gemäß der Verwaltungsvorschrift Täter-Opfer-Ausgleich (VwV TOA) nimmt die Vermittlungsstelle nach Beauftragung durch StA oder Gericht unverzüglich Kontakt mit den Beteiligten auf und klärt deren Bereitschaft zur Durchführung des TOA. Damit wird bereits die Prüfung der Eignung des

Vorgangs für einen TOA nach § 155 a StPO (der entgegenstehende Wille des Verletzten steht einer Eignung entgegen) in die Verantwortung der TOA-Stelle gelegt. Das ist rechtlich nicht zu beanstanden, weil das Gesetz nicht regelt, wie die Prüfung der Eignung zu erfolgen hat. Wenn aber die TOA-Stelle bereits die Eignung der Sache zum TOA mit den Beteiligten erörtert, so ist sie aufgrund dieser Sachnähe auch zum Einholen der erforderlichen Einwilligung nach § 155 b Abs. 2 Satz 2 StPO zuständig. Zudem fordert Art. 4 Nr. 11 DSGVO, dass die Einwilligung in informierter Weise zu erfolgen hat, das heißt, der Betroffene muss umfassend und verständig über die Datenverarbeitung aufgeklärt werden, sodass die Einwilligung hinreichend konkret – beziehungsweise entsprechend beschränkt – abgefasst werden kann. Da aber weder StA noch Gericht Einblick in die Durchführung des TOA haben, sondern ausschließlich die TOA-Stelle, kann auch nur dort eine „informierte" und damit rechtlich wirksame Einwilligung eingeholt werden. Auch im Hinblick auf die Auswirkung der Einwilligung ergibt nur diese Lösung Sinn. Denn die Einwilligung der betroffenen Person bestimmt den Umfang der Verarbeitung ihrer Daten im TOA und – im Wege der Übermittlung – über den TOA hinaus. Im TOA verarbeitete Daten liegen aber ausschließlich der TOA-Stelle vor, sodass auch nur diese in der Lage ist, die Einwilligung umzusetzen und die Verarbeitung dementsprechend zu beschränken.

Was ist zu tun?
Die für den TOA zuständige Stelle wird im Anwendungsbereich der DSGVO tätig. Sie hat die Einwilligung der Beteiligten in die Verarbeitung ihrer Daten einzuholen. Ohne Einwilligung des Betroffenen darf die beauftragte TOA-Stelle nach Abschluss der Tätigkeit ausschließlich und nur in erforderlichem Umfang der StA oder dem Gericht berichten.

2.3.2 Internetveröffentlichung von Wettkampfergebnissen im Jugendgolfsport

↗ Art.5 Abs. 2 DSGVO, Art. 6 Abs. 1 DSGVO, Art. 14 DSGVO, Art 17 DSGVO

Ein golfsportbegeisterter Bürger hatte es sich zur Aufgabe gemacht, sämtliche Wettkampf- und Turnierergebnisse aus dem Jugendgolfsport zu sammeln und diese in einem Internetauftritt gebündelt zu präsentieren. Dort legte er auch für jeden Jugendspieler ein Spielerporträt an und ordnete jedem einen individuellen Rangwert zu. Den Eltern sowie anderen Golfinteressierten bot er nach Anmeldung in einem geschützten Bereich neben erweiterten Auswertungsmöglich-

keiten auch die Möglichkeit, das Spielerporträt mit einem Bild des jugendlichen Golfspielers zu ergänzen.

Geltendmachung eines Löschanspruchs personenbezogener Veröffentlichungen

Nachdem ein Vater offensichtlich mit dem vom Seitenbetreiber ermittelten Rangwert für seine beiden minderjährigen Söhne nicht (mehr) einverstanden war, versuchte er zunächst diesem gegenüber unter Verweis auf Art. 17 Datenschutz-Grundverordnung (DSGVO) die Löschung aller seine Kinder betreffenden Daten zu erreichen, was der Verantwortliche mit Bezugnahme auf die Öffentlichkeit der ausgetragenen Turniere und Wettkämpfe ablehnte. Als letztes Mittel wandte sich der Elternsorgeberechtigte deshalb an meine Behörde und bat mich um Hilfe zur Durchsetzung gegenüber dem Seitenbetreiber.

Erforderlichkeit einer Einwilligung

Zwar werden sportliche Wettkämpfe im Regelfall öffentlich ausgetragen, sodass ein Turnierausrichter oder Veranstalter auch berechtigt ist, die Ergebnisse auf seiner Internetpräsenz darzustellen. Denn Sportwettkämpfe werden grundsätzlich auf der Grundlage sportartbezogener Wettkampfbestimmungen durchgeführt. Für deren Teilnahme ist regelmäßig eine vorherige Registrierung des jeweiligen Sportlers im Lizenzregister des Sportverbandes notwendig, und mit der Wettkampfteilnahme geben die Eltern auch ihr Einverständnis zur Verarbeitung der Daten ihrer Kinder. Vorliegend konnte der Seitenbetreiber jedoch keine Einwilligung der Erziehungsberechtigten vorweisen. Vielmehr bezog er die Spieldaten und damit auch Informationen über die teilnehmenden jugendlichen Sportler sowohl aus öffentlich verfügbaren Ergebnislisten als auch aus von den Turnierveranstaltern an ihn übersendeten Turnierdaten. Somit konnte er einzig auf die berechtigten Interessen des Art. 6 Abs. 1 Buchst. f DSGVO verweisen. Danach ist die Verarbeitung nur rechtmäßig, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich

ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere wenn es sich dabei um Kinder handelt.

Hobby als berechtigtes Interesse?

Mir gegenüber begründete der Verantwortliche sein Tun mit einem „hobbymäßigen Projekt" und machte dabei auf die Möglichkeit des Leistungsvergleichs der einzelnen Spieler aufmerksam. Damit unterscheidet sich sein Interesse jedoch von dem eines reinen Turnierveranstalters/-ausrichters, der mit der Ergebnisdarstellung auf sich und seine Veranstaltung aufmerksam machen und für das Interesse am Golfsport werben möchte. Hinzu kommt, dass sich bei den Veranstaltern bzw. Ausrichtern kein die jeweilige Spielstärke ausdrückender Rang- oder Punktwert findet. Ausgehend davon sah meine Behörde auch keinerlei Erforderlichkeit oder Notwendigkeit, in Ergänzung zu den im Internet abrufbaren Ergebnissen der ausrichtenden Vereine und Sportverbände den interessierten Seitenbesuchern auch noch ein Spielerporträt mit individuellem Rangwert anzubieten. Zudem setzte der Verantwortliche damit seine zusammengetragenen Informationen in neue Bezüge.

Der besondere Schutz von Kindern

Noch deutlicher wird die Unzulässigkeit der Datenverarbeitung bei der Abwägung der wechselseitigen Interessen. Aus der textlichen Formulierung wird bereits deutlich, dass der Schutz von Kindern einen hohen Stellenwert hat. Der Verordnungsgeber hat diesen besonderen Schutz in den Erwägungsgründen außerdem zusätzlich herausgehoben (Erwägungsgrund 38 zur DSGVO). Dem steht allein das hobbymäßige Interesse des Seitenbetreibers gegenüber. Bei einer Internetveröffentlichung kommt im Besonderen zum Tragen, dass die dargestellten persönlichen Daten der Kinder und Jugendspieler für jedermann öffentlich zugänglich sind und über das Internet eine praktisch grenzenlose Verbreitung finden können. Besonders problematisch war in dem dargestellten Fall speziell der individuelle Rangwert, der nach Dar-

stellung des Verantwortlichen die Spielstärke des jeweiligen Spielers ausdrücken und damit letztlich eine Vergleichbarkeit und Rangfolgenbildung ermöglichen sollte. Nimmt man nur die unterschiedlichen Platz- oder auch Witterungsverhältnisse, so bezweifle ich, dass sich überhaupt ein objektiver und das Leistungsvermögen ausdrückender Vergleichswert ermitteln lässt, zumal nicht jeder Jugendspieler auch an allen Veranstaltungen und Turnieren teilgenommen hatte und die dargestellten Ergebnislisten teilweise lückenhaft waren. Letztlich blieb auch der Modus zur Ermittlung des Punktwerts völlig intransparent. Die Seiten-FAQ enthielten hierzu nur ganz allgemeine Angaben zu den einfließenden Kriterien.

Resümee

Für eine datenschutzkonforme Darstellung der Wettkampfergebnisse von Kindern und Jugendspielern im Golfsport hätte der verantwortliche Seitenbetreiber eine Einwilligung der Erziehungsberechtigten (Art. 6 Abs. 1 Buchst. a in Verbindung mit Art. 7 und Art. 4 Nr. 11 DSGVO) vorweisen müssen, ebenso wie für die Spielerporträts (Vorname, Zuname, Lichtbild, Altersgruppe, Rangwert). Nachdem meine Behörde dies aufzeigte und ihm offensichtlich keine Einwilligungen vorlagen, nahm er die Internetseite vom Netz und wies meiner Behörde außerdem die Löschung aller spielerbezogenen persönlichen Daten der Kinder und Jugendlichen nach. Tatsächlich hatte der Verantwortliche die betroffenen Personen noch nicht einmal über deren Aufnahme in sein Internetangebot unterrichtet (Art. 14 DSGVO).

Im Übrigen ist ein Verantwortlicher in jedem Fall nachweispflichtig, dass die von ihm verarbeiteten personenbezogenen Daten in rechtmäßiger Weise verarbeitet werden (Rechenschaftspflicht, Art. 5 Abs. 2 DSGVO). Bei einer auf eine Einwilligung gestützten Verarbeitung bedingt dies, dass diese dem Verantwortlichen jeweils (schriftlich) vorliegt und sich deren Inhalt darüber hinaus an den datenschutzrechtlichen Vorgaben orientiert.

Was ist zu tun?

Auch hobbymäßig betriebene Internetpräsenzen fallen, soweit sie nicht ausschließlich persönlich oder familiär sind – vgl. Art. 2 Abs. 2 Buchst. c DSGVO – unter den Anwendungsbereich der DSGVO. Das gilt auch dann, wenn Informationen zum Teil aus allgemein zugänglichen Quellen zusammengetragen worden sind. Sind dritte Personen und Minderjährige betroffen, sind Einwilligungen erforderlich, insbesondere auch, wenn Abbildungen verbreitet werden sollen.

2.4 Sensible Daten, besondere Kategorien personenbezogener Daten

2.4.1 Corona in der Schule

↗ Art. 6 DSGVO, SächsCoronaSchutzVO, SchulKitaCoVO

Meine Behörde erhielt zahlreiche Eingaben im Zusammenhang mit der Regelung in der Sächsischen Corona-Schutz-Verordnung (SächsCoronaSchVO) bzw. in der späteren schulspezifischen Schul- und Kita-Coronaverordnung (SchulKitaCoVO) des Freistaates Sachsen, wonach der Zutritt zur Schule nur mit Testung zulässig ist. Die Beschwerden betrafen die Testung im Klassenverband und die daraus resultierende Möglichkeit der gegenseitigen Kenntnisnahme der Testergebnisse. Im Ergebnis hatte meine Behörde jedoch keine Bedenken gegen die Durchführung dieser Tests.

Bei einem positiven Testergebnis hat sich die positiv getestete Person unverzüglich abzusondern; minderjährige Schülerinnen und Schüler sind vom restlichen Klassenverband zu trennen und von den Personensorgeberechtigten abzuholen. Dies ist zwingend erforderlich und die damit zwangsläufig verbundene Verarbeitung personenbezogener Daten dementsprechend rechtmäßig. Keinen Unterschied macht es in diesem Zusammenhang daher, ob ein positives Testergebnis bereits beim Test im Klassenverband festgestellt wird.

Beschluss OVG Bautzen:
↗ sdb.de/tb2106

Mit Beschluss vom 9. April 2021 (Az.: 3 B 114/21) hat das Sächsische Oberverwaltungsgericht (OVG) zu damit in Zusammenhang stehenden datenschutzrechtlichen Fragen und der Vereinbarkeit der Testregelung mit der DSGVO Stellung genommen. Das OVG geht in diesem Beschluss unter Zugrundelegung von Art. 6 und 9 DSGVO bei der streitgegenständlichen Regelung in der SächsCoronaSchVO von einer ausreichenden gesetzlichen Ermächtigungsgrundlage nach Art. 6 Abs. 1 Satz 1 Buchst. c und e DSGVO aus. Auch stünde Art. 9 Abs. 1 DSGVO der Erhebung von personenbezogenen Daten nicht entgegen. Nach Art. 9 Abs. 2 Buchst. h DSGVO gelte Absatz 1 der Vorschrift unter anderem dann nicht,

wenn die Verarbeitung für Zwecke der Gesundheitsvorsorge – wie hier – erforderlich sei.

Die SächsCoronaSchVO (bzw. später SchulKitaCoVO) sah weiterhin die Pflicht zum Tragen eines medizinischen Mund-Nasen-Schutzes (OP-Maske), einer FFP2-Maske oder einer vergleichbaren Atemschutzmaske vor. Von dieser Pflicht konnte man durch eine ärztliche Bescheinigung befreit werden. Auch hierzu erreichten meine Behörde zahlreiche Petitionen. Dabei war die oft zu beobachtende Praxis, dass Schulleiter nur Atteste akzeptierten, die die zu erwartenden Beeinträchtigungen benennen und erkennen lassen, auf welcher Grundlage der Arzt zu dieser Einschätzung gelangt ist, zunächst nicht von der Verordnungslage gedeckt. Diese wurde schließlich „der Praxis angepasst" und enthielt diese inhaltlichen Anforderungen an die Atteste. Nachdem dabei bestimmt wurde, dass jeder, der Einsicht in diese Atteste erhält, Stillschweigen über die darin enthaltenen Gesundheitsdaten zu wahren hat, hatte ich keine durchgreifenden Bedenken.

Weitere Petitionen gab es auch zur Dokumentation dieser Atteste. Die SächsCoronaSchVO ließ zunächst eine Glaubhaftmachung durch Gewährung der Einsichtnahme ausreichen. Die gleichwohl oft vorgenommene Kopie war daher allenfalls mit Einwilligung zulässig. Auch hier wurde schließlich eine Befugnis in die SchulKitaCoVO aufgenommen, von dem ärztlichen Attest zur Befreiung eine analoge oder digitale Kopie zu fertigen und diese aufzubewahren. Dies ist vor unbefugtem Zugriff zu sichern und nach Ablauf des Zeitraumes, für welchen das Attest gilt, unverzüglich zu löschen oder zu vernichten, spätestens jedoch mit Ablauf des Jahres 2022.

Schließlich wurde mit der Ermöglichung einer Coronaschutzimpfung für Jugendliche ab 12 Jahren diese als Ausnahme von der Testpflicht in die SchulKitaCoVO aufgenommen. Auch hier war zunächst, trotz der Erfahrungen mit den Attesten zur Maskenbefreiung, lediglich eine Einsichtnahme in den Genesenen- oder Impfnachweis geregelt; eine entsprechende Dokumentation jedoch nicht. Dies hätte zur Folge gehabt, dass ohne entsprechende Einwilligungen diese Nachweise bei jeder Testung erneut hätten vorgelegt wer-

den müssen. Mein Amtsvorgänger regte daher gegenüber dem Verordnungsgeber nachdrücklich an, auch hier eine entsprechende Regelung zu treffen. Dem wurde schließlich auch entsprochen. Schulen können nunmehr erfassen und dokumentieren, an welchem Tag die Einsichtnahme in den Impf- oder Genesenennachweis gewährt wurde.

2.4.2 Biometrische Zutrittskontrolle in Freizeiteinrichtungen

↗ Art. 6 Abs. 1 Buchst. b und f DSGVO, Art. 9 Abs. 1 und Abs. 2 Buchst. f DSGVO, Art. 22 DSGVO

Eine große Freizeiteinrichtung hatte zur Beschleunigung ihrer Einlasskontrolle verpflichtend ein auf Gesichtserkennung basierendes biometrisches Zutrittskontrollsystem eingeführt. Die Dauerkunden hatten ein entsprechendes Informationsschreiben erhalten, in denen ihnen die alternativlose Umstellung des Zutrittskontrollsystems mitgeteilt worden war. Bei ihrem nächsten Besuch in der Einrichtung würde am Drehkreuz eine digitale Aufnahme von ihnen erstellt und anschließend gespeichert (tatsächlich nur als nicht rückrechenbares Template). Bei jedem weiteren Besuch würde fortan dann eine erneute Aufnahme angefertigt und mit der Erstaufnahme verglichen. Soweit sich Kunden diesbezüglich beim Betreiber der Freizeiteinrichtung beschwert hatten, wurde die Rechtmäßigkeit der damit verbundenen Verarbeitung personenbezogener Daten mit Art. 6 Abs. 1 Buchst. b und f Datenschutz-Grundverordnung (DSGVO) einerseits sowie Art. 9 Abs. 2 Buchst. f DSGVO andererseits begründet.

Prüfung des Sachverhalts

Der Verantwortliche hat die Verarbeitung personenbezogener Daten seiner Dauerkunden zutreffenderweise zunächst auf Art. 6 Abs. 1 Buchst. b DSGVO (Erfüllung eines mit der betroffenen Person geschlossenen Vertrags) gestützt und auch richtig erkannt, dass er – wegen der Verarbeitung biometrischer Daten – darüber hinaus auch noch eine Rechtsgrundlage aus Art. 9 DSGVO benötigt. Seine Einschätzung,

sich insoweit auf Art. 9 Abs. 2 Buchst. f DSGVO berufen zu können, war jedoch falsch.

Nach dieser Vorschrift wäre die Verarbeitung biometrischer Daten zulässig, wenn sie zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder bei Handlungen der Gerichte im Rahmen ihrer justiziellen Tätigkeit erforderlich ist. Diese Voraussetzungen waren vorliegend aber nicht erfüllt; die Begründung des Verantwortlichen, mit dem biometrischen Zutrittskontrollsystem die zuvor immer wieder festgestellten Betrugsversuche mit den Dauerkarten (Nutzung durch Dritte trotz Ausschlusses der Übertragbarkeit) wirkungsvoll ausschließen und mittels einer solchen Identitätsprüfung seine vertraglichen Ansprüche schon im Vorfeld eines eventuellen Rechtsstreits wahren zu können, war zwar nachvollziehbar, aber eben nicht von Art. 9 Abs. 2 Buchst. f DSGVO gedeckt.

Ein rechtlicher Konflikt, der Art. 9 Abs. 2 Buchst. f DSGVO zur Anwendung kommen lassen könnte, besteht weder bereits bei Vertragsabschluss noch bei ungestörter Vertragsbeziehung. Erst dann, wenn es Unregelmäßigkeiten bei der Vertragserfüllung gibt, etwa wenn einer der Vertragspartner seinen diesbezüglichen Verpflichtungen nicht nachkommt, insbesondere auch bei Missbrauchsverdacht, und daraus ein Rechtsstreit entsteht, in dem der Verantwortliche seine Ansprüche geltend machen oder verteidigen muss, greift diese Vorschrift. Dies ergibt sich sowohl aus dem Wortlaut der Vorschrift selbst, aus dem Erwägungsgrund 52 (letzter Satz), als auch aus der diesbezüglichen Kommentarliteratur.

Die in Art. 9 Abs. 2 Buchst. f DSGVO bezeichneten Rechtsansprüche können sich zwar aus vertraglichen Regelungen, beispielsweise aus schädigenden, zu Schadenersatzansprüchen führenden Handlungen ergeben, aber das Bestehen einer solchen Rechtsbeziehung allein genügt nicht, um eine Verarbeitung biometrischer Daten rechtfertigen zu können. Vielmehr muss sich hieraus erst ein Konflikt ergeben haben, der den Anspruchsinhaber dazu zwingt, zur Durchsetzung des Anspruchs prozedural tätig zu werden (Kühling/Buchner/Weichert, 3. Aufl. 2020, DS-GVO Art. 9 Rdnr. 84). Erst dann

kann Art. 9 Abs. 2 Buchst. f DSGVO herangezogen werden, um zuvor auf anderer rechtlicher Grundlage, zum Beispiel auf Basis einer Einwilligung, verarbeitete Daten nach Art. 9 Abs. 1 DSGVO auch zur Durchsetzung dieser Rechtsansprüche zu verwenden.

Art. 9 Abs. 2 Buchst. f DSGVO deckt also die Verwendung besonderer Kategorien bei der Durchsetzung derartiger Rechtsansprüche, das heißt im Rahmen des jeweiligen Streitverfahrens, ab, schafft jedoch keine Rechtsgrundlage für deren Verarbeitung in der zugrunde liegenden Rechts- bzw. Vertragsbeziehung. Denn dann wäre auf diese Weise eine Verarbeitung in jedweder Vertragsbeziehung begründbar – Störungen und missbräuchliche Handlungen kann es schließlich in jedem Vertrag geben. Hätte der Verordnungsgeber dies tatsächlich beabsichtigt, hätte er einen Art. 6 Abs. 1 Buchst. b DSGVO vergleichbaren Erlaubnistatbestand in Art. 9 DSGVO aufnehmen können. Die Datenschutz-Grundverordnung differenziert stattdessen begrifflich, aber klar zwischen der Abwicklung eines Vertragsverhältnisses (Art. 6 Abs. 1 Buchst. b DSGVO) und der Durchsetzung von Ansprüchen (Art. 9 Abs. 2 Buchst. f DSGVO). Den Ausnahmetatbestand des Art. 9 Abs. 2 Buchst. f DSGVO bei der Verarbeitung von sensiblen Daten zur Erfüllung von Vertragsbeziehungen heranzuziehen ist daher so nicht vertretbar. Die Erfassung der außergerichtlichen Streitbeilegung in Erwägungsgrund 52 Satz 3 bestärkt in Anbetracht der dortigen Formulierung das Erfordernis eines rechtlichen Konflikts. Sollen sensible Daten Vertragsgegenstand werden, bedarf es also eines eigenständigen Ausnahmetatbestands, beispielsweise einer Einwilligung gemäß Art. 9 Abs. 2 Buchst. a DSGVO.

Gesichtserkennung nur nach Einwilligung

Aus alledem ergibt sich, dass das dargestellte Anwendungsszenario, konkret der Einsatz eines biometrischen Verfahrens zur Vertragserfüllung (hier: Zutrittsgewährung), nicht auf Art. 9 Abs. 2 Buchst. f DSGVO gestützt werden kann. Im Ergebnis ist damit die Lösung des Verarbeitungsproblems auch bereits aufgezeigt. Die Absicherung des Zutritts für Dauer-

kunden mittels Gesichtserkennung ist (nur) möglich, wenn hierfür die Einwilligung der betroffenen Personen eingeholt und sich damit auf Art. 9 Abs. 2 Buchst. a DSGVO gestützt wird.

Damit eine solche Einwilligung auch tatsächlich freiwillig erfolgen kann, bedarf es einer ausführlichen Information durch den Verantwortlichen einerseits sowie auch einer ohne die Verarbeitung biometrischer Daten auskommenden Alternative für die Zutrittskontrolle andererseits. Zudem steht der Verantwortliche in Bezug auf die Erteilung der Einwilligung in der Nachweispflicht (Art. 7 Abs. 1 DSGVO).

Den insoweit unmaßgeblichen Einwand einer schwierigen Umsetzung der Einwilligungslösung teile ich ebenso wenig wie den Vorhalt, dass der organisatorische Aufwand im Fall der Nichterteilung der Einwilligung oder im Fall eines Widerrufs technisch, personell und finanziell nicht darstellbar sei. Ohnehin müssen für den Fall eines Systemausfalls der biometrischen Zutrittskontrolle Alternativlösungen geplant und vorgehalten werden. Im Fall eines Widerrufs der Einwilligung sollte die Sperrung des betroffenen Kunden in der Referenzdatenbank beziehungsweise die Entfernung des ihm zugeordneten Templates mit wenigen Klicks möglich sein.

Der Vollständigkeit halber ist zudem auch noch auf Art. 22 DSGVO – Automatisierte Entscheidungen im Einzelfall (hier: Zutrittsgewährung) – hinzuweisen. Derartige Entscheidungen dürfen nach Art. 22 Abs. 4 DSGVO nicht auf besonderen Kategorien personenbezogener Daten nach Art. 9 Abs. 1 DSGVO beruhen, es sei denn, es liegt eine diesbezügliche Einwilligung der betroffenen Person vor oder aber es kann ein erhebliches öffentliches Interesse geltend gemacht werden. Art. 9 Abs. 2 Buchst. f DSGVO ist bei den diesbezüglichen Ausnahmen jedenfalls nicht erwähnt.

Was ist zu tun?

Der Einsatz eines biometrischen Verfahrens zur Gesichtserkennung zur Vertragserfüllung und reibungsloseren Zutrittsgewährung zu einer Einrichtung kann nicht auf Art. 9 Abs. 2 Buchst. f DSGVO gestützt werden. Der Verantwortliche hat eine explizite Einwilligung der jeweils betroffenen Personen einzuholen.

2.4.3 Einschaltung eines externen Sachverständigen durch eine Sozialleistungsbehörde

↗ SGB X

Die Übermittlung von Unterlagen des Antragstellers an eine Einrichtung, die als Sachverständiger gemäß § 21 Zehntes Buch Sozialgesetzbuch (SGB X) seitens der zuständigen Behörde tätig wird, ist datenschutzrechtlich zulässig.

Die Beauftragung eines externen Sachverständigen, hier zur Erstellung einer versorgungärztlichen, Stellungnahme zu einem bei der Behörde anhängigen Antragsverfahrens, seitens der zuständigen Behörde ist dabei nicht von einer vorab hierzu einzuholenden Einwilligung des Antragstellers abhängig, sondern fällt in das Entschließungsermessen der Behörde. Gleiches gilt, soweit das Verwaltungsverfahren gerichtsanhängig ist.

Auch die Auswahlentscheidung, also welchen externen Gutachter die Behörde als Sachverständigen zur Entscheidungsfindung über den Antrag konkret auswählt, obliegt keinem Einwilligungserfordernis des Antragstellers, sondern fällt in das Auswahlermessen der Behörde.

Für eine aussagefähige versorgungsärztliche Stellungnahme erachte ich es dabei auch für zulässig, dass dem externen Gutachter die der Behörde zur Begutachtung beigezogenen Unterlagen zur Einsicht vorgelegt, mithin übermittelt werden, da andernfalls die Erstellung eines – zumal gerichtsfesten – Gutachtens nicht möglich ist. Der Sachverständige als Helfer und Berater der Behörde hat die Aufgabe, einen von der Behörde festzustellenden und zu würdigenden Sachverhalt zu prüfen. Der Sachverständige muss unparteiisch sein, es dürfen weder Ausschluss- noch Befangenheitsgründe vorliegen. Er muss zudem über besondere Sachkunde verfügen. Die im Verwaltungsverfahren eingeholten Gutachten sind auch im sozialgerichtlichen Verfahren zu verwerten, da es sich nicht um Privatgutachten handelt (so insgesamt Vogelgesang in: Hauck/Noftz Kommentar zum SGB X § 21 Rdnr. 18).

2.4.4 Masernschutzgesetz: Auffälligkeiten bei Attesten

↗ DSGVO, IfSG, StGB

Den mir vorliegenden Anfragen bzw. Beschwerden zum Masernschutz ist zu entnehmen, dass der Leitung von Kindertagesstätten oder anderen Gemeinschaftseinrichtungen vermehrt sogenannte Impfunfähigkeitsbescheinigungen zum Nachweis des ausreichenden Impfschutzes gegen Masern vorgelegt werden.

Im Tätigkeitsbericht 2020 (2.2.9, Seite 589) hatte sich mein Amtsvorgänger bereits zum Masernschutzgesetz geäußert. Damals gab es mehrere Fälle, in denen Eltern gerügt hatten, dass durch die Leitung der Kindertagesstätten Nachweise des ausreichenden Impfschutzes kopiert wurden, um einen Beleg zu den Akten zu nehmen. Dies war – wie dargelegt – unzulässig.

Das Infektionsschutzgesetz (IfSG) regelt die Impfpflicht gegen Masern. Besucht ein Kind eine Gemeinschaftseinrichtung im Sinne des § 33 Nr. 1 bis 3 IfSG, zum Beispiel eine Kindertagesstätte oder Schule, so ist nach § 20 Abs. 9 IfSG der Leitung der Einrichtung der Nachweis vorzulegen, dass ein ausreichender Impfschutz gegen Masern besteht. Dieser Nachweis kann durch eine Impfdokumentation (Impfausweis oder ärztliches Zeugnis), ein ärztliches Zeugnis über eine Immunität gegen Masern oder über das Vorliegen einer medizinischen Kontraindikation oder die Bestätigung einer staatlichen Stelle oder der Leitung einer anderen Einrichtung darüber, dass der Nachweis bereits vorgelegen hat, geführt werden.

Nach meiner Auffassung dürfen der Impfausweis oder auch ein ärztliches Zeugnis/Attest aus datenschutzrechtlichen Gründen nicht kopiert werden, da diese andere als die gesetzlich geforderten Daten enthalten – Grundsatz der Datenminimierung. § 20 Abs. 9 IfSG fordert lediglich die Vorlage des Nachweises. Deshalb ist, wie im oben genannten Tätigkeitsbericht dargelegt, ein Kopieren der Nachweise nicht zulässig.

Bei der „Impfunfähigkeitsbescheinigung" handelt sich um ein ärztliches Attest, mit dem bescheinigt wird, dass in Be-

zug auf das betroffene Kind aufgrund einer medizinischen Kontraindikation ein dauerhaftes „Impfverbot" jeglicher Art besteht. Eine Impfunfähigkeitsbescheinigung kann ein Anhaltspunkt für ein Gefälligkeitsattest sein.

Das Sächsische Staatsministerium für Soziales und Gesellschaftlichen Zusammenhalt (SMS) hat mit Schreiben vom 7. September 2021 die fachaufsichtliche Weisung (Erlass) zur Umsetzung des Masernschutzgesetzes für die Landesdirektion Sachsen und die Gesundheitsämter des Freistaates Sachsen erlassen. In der Anlage zu diesem Erlass wird ausgeführt, dass das Zeugnis nicht anerkannt werden muss, wenn sich für die Leitung der Einrichtung Anhaltspunkte ergeben, dass es sich um ein Gefälligkeitsattest handeln könnte oder sonstige berechtigte Zweifel an der Richtigkeit des Zeugnisses bestehen. Dies kann zum Beispiel bei pauschaler Verneinung jeglicher Impftauglichkeit unter Verweis auf eine nicht näher benannte Kontraindikation vorliegen.

Mehr Informationen:
↗ www.masernschutz.de

Auf der gemeinsamen Internetseite des Bundesministeriums für Gesundheit mit anderen öffentlichen Institutionen wird unter dem Stichwort „Leitungen von Einrichtungen, Ärzteschaft einschließlich Öffentlicher Gesundheitsdienst" zu der Frage „Wie kann verhindert werden, dass unrichtige Impfdokumente/Nachweise verwendet werden?" Folgendes ausgeführt:

> „Dokumente in einer anderen Sprache, offensichtlich gefälschte Dokumente oder offensichtliche Gefälligkeitsatteste müssen nicht anerkannt werden. In diesen Fällen ist das Gesundheitsamt zu benachrichtigen. Das Ausstellen und der Gebrauch unrichtiger Gesundheitszeugnisse zur Vorlage bei einer Behörde ist nach §§ 278 und 279 des Strafgesetzbuches (StGB) strafbar. Darunter fallen auch Impfdokumentationen. Den ausstellenden Ärzten drohen auch berufsrechtliche Konsequenzen."
>
> (www.masernschutz.de/leitungen-und-aerzteschaft.html)

In diesen Fällen liegt nach meiner Auffassung § 20 Abs. 9 Satz 4 IfSG vor, da der Nachweis nicht erbracht wurde. Das Gesundheitsamt ist darüber zu benachrichtigen und personenbezogene Angaben zu übermitteln.

Was ist zu tun?
Bestehen Zweifel an der Echtheit oder inhaltlichen Richtigkeit des vorgelegten Nachweises des ausreichenden Impfschutzes gegen Masern, hat die Leitung der Einrichtung nach § 20 Abs. 9 Satz 2 IfSG unverzüglich das zuständige Gesundheitsamt darüber zu benachrichtigen. In diesem Fall sind auch personenbezogene Daten zu übermitteln.

Der Gesetzgeber hat zwischenzeitlich auf die Gefälligkeitsatteste reagiert und bei der Änderung des IfSG durch das Gesetz vom 10. Dezember 2021 § 20 Abs. 9 bis 12 neu gefasst und einen Abs. 9a eingefügt. Es wird geregelt, wie bei Zweifeln an der Echtheit oder inhaltlichen Richtigkeit der Nachweise zu verfahren ist. Nach § 20 Abs. 12 IfSG hat das Gesundheitsamt zum Beispiel die Möglichkeit, Personen, die in Gemeinschaftseinrichtungen betreut werden, aufzufordern, einen Nachweis nach Abs. 9 Satz 1 IfSG vorzulegen.

2.4.5 Einsatz von Polizeibediensteten für Kontrollen der häuslichen Quarantäne

↗ DSGVO, IfSG, IfSGZuVO

Anfang 2021 wandte sich ein Petent an meine Behörde und bat den Einsatz von Polizeibediensteten bei der Kontrolle seiner Absonderung zu überprüfen. Zum Zeitpunkt der Kontrolle befand er sich als Kontaktperson der Kategorie 1 einer an Covid-19 erkrankten Person in Absonderung (häusliche Quarantäne). Während seiner Absonderung war er mehrmals kontrolliert worden. Eines der Kontrollteams bestand aus zwei Polizeibediensteten. Der Beschwerdeführer befürchtete, dass das Gesundheitsamt seine personenbezogenen Daten bzw. Gesundheitsdaten an die Polizei weitergegeben habe, und bat mich, dies zu überprüfen.
Das Gesundheitsamt der Kreisfreien Stadt bestätigte die Durchführung der Kontrollmaßnahmen beim Petenten und teilte mit, dass die Polizeibediensteten im Rahmen der Amtshilfe im fraglichen Zeitraum an die Kommune abgeordnet waren. Sie wurden bei der Durchführung von Kontrollmaßnahmen wie kommunale Bedienstete eingesetzt. Bei den Kontrollhandlungen nutzten sie Zivilfahrzeuge. Sie traten in Uniform auf. Die zu kontrollierenden Personen wurden per Zufallsauswahl bestimmt. Dies führte im vorliegenden Fall zu den kurz nacheinander durchgeführten Kontrollen beim Petenten.
Die Befugnis zur Anordnung der häuslichen Quarantäne und zur Kontrolle, ob diese eingehalten wird, ergibt sich aus § 28

Abs. 1 und 3 Infektionsschutzgesetz (IfSG) in Verbindung mit § 30 Abs. 1 Satz 2, § 16 Abs. 2 IfSG. Danach hat die zuständige Behörde die notwendigen (Infektions-)Schutzmaßnahmen zu treffen, soweit und solange es zur Verhinderung der Verbreitung übertragbarer Krankheiten erforderlich ist.
Die Landkreise und Kreisfreien Städte sind nach § 1 Infektionsschutzgesetz-Zuständigkeitsverordnung (IfSGZuVO) die zuständigen Behörden.
Das Gesundheitsamt unterrichtet nach § 27 Abs. 1 IfSG insbesondere in den Fällen des § 25 Abs. 1 unverzüglich die zuständigen Behörden und übermittelt ihnen die zur Erfüllung von deren Aufgaben erforderlichen Angaben. Die Übermittlung der Angaben, wer sich in häuslicher Quarantäne befindet, konnte deshalb vom Gesundheitsamt an das Ordnungsamt der Kreisfreien Stadt erfolgen. Ebenfalls vom Zweck der Rechtsgrundlage umfasst ist die Überwachung der angeordneten Quarantäne. Beides ist nach Art. 6 Abs. 1 Buchst. e, Abs. 3, Art. 9 Abs. 2 Buchst. i DSGVO zulässig, da dafür eine Rechtsgrundlage im IfSG besteht.

Was ist zu tun?
Es ist sicherzustellen, dass Polizeibedienstete, die im Rahmen einer Abordnung von einer Kreisfreien Stadt eingesetzt werden, keine personenbezogenen Daten ohne gesetzliche Grundlage an den Polizeivollzugsdienst übermitteln.

Der Einsatz der Polizeibediensteten während der Abordnung erfolgt durch die Kreisfreie Stadt. Die Polizeibediensteten nehmen Aufgaben der Kreisfreien Stadt wahr. Während der Abordnung nehmen die Polizeibediensteten keine Aufgaben des Polizeivollzugsdienstes wahr. Dabei dürfen keine Daten an den Polizeivollzugsdienst „abfließen", es sei denn, gesetzliche Übermittlungsgrundlagen würden greifen.

2.4.6 Übermittlung personenbezogener Daten durch Rettungsleitstellen an die Polizei zum Zwecke der Strafverfolgung

↗ SächsBRKG

Ein Rettungszweckverband schilderte meiner Behörde, dass Gerichte, Staatsanwaltschaften und in deren Auftrag auch Polizeidienststellen häufig im Zusammenhang mit strafrechtlichen Ermittlungsverfahren Auskunft verlangten, welche Ärzte bzw. welches nichtärztliche Personal an bestimmten Einsätzen beteiligt war, um diese als Zeugen zu

vernehmen. Außerdem gäbe es Anfragen zu Einsätzen; etwa, ob es an einem bestimmten Tag zu einer bestimmten Uhrzeit einen Einsatz wegen Körperverletzungen gegeben habe und wer hierbei als Patient behandelt wurde bzw. ob eine bestimmte Person hierbei als Patient behandelt wurde.

Das von meiner Behörde kontaktierte Sächsische Staatsministerium des Innern (SMI) teilte mit, dass eine Übermittlung personenbezogener Daten, die die Rettungsleitstellen im Rahmen ihrer Aufgaben nach dem Sächsischen Gesetz über den Brandschutz, Rettungsdienst und Katastrophenschutz (SächsBRKG) verarbeiten, an die Polizei zum Zwecke der Strafverfolgung unzulässig sei. Die Erhebung der Daten durch die Rettungsleitstellen erfolge nach Maßgabe des § 72 Abs. 1 SächsBRKG. Eine Übermittlung der Daten zu anderen Zwecken, auch zu Zwecken der Strafverfolgung nach § 161 Strafprozessordnung (StPO), sei durch § 72 Abs. 2 SächsBRKG ausgeschlossen. Diese gesetzliche Regelung sei auch sachgerecht, da es sich bei den personenbezogenen Daten der im Rahmen eines Rettungsdiensteinsatzes Betreuten um Patientendaten handelt. Anderes gilt nur bei einer entsprechenden Schweigepflichtentbindungserklärung.

Soweit für polizeiliche Zwecke die personenbezogenen Daten der an einem Rettungsdiensteinsatz beteiligten Mitarbeiter benötigt werden, verfüge die Rettungsleitstelle hierüber nicht. Die Erstellung der Dienstpläne für den Notarzteinsatz obliege nach § 28 Abs. 2 Satz 2 SächsBRKG den gesetzlichen Krankenkassen. Die Erstellung der Dienstpläne für die bedarfsgerechte Besetzung der Rettungsmittel erfolge hingegen durch die Leistungserbringer nach § 31 Abs. 1 Satz 2 SächsBRKG bzw. die örtlich zuständigen Träger des Rettungsdienstes (Landkreis, Kreisfreie Stadt oder Rettungszweckverband). Insoweit habe sich die Polizei an den jeweiligen Personalverantwortlichen um Auskunft zu wenden, für den insoweit die allgemeinen datenschutzrechtlichen Maßgaben zum Umgang mit Beschäftigtendaten gelten.

3 Betroffenenrechte

3.1 Spezifische Pflichten des Verantwortlichen

3.1.1 Datenschutzinformationen bei Bürgerbegehren

↗ Art. 13 DSGVO

Die Initiatoren eines Bürgerbegehrens fragten an, in welcher Form die Informationspflichten bei der Erhebung von personenbezogenen Daten nach Art. 13 Datenschutz-Grundverordnung (DSGVO) erfüllt werden können. Sie wiesen dazu darauf hin, dass entsprechende Unterschriftenlisten nicht unbegrenzten Platz für Zusatzinformationen böten.

Das von meiner Behörde kontaktierte Sächsische Staatsministerium des Innern (SMI) verwies zunächst auf die Hinweise zum Datenschutz bei den Kommunalwahlen 2019. Zu der vergleichbaren Thematik der Sammlung von Unterstützungsunterschriften für Wahlvorschläge war empfohlen worden, das Infoblatt zum Datenschutz im Raum der Gemeindeverwaltung, in dem die Unterschriftenlisten ausliegen, auszuhängen und weitere Exemplare zur Mitnahme anzubieten.

Auf Nachfrage schloss sich das SMI auch meiner Ansicht an, dass es ausreicht, das Infoblatt separat in Papierform bereitzuhalten und zusätzlich auf eine Abrufbarkeit im Internet hinzuweisen (soweit die Vertrauenspersonen einen solchen Internetauftritt erstellen wollen). Neben einem Leseexemplar sollten mehrere Exemplare zum Mitnehmen vorhanden sein. Es sollten entsprechende Hinweis erfolgen. Ein „Auf-

drängen" des Infoblattes dahingehend, dass dieses zwingend jedem vor Unterschrift gegeben werden muss, ist nicht erforderlich.

3.1.2 Informationspflichten bei Videoüberwachung: Zweck und berechtigte Interessen

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

Im Zuge der aufsichtlichen Befassung mit Videoüberwachungsanlagen ist regelmäßig auch die Erfüllung der Informationspflichten nach Art. 13 Datenschutz-Grundverordnung (DSGVO) ein Thema. Im Tätigkeitsbericht 2019 hat mein Amtsvorgänger unter Punkt 3.1.1 (Seite 71ff.) bereits das von den deutschen Aufsichtsbehörden diesbezüglich empfohlene und auch vom europäischen Datenschutzausschuss geteilte zweistufige Informationskonzept vorgestellt. Praktische Probleme bereitet dabei regelmäßig die Differenzierung zwischen dem nach Art. 13 Abs. 1 Buchst. c DSGVO anzugebenden Zweck der Datenverarbeitung einerseits und den berechtigten Interessen nach Art. 13 Abs. 1 Buchst. d DSGVO andererseits.

In der Tat sind beide Informationen nur schwer voneinander abzugrenzen. Die Kommentarliteratur geht überwiegend nicht auf eine Unterscheidung ein und verwendet diesbezügliche Formulierungsbeispiele munter sowohl für den Zweck der Datenverarbeitung als auch für die mit der Verarbeitung verfolgten Interessen. Da die Videoüberwachung in der Datenschutz-Grundverordnung bekanntermaßen nicht speziell geregelt ist, finden sich dort für diesen Anwendungsbereich ohnehin keine speziellen Vorgaben oder Beispiele für die Erfüllung der Informationspflichten.

Zumindest angeschnitten wird die Problematik durch Bäcker (Kühling/Buchner, 3. Aufl. 2020, DS-GVO Art. 13 Rdnr. 27), der erklärt, dass sich die Informationspflicht nach Art. 13 Abs. 1 Buchst. d DSGVO teilweise mit der Pflicht aus Art. 13 Abs. 1 Buchst. c DSGVO überschneidet, da in den Fällen des Art. 6 Abs. 1 Buchst. f DSGVO das berechtigte Interesse zugleich

den Zweck der Datenverarbeitung bildet. Ihr eigenständiger Gehalt ergebe sich daraus, dass ein berechtigtes Interesse des Verantwortlichen oder eines Dritten eine Datenverarbeitung nur rechtfertigt, wenn es die gegenläufigen Interessen und Rechte der betroffenen Person überwiegt. Der Verantwortliche sei nach Art. 13 Abs. 1 Buchst. d DSGVO verpflichtet, die für diese Interessenabwägung maßgeblichen Gesichtspunkte so darzustellen, dass die betroffene Person die Abwägung nachvollziehen und gegebenenfalls substantiierte Einwände gegen sie vorbringen kann.

OH Videoüberwachung:
↗ sdb.de/tb2107

In der Orientierungshilfe Videoüberwachung der Datenschutzkonferenz finden sich zu diesem Thema Aussagen unter den Punkten 2.1 und 2.2.1:

> „Bevor eine Videokamera aktiviert wird, ist für jede Verarbeitung eindeutig zu bestimmen und festzulegen, welcher Zweck mit der Videoüberwachung erreicht werden soll. Eine Videoüberwachung kann beispielsweise eingesetzt werden, um vor Einbrüchen, Diebstählen, Vandalismus (Eigentumsschutz) oder Übergriffen (Personenschutz) zu schützen. […] Soll daher die Videoüberwachung vor Einbrüchen, Diebstählen oder Vandalismus schützen, ist darin grundsätzlich ein berechtigtes Interesse zu sehen. Gleiches gilt für Interessen wie Beweissicherung zur Durchsetzung von Rechtsansprüchen, Verhütung von Betrug, Leistungsmissbrauch oder Geldwäsche."

EDSA-Leitlinien 3/2019:
↗ sdb.de/tb2108

In gleicher Weise vermengen die EDSA-Leitlinien 3/2019 zur Verarbeitung personenbezogener Daten durch Videogeräte, Version 2.0, diese beiden Begrifflichkeiten. In Rdnr. 19 des Papiers heißt es:

> „Der Zweck, Eigentum vor Einbruch, Diebstahl oder Vandalismus zu schützen, kann ein legitimes Interesse an einer Videoüberwachung darstellen, wenn eine tatsächliche Gefährdungslage vorliegt."

Insoweit wird also auch dort von einer Begriffsidentität ausgegangen. Daran ändert sich auch unter Beiziehung der in

Rdnr. 15 der Leitlinien aufgeführten Zweckbeispiele oder der in Rdnr. 18 getroffenen Aussage, dass berechtigte Interessen eines Verantwortlichen oder eines Dritten rechtlicher, wirtschaftlicher oder immaterieller Art sein können, nichts.

> „Eine Videoüberwachung kann unterschiedlichen Zwecken dienen, zum Beipsiel dem Schutz von Eigentum und anderen Vermögenswerten, dem Schutz des Lebens und der körperlichen Unversehrtheit von Einzelpersonen, der Erhebung von Beweismitteln zur Durchsetzung zivilrechtlicher Ansprüche."
>
> EDSA-Leitlinien 3/2019 zur Verarbeitung personenbezogener Daten durch Videogeräte, Rdnr. 15

Auch aus der begrifflichen Bedeutung des Wortes Zweck – allgemein verstanden als Beweggrund einer zielgerichteten Tätigkeit – lässt sich keine griffige Abgrenzung zu den berechtigten Interessen herleiten, vielmehr führt auch dies eher dazu, eine weitgehende Deckungsgleichheit mit den berechtigten Interessen anzunehmen.
Für die Praxis kann ich vor diesem Hintergrund als grobe Empfehlung nur den Hinweis geben, dass es regelmäßig ausreichend sein dürfte, bei der Angabe des Zweckes eine eher allgemein gehaltene, schlagwortartige Angabe (übergeordnetes Ziel) zu wählen, während die Darstellung bei den berechtigten Interessen dann konkreter und detaillierter erfolgen sollte, um den betroffenen Personen das Nachvollziehen der nach Art. 6 Abs. 1 Buchst. f DSGVO vorgenommenen Interessenabwägung zu ermöglichen. Letztendlich kommt es darauf an, dass den Adressaten insgesamt, das heißt aus beiden Angaben gemeinsam, klar wird, aus welchem – berechtigten – Grund die Videoüberwachungsanlage betrieben wird. Denkbar als Zweckangabe wären daher beispielsweise Angaben wie

- Eigentumsschutz (Einbruch, Diebstahl, Vandalismus)
- Personenschutz (Schutz der körperlichen Unversehrtheit)
- Wahrnehmung der Aufsichtspflicht
- Wahrnehmung des Hausrechts

- Verkehrsüberwachung/Verkehrskoordination
- Gebührenabrechnung (zum Beispiel bei der Nutzung von Parkflächen)

während bei den berechtigten Interessen dann nähere Ausführungen wie

- Abschreckung potenzieller Straftäter
- Aufklärung von Straftaten/Beweissicherung
- Durchsetzung zivilrechtlicher Ansprüche/ Beweissicherung
- Sicherung/Überwachung von Gefahrenbereichen
- Verhinderung und Verfolgung von Diebstahl, Vandalismus und Einbruch
- Ermittlung der Standzeiten (zum Beispiel auf Parkflächen)
- Ein- und Ausfahrtskontrolle
- Prüfung der Durchfahrtsberechtigung

gemacht werden könnten. Soweit Verantwortliche schon unter dem Zweck ausreichend detaillierte Angaben machen, sollte es dessen ungeachtet auch legitim sein, bei den berechtigten Interessen lediglich auf den Zweck zu verweisen.

Was ist zu tun?
Zur Erfüllung der Informationspflicht sind die Zwecke der Datenverarbeitung zu benennen. Die Zwecke der Datenverarbeitung einerseits und berechtigte Interessen nach Art. 13 Abs. 1 Buchst. d DSGVO sind zu unterscheiden. Stützt sich der Verantwortliche auf berechtigte Interessen, hat er nach der Verordnung auch dazu zu informieren.

3.1.3 Betrieb eines Kundencenters durch einen Auftragnehmer des Verantwortlichen

↗ Art. 13 Abs. 1 Buchst. e DSGVO, Art. 28 DSGVO

Ein Kunde eines Bestattungsinstitutes (Verantwortlicher) beschwerte sich darüber, dass dieses ein Subunternehmen als Betreiber eines „Kundencenters" nutzte und dorthin die zur Vorbereitung eines Kundenkontos erforderlichen Kundendaten weitergeleitet hätte. Die betroffene Person monierte zudem, dass in den Datenschutzinformationen und -hinweisen nicht die Beauftragung und Datenweitergabe dargelegt worden wäre.
Zunächst war im Rahmen der Datenschutzkontrolle meinerseits festzustellen gewesen, dass eine Auftragsverarbeitung im Sinne von Art. 28 Datenschutz-Grundverordnung (DSGVO) zu bejahen war. Die Informationspflicht des Ver-

antwortlichen gegenüber der betroffenen Person gemäß Art. 13 Abs. 1 Buchst. b DSGVO hätte demzufolge auch konkrete Angaben über diesen (bereits bekannten) Auftragsverarbeiter enthalten müssen, was, so der Beschwerdeführer, nicht der Fall gewesen sei.

Es bestätigte sich, dass Datenverarbeitungsprozesse, wie die für den Beschwerdeführer durchgeführte Prozedur der Vorbereitung eines Kundenkontos einschließlich der Zusendung eines Anmeldelinks auf dessen E-Mail-Adresse, in den Datenschutzhinweisen des Bestattungsinstitutes nicht vorhanden waren. Allerdings war dieses Subunternehmen in anderen Zusammenhängen in den Datenschutzhinweisen mit vollständigen Angaben benannt worden. So wurde dargestellt, dass es zur „Durchführung und Verwaltung von Online-Abmeldung und zur Regelung des digitalen Nachlasses" beauftragt werden sollte. Außerdem wurde eine – allerdings vom Kunden gesondert zu beauftragende – Einrichtung eines „Gedenkportals" für die Verstorbenen als Aufgabe des Subunternehmens genannt. Die Detailleistungen waren als relativ komplex und die damit verbundenen Datenverarbeitungen als vielschichtig zu betrachten.

Dennoch blieb als vorwerfbares Versäumnis des Verantwortlichen die fehlende Bezugnahme darauf, dass bereits die Vorbereitung des Kundenkontos durch eben diesen Dienstleister ausgeführt werden sollte. Die Erklärung war insoweit im Sinne von Art. 13 Abs. 1 Buchst. e DSGVO als unvollständig zu werten gewesen.

Eine Verdeckung der Tätigkeit des Dienstleisters als Auftragnehmer lag dennoch in dem Fall nicht vor, da die entsprechende Beauftragung zur „Durchführung und Verwaltung von Online-Abmeldung und zur Regelung des digitalen Nachlasses" mit dem Kunden einzelvertraglich vereinbart worden war. Auch war keine zusätzliche oder belastende Datenverarbeitung mit der Tätigkeit des Auftragnehmers verbunden.

Unter Berücksichtigung der Gesamtumstände hat meine Behörde den Mangel der nicht granular formulierten Datenschutzhinweise als nicht durchgreifend eingeschätzt. Den

Vorgang habe ich mit allgemeinen Hinweisen an den Verantwortlichen abgeschlossen.

Allgemein bleibt zu resümieren, dass Kunden besser mehr zu Datenverarbeitung und Leistungen im Vorfeld nachfragen sollten als zu wenig, und sobald sie Klarheit gewonnen haben, auch gewollte Besonderheiten bzw. Abweichungen vom üblichen Vertragsinhalt mit einer beiderseits akzeptierten Formulierung fixieren sollten.

Verantwortliche sollten beachten, dass wiederum zusammenfassende oder summarische Darstellungen von Verarbeitungsprozessen zu Informationsverlusten führen können. Es gilt auch tiefgreifend individualisierte Vertragsgestaltungen in der Information gemäß Art. 13 und 14 DSGVO datenschutzgerecht und transparent abzubilden, Art 5 Abs. 1 Buchst. a DSGVO.

Was ist zu tun?
Verantwortlichen rate ich, ihre Datenschutzhinweise gemäß Art. 13 und 14 DSGVO nach Verarbeitungszwecken zu gruppieren und diese Zwecke jeweils vollständig abzuhandeln. Sollen die Datenschutzhinweise nicht durch eine Darstellung aller denkbaren Verarbeitungsvarianten überfrachtet werden, ist den Betroffenen auch zur Information gegebenenfalls zwingend eine auf den geschlossenen Vertrag zugeschnittene Ergänzung bzw. Abänderung zugänglich zu machen.

3.1.4 Auftragsverarbeiter als Empfänger gemäß Artikel 13 DSGVO

Damit Betroffene ihre Rechte nach der DSGVO wahrnehmen können, benötigen sie aussagekräftige Informationen darüber, dass und wie ihre personenbezogenen Daten verarbeitet werden. Deshalb sieht die DSGVO Informationspflichten für Verantwortliche vor. Dabei sind auch die Empfänger der Daten vom Verantwortlichen zu benennen.

Nach herrschender Meinung sind Auftragsverarbeiter auch nach Inkrafttreten der Datenschutz-Grundverordnung (DSGVO) noch „Empfänger" (Ehmann/Selmayr/Knyrim Art. 13 Rdnr. 33; Gola/Franck Art. 13 Rdnr. 15; Kühling/Buchner/Bäcker Art. 13 Rdnr. 28; Paal/Pauly/Paal Art. 13 Rdnr. 18, Art. 4 Rdnr. 57; BeckOK DatenschutzR/Schmidt-Wudy, 35. Ed. 1.2.2021, DS-GVO Art. 14 Rdnr. 51), mit der Folge, dass sie auch von der Informationspflicht nach Art. 13 Abs. 1 Buchst. e DSGVO umfasst sind.

Nach Paal/Pauly/Paal DS-GVO Art. 15 Rdnr. 26 besteht grundsätzlich zwischen „Empfängern" und „Kategorien von Empfängern" ein Wahlrecht zugunsten des Verantwortlichen.

Bäcker in Kühling/Buchner DS-GVO Art. 15 Rdnr. 16 führt hingegen aus: „Soweit er die Empfänger der Daten noch oder schon kennt, muss er sie auf Verlangen benennen. Dadurch kann es allerdings zu einer Kollision zwischen dem Datenschutzrecht der betroffenen Person auf Auskunft und gegenläufigen Geheimhaltungsinteressen der Datenempfänger kommen. Wenn diese Geheimhaltungsinteressen überwiegen, darf (und gegebenfalls muss) der Verantwortliche die Auskunft auf eine kategoriale Beschreibung beschränken (anders noch die Vorauflage)."

Das „oder" in Art. 15 Abs. 1 Buchst. c DSGVO lässt sich nur schwer überwinden. Im Zweifel lasse ich die Angabe der Kategorie also gelten, wobei „Auftragsverarbeiter" tatsächlich sehr allgemein gehalten ist und vom Aktenvernichter über den Lettershop bis zum Lohnrechenzentrum alles sein kann. Erwägungsgrund 63 scheint zwar eher die Ansicht zu stützen, dass in jedem Fall die „Empfänger" zu beauskunften sind und die Kategorien von Empfängern fakultativ beauskunftet werden können.

Dabei wird aber als Kategorie die schlichte Angabe „Auftragsverarbeiter" nicht ausreichend sein, es ist also eine Präzisierung angezeigt.

Was ist zu tun?
Zur Herstellung der erforderlichen Transparenz sind für eine ordnungsgemäße Erfüllung der Informationspflichten auch Auftragsverarbeiter seitens des Verantwortlichen anzugeben.

3.2 Auskunftsrecht

3.2.1 Auskunft nach Artikel 15 DSGVO durch den Gerichtsvollzieher

↗ Art. 12, 15 DSGVO

Ein Petent wandte sich mit dem Vortrag an meine Behörde, dass ein Gerichtsvollzieher, den er um Auskunft zur Verarbeitung seiner Daten nach Art. 15 Datenschutz-Grundverordnung (DSGVO) gebeten habe, die Auskunft mit der Begründung verweigert hätte, diese sei durch das Amtsgericht, in dessen Gerichtsbezirk er tätig sei, zu erteilen.

Gemäß Art. 15 Abs. 1 DSGVO hat die betroffene Person das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten

verarbeitet werden; ist dies der Fall, so hat sie ein Recht auf Auskunft über diese personenbezogenen Daten und auf weitere Informationen.

Das von meiner Behörde um Stellungnahme gebetene Amtsgericht teilte zunächst mit, dass es eine eigenständige Auskunftspflicht der Gerichtsvollzieher auf Ersuchen nach Art. 15 DSGVO nicht erkennen könne und entsprechende Auskunftsanträge durch die Behördenleitung des zuständigen Amtsgerichts zu beantworten seien.

Meine – gegenteilige – Position lautet wie folgt:

Ich sehe den Gerichtsvollzieher, der ein eigenständiges Vollstreckungsorgan neben dem Vollstreckungsgericht ist (BVerwG, 29.04.1982, Az.: 2 C 33/80), seit jeher als datenverarbeitende bzw. verantwortliche Stelle und seit Inkrafttreten der DSGVO als Verantwortlichen im Sinne von Art. 4 Nr. 7 DSGVO an (vgl. 19. Tätigkeitsbericht für den öffentlichen Bereich, 04/2017 bis 12/2018, Seite 196). Aus meiner Sicht sind für diese Einordnung die folgenden Erwägungen maßgeblich.

Tätigkeitsbericht 2017/2018:
↗ sdb.de/tb2109

Bei der ihm zugewiesenen Zwangsvollstreckung handelt der Gerichtsvollzieher selbstständig (§ 1 Abs. 1 Satz 1 Gerichtsvollzieherordnung {GVO}). Er führt ein Dienstsiegel und Geschäfts- und Kassenbücher sowie in eigener Verantwortlichkeit die Akten. Seinen Geschäftsbetrieb regelt er nach eigenem pflichtgemäßen Ermessen (§ 29 GVO) und hält an seinem Amtssitz ein Geschäftszimmer auf eigene Kosten (§ 30 Abs. 1 GVO). Der Gerichtsvollzieher ist verpflichtet, Büroangestellte auf eigene Kosten zu beschäftigen, soweit es der Geschäftsbetrieb erfordert; für ihre Tätigkeit ist er verantwortlich (§ 33 Abs. 1 GVO). Er führt die Akten nach den §§ 38ff. GVO und ist für deren korrekte Aufbewahrung und Vernichtung verantwortlich (§ 43 GVO).

Über die Einführung von Datenverarbeitungsverfahren in seinem Büro entscheidet gemäß § 29 GVO der Gerichtsvollzieher in eigener Verantwortung (Punkt C.I. der Verwaltungsvorschrift zur Geschäftsanweisung für Gerichtsvollzieher {GVGA} und die GVO); er hat beim Einsatz von

Datenverarbeitungsverfahren für die Einhaltung der datenschutzrechtlichen Bestimmungen zu sorgen (Punkt C.XV. der VwV zur GVGA und GVO).

Das in diesen Bestimmungen zum Ausdruck kommende Maß an Selbstständigkeit und Eigenverantwortung bei der Erfüllung seiner Aufgaben – auch und gerade in Bezug auf datenschutzrechtliche Aspekte – rechtfertigt die Betrachtung des Gerichtsvollziehers als Verantwortlichen, der über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet (Art. 4 Nr. 7 DSGVO) und Betroffenenrechte im Sinne des Art. 13ff. DSGVO in eigener Verantwortung zu erfüllen hat. Er ist gerade nicht als Beschäftigter des Amtsgerichts anzusehen.

Verortete man die Pflicht zur Erfüllung etwa von Auskunftsansprüchen betroffener Personen hinsichtlich ihrer beim Gerichtsvollzieher verarbeiteten Daten bei der Behördenleitung des Amtsgerichts, führte dies zu der datenschutzrechtlich absurden Situation, dass der Gerichtsvollzieher zunächst dem Gericht dort nicht vorliegende Daten über den Betroffenen zur Verfügung stellen müsste, die das Gericht allein für den Zweck der Auskunftserteilung zur Kenntnis nehmen und an den Betroffenen weiterleiten müsste. Das widerspräche sowohl dem Grundsatz der Datenminimierung (Art. 5 Abs. 1 Buchst. c DSGVO) als auch dem gesetzgeberischen Willen, die Verarbeitung personenbezogener Angaben aus Vollstreckungszusammenhängen zunächst – und ohne vollstreckungsgerichtliche Verfahren dauerhaft – ausschließlich beim Gerichtsvollzieher anzusiedeln (vgl. hierzu auch § 42a Abs. 3 Sächsisches Justizgesetz).

Unterstrichen wird dieser Befund durch die Regelungen zur Akteneinsicht für Verfahrensbeteiligte, die der Gerichtsvollzieher zu gewähren hat und nicht das (Vollstreckungs-)Gericht, § 760 Zivilprozessordnung (ZPO), § 42 GVO.

Der Hessische Verwaltungsgerichtshof ging bereits in einer Entscheidung vom 20.5.1998, Az.: 1 UE 1127/95, ganz selbstverständlich davon aus, dass der Gerichtsvollzieher als eigenverantwortliche datenverarbeitende Stelle handelt und entsprechende datenschutzrechtliche Pflichten – auch

gegenüber betroffenen Personen – zu erfüllen hat. Die der Entscheidung zugrunde liegende Rechtslage hat sich in materiell-rechtlicher Hinsicht durch das Inkrafttreten der DSGVO nicht verändert.

In diesem Zusammenhang ist erwähnenswert, dass auch nach Ansicht des Sächsischen Staatsministeriums der Justiz und für Demokratie, Europa und Gleichstellung die Gerichtsvollzieher im Freistaat Sachsen meiner datenschutzrechtlichen Aufsicht unterliegen, weil sie bei der Vornahme von Zwangsvollstreckungshandlungen keine Gerichte seien.

Das Amtsgericht wurde von meiner Behörde aufgefordert, von der bisherigen Verfahrensweise Abstand zu nehmen und Auskunftsbegehren an Gerichtsvollzieher von diesen eigenverantwortlich bearbeiten zu lassen. Im konkreten Fall traf den Gerichtsvollzieher die Pflicht, an ihn gerichtete Auskunftsbegehren gemäß Art. 12 und 15 DSGVO zu beantworten.

Das Amtsgericht teilte daraufhin mit, die Verfahrensweise korrigiert und die für den zuständigen Amtsgerichtsbezirk tätigen Gerichtsvollzieher entsprechend informiert zu haben.

Was ist zu tun?
An Gerichtsvollzieher gerichtete Anträge betroffener Personen auf Auskunft nach Art. 15 DSGVO sind durch die Gerichtsvollzieher selbst zu beantworten, die insoweit Verantwortliche im Sinne von Art. 4 Nr. 7 DSGVO sind.

3.2.2 Zulässigkeit der Datenlöschung bei Rücksendung einer defekten Festplatte und Auskunftsanspruch

↗ Art. 4 Nr. 2 DSGVO, Art. 6 Abs. 1 Buchst. a DSGVO, Art. 15 DSGVO

Nachdem ein Beschwerdeführer im April 2018 einen Laptop gekauft hatte, stellte er innerhalb der Garantiezeit von drei Jahren einen Festplattendefekt fest. Daraufhin übersandte er die Festplatte samt den darauf gespeicherten personenbezogenen Daten im April 2020 an den Händler, obgleich er von diesem zuvor darauf hingewiesen worden war, dass die Datensicherung in seiner Verantwortung als Käufer liege. Kurze Zeit später erhielt der Käufer von dem Händler eine Festplatte zugesandt, die, wie sich unmittelbar nach dem ersten Test herausstellte, nicht seine eigene war.

Zunächst versuchte der Käufer auf dem Zivilrechtsweg, Auskunft zum Verbleib seiner auf der Festplatte befindlichen personenbezogenen Daten zu erhalten, und machte auf die-

sem Wege außerdem einen Schadensersatzanspruch geltend. Obgleich eine zivilgerichtliche Entscheidung unmittelbar bevorstand, sah sich der Käufer gleichwohl veranlasst, sich parallel mit einer datenschutzrechtlichen Beschwerde (auch) an meine Behörde zu wenden. Darin trug er zunächst vor, dass sich auf der zugesandten Festplatte fremde, hochsensible personenbezogene Daten eines Dritten befunden hätten. Daraus schloss er, dass die auf seiner mutmaßlich defekten Festplatte befindlichen Daten (auch) in fremde Hände gelangt sein könnten, da er weder eine Bestätigung über die ordnungsgemäße Löschung sämtlicher Daten noch ein die Vernichtung der Festplatte dokumentierendes Zertifikat vom Händler erhalten habe.

Gericht entscheidet

Das Zivilgericht folgte in seiner Entscheidung der Argumentation des Händlers, der behauptete, nicht mehr im Besitz der Festplatte zu sein. Die Festplatte sei ausgetauscht, die alte Festplatte vernichtet und somit die vermeintlich darauf befindlichen personenbezogenen Daten keinem Dritten gegenüber weitergegeben worden. Die datenschutzrechtliche Beschwerde ebenso wie die Zivilklage waren einzig auf die Vermutung einer unzulässigen Offenlegung der auf der Festplatte vermeintlich vorhandenen personenbezogenen Daten gestützt. Es fehlte indes an objektiven Anhaltspunkten für einen diesbezüglichen Datenschutzverstoß, da der Käufer einen Nachweis für einen Festplattenzugriff und damit den Zugriff auf darauf vorhandene Daten schuldig geblieben war. In der Folge legte der Beschwerdeführer zum einen Berufung gegen das erstinstanzliche Urteil des Zivilgerichts ein, gleichzeitig erhob er beim zuständigen Verwaltungsgericht Klage gegen meine ablehnende Entscheidung. Das Berufungsgericht jedoch lehnte die Berufung unter Verweis auf das erstinstanzliche Urteil in vollem Umfang ab. In der Folge sah der Beschwerdeführer offenbar auch auf dem Verwaltungsrechtsweg nur wenige Erfolgsaussichten, sodass er sich zur Rücknahme der gegen meine Behörde gerichteten Klage entschied.

In der Sache sah das Berufungsgericht in der Vernichtung der Festplatte keine unzulässige Datenverarbeitung des Händlers. Die damit einhergehende Löschung der Daten stellt eine Datenverarbeitung nach Art. 4 Nr. 2 Datenschutz-Grundverordnung (DSGVO) dar. Dies gilt auch, soweit sie allein durch Zerstörung des Datenträgers erfolgt ist (vgl. insoweit Kühling/Buchner/Herbst, 3. Aufl. 2020, DS-GVO Art. 17 Rdnr. 39). Aus datenschutzrechtlicher Sicht bedurfte es für deren Zulässigkeit einer Einwilligung oder einer anderen gesetzlichen Grundlage aus Art. 6 Abs. 1 DSGVO.
Die Zerstörung der Festplatte war insoweit weder zur Erfüllung des zwischen Käufer und Händler bestehenden Vertrags erforderlich (Art. 6 Abs. 1 Buchst. b DSGVO) noch aufgrund einer rechtlichen Verpflichtung (Buchst. c), zur Wahrnehmung einer Aufgabe im öffentlichen Interesse (Buchst. e) oder zum Schutz eines lebenswichtigen Interesses der betroffenen Person oder einer anderen natürlichen Person (Buchst. d). Jedoch sah das Gericht die Datenträgervernichtung vorliegend durch die Einwilligung des Käufers legitimiert (Art. 6 Abs. 1 Buchst. a DSGVO). Die einwilligende Handlung lag dabei in dem schlüssigen Verhalten des Käufers mit Rücksendung der Festplatte im Rahmen der vertraglichen Garantie, da der Händler auf die alleinige Verantwortlichkeit des Käufers für die Datensicherung hingewiesen hatte.

Auskunftsbegehren

Was das auf dem Zivilrechtsweg monierte Auskunftsbegehren auf Basis von Art. 15 DSGVO anbelangt, so umfasst dieses nur den Anspruch auf Auskunft, ob personenbezogene Daten verarbeitet werden. Eine vergangenheitsbezogene Auskunftspflicht, die auch bereits gelöschte Daten umfasst, widerspräche ansonsten dem Grundsatz der Speicherbegrenzung in Art. 5 Abs. 1 Buchst. e DSGVO sowie den über Art. 15 Abs. 1 Buchst. d DSGVO anzugebenden Speicherfristen (Kamlah in: Plath, DSGVO/BDSG, 3. Aufl. 2018, Art. 15 DSGVO, Rdnr. 5; BeckOK DatenschutzR/Schmidt-Wudy, Art. 15 DSGVO Rdnr. 52; Kühling/Buchner/Bäcker, Art. 15 DSGVO Rdnr. 9).

Mit der Auskunft über den Verbleib der Festplatte sah das Gericht den Auskunftsanspruch nach § 362 Bürgerliches Gesetzbuch (BGB) als erfüllt an.
Es verwies hierzu auf die Entscheidungen des Bundesgerichtshofs, nach denen ein Auskunftsanspruch erfüllt ist, wenn die Angaben nach dem erklärten Willen des Schuldners die Auskunft im geschuldeten Gesamtumfang darstellen. Eine etwaige inhaltliche Unrichtigkeit der Auskunft steht der Erfüllung der Auskunftspflicht nicht entgegen, denn hierfür ist allein die gegebenenfalls konkludente Erklärung des Auskunftsschuldners wesentlich, dass die Auskunft vollständig ist. Einzig der Verdacht, die erteilte Auskunft sei unvollständig oder unrichtig, kann einen Anspruch auf Auskunft in weitergehendem Umfang nicht begründen (vgl. BGH, Urteil vom 3. September 2020 - III ZR 136/18, GRUR 2021, 110 Rdnr. 43 mit weiteren Nachweisen). Die Annahme eines derartigen Erklärungsinhalts setzt demzufolge voraus, dass die erteilte Auskunft erkennbar den Gegenstand des berechtigten Auskunftsbegehrens vollständig abdecken soll (BGH, Urteil vom 15. Juni 2021 – VI ZR 576/19 –, Rdnr. 19 –20, juris).
Damit lässt sich Folgendes zusammenfassen:

- Aus datenschutzrechtlicher Sicht unbestritten ist, dass in der Vernichtung eines Datenträgers, der personenbezogene Daten beinhaltet, eine Verarbeitung personenbezogener Daten nach Art. 4 Nr. 2 DSGVO liegt.
- Die Einwilligung nach Art. 6 Abs. 1 Buchst. a DSGVO in die Datenverarbeitung (hier: Vernichtung bzw. Löschung) kann auch durch schlüssiges Verhalten erfolgen, wie in der Rücksendung einer Festplatte an den Verkäufer im Rahmen einer vertraglichen Garantie bei vorhergehendem Hinweis auf die alleinige Verantwortung des Käufers für die Datensicherung.
- Zur Erfüllung der Auskunftspflicht nach Art. 15 DSGVO ist es ausreichend, wenn die Auskunft nach dem Willen des Auskunftspflichtigen den geschuldeten Umfang umfasst, auch bei einer etwaigen inhaltlichen Unrichtigkeit der Auskünfte.

Was ist zu tun?
Soweit betroffene Personen IT-Dienstleister in Anspruch nehmen, ist anzuempfehlen, die auf den Dienstleistern anvertrauten Datenträgern gespeicherten personenbezogenen Daten zuvor zu sichern, um im Falle eines möglichen Datenverlusts auf Kopien zurückgreifen zu können.
Die Auskunft des Verantwortlichen hat vollständig zu erfolgen. Um die inhaltliche Richtigkeit geht es dabei nicht. Subjektive Zweifel an der Vollständigkeit begründen keinen Anspruch auf einen weitergehenden Auskunftsumfang.

Der Rechtsstreit war am Oberlandesgericht Dresden anhängig, Urteil vom 31. August 2021 - 4 U 324/21 -.

3.2.3 Kostenfreie Kopien von Examensklausuren

↗ § 28 Abs. 2 SächsJAPO, Art. 15 Abs. 3 Satz 1 in Verbindung mit Art. 12 Abs. 5 Satz 1 DSGVO, Art. 23 DSGVO

Im Berichtszeitraum wandte sich ein Petent mit einer Datenschutzbeschwerde an meine Behörde. Er teilte mit, dass er nach erfolgreicher Absolvierung der Staatlichen Pflichtfachprüfung Kopien seiner Examensklausuren in elektronischer Form beim Landesjustizprüfungsamt (LJPA) beantragt habe. Dem sei das LJPA auch nachgekommen, habe aber Kosten in Höhe von 30 Euro in Rechnung gestellt. Der Petent sah die Pflicht des LJPA, gemäß Art. 15 Abs. 3 Satz 1 in Verbindung mit Art. 12 Abs. 5 Satz 1 Datenschutz-Grundverordnung (DSGVO) die Kopien unentgeltlich zur Verfügung zu stellen, verletzt.
Auf Nachfrage teilte das LJPA meiner Behörde mit, dass die Kosten auf Grundlage von § 13 Abs. 5 des Sächsischen Verwaltungskostengesetzes (SächsVwKG) als Aufwendungen für Vervielfältigungen erhoben würden. Bis zur Entscheidung des Bundesverwaltungsgerichts in einem (scheinbar) ähnlich gelagerten Rechtsstreit aus Nordrhein-Westfalen (siehe Oberverwaltungsgericht für das Land Nordrhein-Westfalen, 8.6.2021, Az.: 16 A 1582/20) werde man an diesem Vorgehen festhalten.

DSGVO findet Anwendung

Die Vorgehensweise des LJPA, für die Bereitstellung von Kopien von Prüfungsarbeiten Auslagen zu erheben, verstößt gegen Art. 15 Abs. 3 Satz 3 in Verbindung mit Art. 12 Abs. 5 Satz 1 DSGVO. Die Auskunftserteilung nach Art. 15 Abs. 3 DSGVO erfolgt bei Erstauskunft gemäß Art. 12 Abs. 5 Satz 1 DSGVO unentgeltlich. Dies gilt auch für eine Kopie. Das Sächsische Verwaltungskostengesetz findet auf die Erteilung von Kopien nach Art. 15 Abs. 3 Satz 1 und Satz 3 DSGVO keine Anwendung.

Die DSGVO ist auf schriftliche Prüfungsarbeiten anwendbar. Bei den vom Petenten angefertigten Examensklausuren und den Prüfergutachten handelt es sich um personenbezogene Daten im Sinne von Art. 4 Nr. 1 DSGVO, hinsichtlich derer er grundsätzlich ein Auskunftsrecht gemäß Art. 15 Abs. 1 DSGVO und das Recht auf Zurverfügungstellung von Kopien gemäß Art. 15 Abs. 3 Satz 1 DSGVO hat. Dies entspricht der höchstrichterlichen Rechtsprechung des Europäischen Gerichtshofs (EuGH, 20.12.2017, Az.: C-434/16). Zudem erfolgt auch eine Speicherung dieser personenbezogenen Daten in einem Dateisystem gemäß Art. 2 Abs. 1 DSGVO. Nach dem schriftlichen Austausch mit dem LJPA bestand hinsichtlich der Anwendbarkeit der DSGVO auf den vorliegenden Fall früh Einigkeit zwischen unseren Häusern.

Im Freistaat Sachsen existiert keine Vorschrift, die den Anspruch auf Auskunft und die Erteilung einer kostenfreien ersten Kopie im Hinblick auf juristische Prüfungsarbeiten nach den Vorgaben von Art. 23 DSGVO beschränken würde.

Die sächsische Regelung zur Einsichtnahme in Prüfungsarbeiten kann den europarechtlichen Anspruch auf Erhalt einer kostenfreien Kopie nicht beschränken. Der Anspruch auf Einsicht in Prüfungsarbeiten ist lediglich in einer Rechtsverordnung, nämlich in § 28 Abs. 2 der Sächsischen Juristenausbildungs- und -prüfungsordnung (SächsJAPO) normiert. Diese – den europarechtlich bestimmten und schriftliche Prüfungsarbeiten umfassenden Auskunftsanspruch an keiner Stelle in Bezug nehmende – Vorschrift als rechtsbeschränkende, den Anspruch nach Art. 15 DSGVO verdrängende Norm zu qualifizieren, ist mit den Anforderungen des Art. 23 Abs. 2 DSGVO an eine rechtsbeschränkende Vorschrift ebenso wenig in Einklang zu bringen wie mit der Wesentlichkeitstheorie des Bundesverfassungsgerichts, wonach die Entscheidung wesentlicher Fragen dem parlamentarischen Gesetzgeber vorbehalten ist und nicht auf die Exekutive übertragen werden kann. Der Anspruch auf Einsicht in Prüfungsarbeiten findet in § 9 des Sächsischen Juristenausbildungsgesetzes (SächsJAG), der gesetzlichen Grundlage für den Erlass einer Rechtsverordnung, keine Erwähnung; in

§ 9 SächsJAG findet sich aber auch keinerlei Bezug zu Art. 15 DSGVO oder zu einer Möglichkeit der Beschränkung des Auskunftsanspruch nach Art. 15 DSGVO. Seit der unmittelbaren Geltung der DSGVO am 25. Mai 2018 wurden sowohl das Sächsische Juristenausbildungsgesetz als auch die Sächsische Juristenausbildungs- und -prüfungsordnung geändert. Bei keiner dieser Änderungen wurde eine Beschränkung des Auskunftsanspruchs nach Art. 15 DSGVO in Erwägung gezogen oder gar umgesetzt.

Das Sächsische Verwaltungskostengesetz und mithin § 13 Abs. 5 SächsVwKG, auf den sich das LJPA stützt, gelten zwar für die Erhebung von Gebühren und Auslagen (Verwaltungskosten) für individuell zurechenbare öffentlich-rechtliche Leistungen der Behörden des Freistaates Sachsen, finden allerdings gemäß § 1 Abs. 2 SächsVwKG auf die Erhebung von Verwaltungskosten nach anderen Rechtsvorschriften einschließlich der unmittelbar geltenden Rechtsakte der Europäischen Union nur ergänzende Anwendung, soweit dort nichts Abweichendes bestimmt ist. In Art. 12 Abs. 5 Satz 1 DSGVO ist die Kostenfreiheit klar normiert – in Verbindung mit Art. 15 Abs. 3 Satz 1 und 2 DSGVO bezieht sie sich auch unmissverständlich auf eine erste Kopie –, sodass das Sächsische Verwaltungskostengesetz insoweit, eben wegen einer abweichenden Regelung in einer unmittelbar geltenden EU-Verordnung, nicht zur Anwendung kommt. Der Landesgesetzgeber hat hier den Anwendungsvorrang europäischen Rechts gesehen und bei der Formulierung des § 1 Abs. 2 SächsVwKG – deklaratorisch – besonders hervorgehoben.

Verfahren geändert

Leider ging das LJPA auf diese Hinweise zur – klaren – sächsischen Rechtslage nicht ein und teilte mit, dass es bis zu einer Entscheidung des Bundesverwaltungsgerichts im nordrhein-westfälischen Rechtsstreit (siehe oben) daran festhalte, Kosten für Kopien von Prüfungsarbeiten nach § 13 Abs. 5 SächsVwKG zu erheben.

Erst auf meine direkt gegenüber dem Sächsischen Staatsministerium der Justiz und für Demokratie, Europa und Gleich-

Was ist zu tun?
Das LJPA hat Prüflingen eine von ihnen beantragte Kopie ihrer Prüfungsarbeiten kostenfrei zur Verfügung zu stellen.

stellung geäußerte Absicht, im Wege der Anordnung nach Art. 58 Abs. 2 Buchst. c DSGVO das LJPA anzuweisen, Prüflingen auf Antrag eine erste Kopie ihrer schriftlichen Prüfungsarbeiten kostenfrei zur Verfügung zu stellen, hat das LJPA seinen Rechtsstandpunkt und die bisherige Praxis noch einmal überprüft und entschieden, hieran nicht mehr festzuhalten und Kopien kostenfrei auszugeben.

4 Pflichten Verantwortlicher und Auftragsverarbeiter

4.1 Verantwortung für die Verarbeitung, Technikgestaltung

4.1.1 Vereinfachtes Prüfschema für den Einsatz von Zusatzdiensten auf Websites/Apps nach DSGVO, TTDSG und Schrems II

↗ § 25 TTDSG; Art. 6, 8, 25, 28, 32, 49 DSGVO

OH Telemedien:
↗ sdb.de/tb2110

Immer wieder werde ich von Verantwortlichen angesprochen, dass es so schrecklich kompliziert sei mit den Cookies und dem Datenschutz. Nun ganz so kompliziert ist es eigentlich nicht, es gibt auch sehr viele Arbeitshilfen der Aufsichtsbehörden, zuletzt die aufgrund der Änderungen im Telemedienrecht aktualisierte Orientierungshilfe Telemedien. Dennoch will ich an dieser Stelle versuchen, in Kurzform darzustellen, welche Anforderungen zu beachten sind und auf welche Punkte die Aufsichtsbehörden bei Überprüfungen von Websites und Apps besonders achten.

Im Grundsatz gilt es drei Gruppen von Anforderungen zu beachten. Zum einen natürlich die Datenschutz-Grundverordnung (DSGVO) – insbesondere Art. 25 und 32 – für alle Verarbeitungen einer Website oder einer App. Dabei ist zu beachten, dass jede Ressource, also auch eine eingebundene Schriftart oder ein eingebettetes Video eines fremden Servers, eine eigene Verarbeitung darstellt. Des Weiteren gilt seit 1. Dezember 2021 das Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG), welches im Grundsatz eine Einwilligung in das Setzen und Auslesen von Cookies und

ähnlichen Technologien auf Endgeräten fordert. Schlussendlich ist das sogenannte Schrems-II-Urteil des Europäischen Gerichtshofs zu beachten, welches Datenübermittlungen in außereuropäische Drittländer deutlich erschwert.

Wie können diese Anforderungen erfüllt werden, und wann ist eine Einwilligung erforderlich?

Verständlicherweise wollen viele Verantwortliche auf die ungeliebten und von vielen Nutzerinnen und Nutzern als lästig empfundenen Einwilligungsbanner verzichten. Dies ist aber nur unter sehr engen Voraussetzungen möglich. Die DSGVO regelt alle Verarbeitungen und fordert die Existenz einer gültigen Rechtsgrundlage. Die für Websites und Apps am ehesten infrage kommende Rechtsgrundlage ist neben der Einwilligung (Art. 6 Abs. 1 Buchst. a) das berechtigte Interesse (Art. 6 Abs. 1 Buchst. f). Dieses berechtigte Interesse muss aber nachgewiesen werden und fordert eine Abwägung zwischen den Interessen des Verantwortlichen und den Interessen oder Grundrechten und Grundfreiheiten der betroffenen Person. Dies ist alles andere als trivial, eine bloße Nützlichkeitsbegründung seitens des Verantwortlichen ist nicht ausreichend. Dies ist in der Praxis einer der häufigsten Fehler, wenn auf Nachfrage der Aufsichtsbehörde der Einsatz eines Dritt-Dienstes rein mit den Interessen des Verantwortlichen begründet wird und bestehende Risiken rein damit begründet werden, dass die Nutzerinnen und Nutzer das doch so wollen. Das ist zum einen keine Risikoabwägung und zudem falsch, wie das beständig hohe Beschwerdeaufkommen im Telemedienbereich zeigt (siehe 6.2.2).

Fakten, die für eine Interessenabwägung zugunsten des Verantwortlichen sprechen, sind zum Beispiel eine nachweisbare und den Anforderungen des Art. 28 DSGVO entsprechende Auftragsverarbeitung mit einem eingebundenen Dienstleister oder eine Verarbeitung durch den Verantwortlichen selbst bzw. technisch-organisatorische Maßnahmen wie eine zügige Anonymisierung von personenbezogenen Daten (zum Beispiel IP-Adressen, Cookie-Identifikatoren). Verarbeitungen, die aufgrund ihres Risikos eher nicht auf ein berechtig-

tes Interesse gestützt werden können, sind die Bildung von Profilen und sogenannten Nutzer-Journeys, also all das, was landläufig unter Tracking verstanden wird. Das berechtigte Interesse ist in aller Regel auch dann infrage zu stellen, wenn ein Dritter die erlangten Daten für eigene Zwecke nutzt oder dies nicht klar ausgeschlossen ist. Um es klar zu sagen: Die Nutzung von Diensten großer Anbieter, deren Geschäftsmodell das Sammeln und Aggregieren von Nutzungsdaten zu Werbezwecken ist und die dazu noch über eine entsprechende Marktmacht verfügen, ist mit einem berechtigten Interesse des Verantwortlichen nicht vereinbar. Zumal in vielen Fällen der Verantwortliche gar nicht weiß, wie der Dienstleister mit den erlangten Daten genau umgeht. Die Rechtsprechung geht aber klar von einer Mitverantwortung des Verantwortlichen auch für genutzte Dienste aus. Fehlen die Voraussetzungen für ein berechtigtes Interesse, bleibt in aller Regel nur ein Rückgriff auf eine Einwilligung. Dabei sind alle Anforderungen aus der DSGVO zu beachten, die strikte Regeln für Transparenz, Bestimmtheit und Freiwilligkeit fordert sowie in Fällen der Nutzung durch Minderjährige eine Einwilligung der Erziehungsberechtigten vorsieht. All diese Anforderungen in der Praxis zu erfüllen ist in der Tat schwierig, ich empfehle daher stets eine genaue Prüfung, welche Verarbeitungen tatsächlich unbedingt erforderlich sind.

Werden Einwilligungen eingeholt, müssen diese auch eine tatsächliche Einwilligung darstellen. In der Praxis häufig zu findende Tricks (Stichworte: Dark Pattern und Nudging) sind, wenn sie eine gewisse Grenze überschreiten, klar rechtswidrig.

Geringer Spielraum für Cookies ohne Einwilligungserfordernis

Werden zusätzlich zu einer Verarbeitung auch Cookies oder ähnliche Technologien eingesetzt, muss deren Einsatz den Anforderungen des TTDSG entsprechen, welches dafür grundsätzlich eine Einwilligung vorsieht. Auch wenn sich mit diesem Gesetz, das die seit dem Jahr 2002 geltende europäische ePrivacy-Richtline in deutsches Recht um-

setzt, nicht viel geändert hat, sollte jedem Verantwortlichen klar sein, dass das massenhafte Setzen von Cookies nun ein Ende haben muss. Ausnahmen von einem Einwilligungserfordernis sind eng begrenzt auf eine unbedingte Erforderlichkeit, damit der Anbieter einen vom Nutzer ausdrücklich gewünschten Telemediendienst zur Verfügung stellen kann. Was heißt das nun in der Praxis? Die von einigen Stimmen geforderte Umkehr des Einwilligungserfordernisses nach dem Motto „Die Leute wollen das doch so!" vertrete ich natürlich nicht, aber auch ich sehe Möglichkeiten für das Setzen und Auslesen von Cookies ohne Einwilligung. Ausgehend von den Begrifflichkeiten des Nutzerwunsches und der Erforderlichkeit muss jeder Cookie überprüft werden: Wann, wie, für wie lange und für wen wird ein Cookie gesetzt? Es geht dabei um eine Bewertung des Zweckes und der Mittel!

Das „Wann?" bezieht sich auf den Zeitpunkt des Setzens. So muss ein individualisierter Warenkorb-Cookie in einem Online-Shop erst dann gesetzt werden, wenn der Warenkorb genutzt wird. Für ein bloßes Browsen ist dieser nicht erforderlich. Gleiches gilt für Cookies für Zusatzfunktionen wie Chats oder Karten-Widgets. Hier kann das „Wann" am Nutzerwunsch festgemacht werden, der Cookie ist erst dann erforderlich, wenn der betreffende Dienst auch tatsächlich genutzt wird.

Das „Wie?" bezieht sich auf den Inhalt des Cookies. Besonders relevant im Sinne der Vorschrift des § 25 TTDSG (Schutz der Privatsphäre bei Endeinrichtungen) sind Cookies, die individuelle Pseudonyme in Form von zufallsgenerierten oder anderweitig erlangten Informationen (eindeutige Gerätemerkmale in Form von Fingerprints oder gerätespezifische Identifikationsnummern) setzen und/oder auslesen. In vielen Fällen besteht dafür keine Erforderlichkeit. So ist zum Beispiel nicht als erforderlich zu betrachten, dass ein Einwilligungsmanagement, welches die Entscheidung über die Auswahl an gewünschten Verarbeitungen speichern soll, einen individualisierten Cookie setzt (und schon gar nicht beim initialen Aufruf einer Website, bevor eine Entscheidung getroffen wurde, siehe obiger Absatz). Für die Speicherung der Ent-

scheidung reicht es, diese nichtindividualisiert zu speichern (zum Beispiel in Form von „tracking=false; comfort=true …). Da Cookies mit individueller ID das größte Risiko für die Privatsphäre von Nutzerinnen und Nutzern darstellen, sind diese für die Aufsichtsbehörden von besonderem Interesse.

Das „Wie lange?" bezieht sich auf die Lebensdauer eines Cookies. Auch hier ist es entscheidend, ob es sich um einen individualisierten Cookie handelt, weil dieser in Kombination mit einer langen Laufzeit eine Erkennung wiederkehrender Besucherinnen und Besucher einer Website ermöglicht. Um es klar zu sagen: Fälle von individualisierten Cookies mit einer Laufzeit über eine Session hinaus sind in der Praxis schwer ohne Einwilligung vorstellbar. Auch beim im obigen Absatz bereits erwähnten Warenkorb-Cookie ist eine dauerhafte Markierung von Besucherinnen und Besuchern sicherlich im Interesse eines Shop-Betreibers, aber ohne explizite Einwilligung ist dies nicht möglich.

Das „Für wen?" bezieht sich auf die setzende Domäne eines Cookies oder allgemein auf den Empfänger der Daten. Cookies und andere Merkmale, die über die Grenzen der eigentlich aufgerufenen Website gesetzt und ausgelesen werden, stellen aufgrund der damit verbundenen Möglichkeit der webseitenübergreifenden Nachverfolgung ein hohes Risiko für die Privatsphäre dar. Auch hier sind in der Praxis nur sehr wenige Fälle denkbar, in denen die Ausnahmen von einem Einwilligungserfordernis greifen werden.

Besser auf Cookies verzichten

Es muss jedem Verantwortlichen klar sein, dass das Gesetz erfordert, dass jeder Cookie auf den Prüfstand muss. Gegebenenfalls sollte bei dieser Gelegenheit auch geprüft werden, welche Dienste auch ohne das Setzen von Cookies funktionieren. Klar ist auch, dass die Aufsichtsbehörden nicht nur den Zweck, sondern auch die konkreten Mittel überprüfen und eine pauschale Aussage, wonach ein Cookie für zum Beispiel das Load-Balancing erforderlich sei, technisch genau überprüft wird.

Vom Einwilligungserfordernis sind auch „harmlose" Cookies umfasst, beispielsweise ein Cookie, welcher Spracheinstellungen speichert in Form eines Inhaltes wie zum Beispiel „language=de". In diesem konkreten Fall ist es durchaus möglich, dass die Aufsichtsbehörde darüber hinwegsieht, wenn dieser Cookie bereits beim Aufruf der Website gesetzt wird.

Einsatz von US-Dienstleistern meist nicht möglich

Schlussendlich sind als dritter Aspekt eines Telemediendienstes auch mögliche Bezüge in Drittstaaten außerhalb der EU zu beachten. Zwar haben viele Dienstleister, vor allem aus den USA, europäische Niederlassungen und bieten Auftragsverarbeitungsverträge an (deren Konformität mit Art. 28 DSGVO hier zunächst dahingestellt sei) und sichern eine Datenverarbeitung in Europa zu. Allerdings wird in den Verträgen eine Datenverarbeitung im Ausland „im Ausnahmefall" häufig dennoch nicht ausgeschlossen. Der Einsatz solcher Dienstleister ist in vielen Fällen schlicht nicht möglich. Auch schützt der Vertragsabschluss mit der europäischen Niederlassung eines US-amerikanischen Dienstleisters nicht vor Zugriffen von ausländischen Behörden im Rahmen des Cloud-Acts.

Weiterhin existieren für den Bereich Nutzungsdatenverarbeitung keine zusätzlichen Maßnahmen, die einen Schutz der Daten sicherstellen können, mindestens die IP-Adresse und Nutzungsdaten des Endgeräts sind immer betroffen und können nicht abgesichert werden. Auch wenn es von Verantwortlichen gelegentlich als „zusätzliche Schutz-Maßnahme" vorgebracht wird, eine Transportverschlüsselung ist klar keine solche Maßnahme, sondern Standard und zudem untauglich zum Schutz von exportierten Daten. Der Europäische Datenschutzausschuss hat in seinen Leitlinien 2/2018 zu den Ausnahmen nach Artikel 49 der Verordnung 2016/679 auch festgestellt, dass personenbezogene Daten, die im Zusammenhang mit der regelmäßigen Nachverfolgung von Nutzerverhalten auf Webseiten oder in Apps verarbeitet werden, grundsätzlich nicht auf Grundlage einer Einwilligung nach

Was ist zu tun?
Betreiber von Websites und Apps sollten die Verwendung von Cookies und anderen Technologien dringend überprüfen. Insbesondere ist die genaue Ausgestaltung der Technologien und deren Notwendigkeit einer Revision zu unterziehen. Art und Dauer der Speicherung sowie die nachgelagerte Verarbeitung müssen den Anforderungen an TTDSG und DSGVO entsprechen.

Art. 49 Abs. 1 Buchst. a DSGVO in ein Drittland übermittelt werden können.
Dieser Beitrag kann nicht alle Aspekte, insbesondere die der Einwilligung, in Gänze behandeln, soll aber Verantwortlichen Möglichkeiten des sicheren Betriebs einer Website oder App eventuell auch ohne Einwilligungserfordernis aufzeigen. Denn nach wie vor ist es möglich, auch ohne die ungeliebten Einwilligungsbanner rechtskonform Dienste anzubieten. Es erfordert aber eine genaue Bestandsaufnahme und präzise Begründungen.

4.1.2 Elektronisches Klassenbuch

↗ VwV Schulformulare

18. Tätigkeitsbericht:
↗ sdb.de/tb2111

Im 18. Tätigkeitsbericht (2017) schilderte mein Amtsvorgänger unter 7.5 auf Seite 96, dass mehrere Anfragen nach der Zulässigkeit eines rein elektronischen Notenbuches leider abschlägig beantworten werden mussten, da die einschlägige VwV Schulformulare für dieses wie für das Klassentagebuch vorschrieb, sie im Format DIN A4 zu führen.
Mit der Neufassung der Verwaltungsvorschrift vom 25. August 2021 ergibt sich ein anderes Bild. Demnach können nunmehr Schülerübergabeverzeichnis, Schülerkartei, Notenbuch, Klassenbuch und Kursbuch in elektronischer Form geführt werden, sofern näher bestimmte technische Anforderungen erfüllt werden. So ist für diese Unterlagen beispielsweise eine vollständige Sicherung in unveränderbarer elektronischer Form oder in gedruckter Form als geheftetes Dokument durchzuführen. Anstelle des Signums und der Unterschrift ist zudem eine elektronische Signatur zu verwenden. Es bleibt abzuwarten, wie gerade Letzteres in der Praxis umgesetzt werden wird. Leider wurde meine Anregung, eine entsprechende Software im Rahmen der Sächsischen Schulverwaltungssoftware (SaxSVS) zur Verfügung zu stellen, bislang nicht aufgegriffen.

4.1.3 Mitteilungen von Gerichtsvollziehern nur in verschlossenen Umschlägen

↗ Art. 5 Abs. 1 Buchst. f DSGVO, Art. 32 DSGVO

Immer wieder beschweren sich Bürger bei mir über Gerichtsvollzieher, die amtliche Schreiben oder die ein Zwangsvollstreckungsverfahren betreffende Mitteilung ohne Umschlag in den Briefkasten, auf den auch andere Personen Zugriff haben, werfen oder direkt offen an Dritte (Mitbewohner oder Angestellte) übergeben würden. So sei es diesen Personen (Dritten) möglich, Kenntnis von der Existenz eines gegen die betroffene Person geführten Zwangsvollstreckungsverfahrens und vom Inhalt des Schreibens selbst zu erlangen.

Zum Thema Zustellungen durch Gerichtsvollzieher wurde bereits im 13. Tätigkeitsbericht für den öffentlichen Bereich (2007), Seite 138, auf die Pflicht zur Benutzung von Umschlägen hingewiesen. Damals ging es um die förmliche (Ersatz-)Zustellung eines Gerichtsbeschlusses.

Anlässlich der mich nach wie vor erreichenden Petitionen zu diesem Thema möchte ich betonen, dass nicht nur förmlich zuzustellende Dokumente, sondern grundsätzlich auch „einfache" Nachrichten, zum Beispiel schon die Mitteilung, dass in einem konkreten Verfahren um Kontaktaufnahme gebeten wird, in einem verschlossenen Umschlag in den Briefkasten des Adressaten zu legen oder – ersatzweise – an Dritte auszuhändigen sind. Eine Ausnahme kann – theoretisch – nur dann zulässig sein, wenn der Gerichtsvollzieher sicher weiß, dass ausschließlich der Empfänger Zugriff auf den Briefkasten hat. Dies wird jedoch in aller Regel nicht der Fall sein.

Grund für die Pflicht zur Verwendung eines verschlossenen Umschlags – dies gilt auch, wenn der Einwurf in einen Familienbriefkasten erfolgt, auf dem lediglich der Familienname angegeben ist – ist, dass der Gerichtsvollzieher zur Amtsverschwiegenheit und zur Wahrung der Persönlichkeitsrechte des betroffenen Schuldners als Adressat der Schreiben verpflichtet ist. Bereits der Umstand, dass der Adressat Beteiligter in einem Zwangsvollstreckungsvorgang ist, ist eine insoweit geheimhaltungsbedürftige Tatsache, die nicht unbefugt

an Dritte übermittelt werden darf. Der Amtsverschwiegenheit unterliegende Informationen zum Schuldner oder zum Gegenstand des Verfahrens dürfen ohne Rechtsgrundlage nicht an Dritte (hierunter zählen eben auch Familienangehörige) gelangen. Für eine Offenlegung personenbezogener Daten aus dem Zwangsvollstreckungsverfahren gegenüber Dritten, die eben auch im Ermöglichen der Kenntnisnahme eines offenen Schreibens liegen kann, fehlt es an einer solchen Rechtsgrundlage. Deshalb hat der Gerichtsvollzieher stets die für den Schutz des Rechts des Schuldners erforderlichen organisatorischen Maßnahmen – hier die Verwendung eines verschlossenen Umschlags – zu treffen.

Was ist zu tun?
Um unbefugte Kenntnisnahme Dritter zu vermeiden, haben Gerichtsvollzieher Mitteilungen und zuzustellende Urkunden stets in einem verschlossenen Umschlag in den Briefkasten zu werfen oder Dritten zu übergeben.

4.1.4 Weiterleitung einer E-Mail an einen Stadtrat durch den Oberbürgermeister

↗ § 52 Abs. 5 SächsGemO, Art. 6 DSGVO

Ein Stadtrat informierte meine Behörde, dass der Oberbürgermeister einer sächsischen Stadt die an ihn gerichtete E-Mail einer Bürgerin, die als Reaktion auf eine öffentliche Stadtratssitzung erfolgte und sich bereits in der Anrede allein an den Stadtrat richtete, gelesen und die „Ratsschreibstube" angewiesen hätte, diese E-Mail an alle anderen Stadträte weiterzuleiten.

Der um Stellungnahme gebetene Oberbürgermeister konnte zunächst keinen Datenschutzverstoß feststellen, da die Nachricht an das allgemeine städtische E-Mail-Postfach gerichtet war. Auch sei das ursprüngliche Schreiben des Stadtrats, auf das die Bürgerin reagiert hatte, „an die Gemeinschaft der Stadträte und die Öffentlichkeit" gerichtet gewesen. Schließlich wurde eingewandt, dass die Bürgerin mit der Nachricht den gesamten Stadtrat adressieren wollte. Letzteres kann schon deswegen nicht überzeugen, da der Stadtrat in der E-Mail persönlich angesprochen wurde. Auch kann eine Adressierung des Schreibens des Stadtrats „an die Gemeinschaft der Stadträte und die Öffentlichkeit" keine Bindungswirkung für die Absenderin des gegenständlichen Schreibens entfalten. Ebenso war die Weiterleitung der E-Mail nicht

erforderlich. Zwar ist ein Bürgermeister gemäß § 52 Abs. 5 Sächsische Gemeindeordnung (SächsGemO) kraft Amtes verpflichtet, den Stadtrat über alle die Gemeinde und Verwaltung betreffenden Angelegenheiten zu informieren, doch umfasst dies gerade nicht die Weiterleitung einer an allein einen Stadtrat gerichteten E-Mail. Gegenteiliges ergibt sich auch nicht aus einem weiten Verständnis des Begriffs der Angelegenheit in § 52 SächsGemO, bei der ein Bürgermeister über die Reichweite seiner Informationspflicht nach pflichtgemäßem Ermessen entscheidet. Die Befugnisse enden dort, wo die Persönlichkeitsrechte des Empfängers wie hier überwiegen.
Dies sah der Bürgermeister schließlich ein und sicherte zu, dass künftig die dargestellten datenschutzrechtlichen Vorgaben bei explizit adressierten E-Mails beachtet werden.

4.1.5 Mitarbeit an einer Nachfolgelösung für den Videokonferenzdienst

↗ Art. 25 und 32 DSGVO

Die Staatskanzlei verantwortet die Bereitstellung und den Betrieb des Sächsischen Verwaltungsnetzes (SVN), mit dem alle staatlichen und kommunalen Behörden innerhalb eines gesicherten Netzes kommunizieren können. Teil des SVN sind auch sogenannte Basisdienste wie zum Beispiel ein Videokonferenzdienst. Dieser wurde bei der Planung der jetzigen SVN-Lösung als On-Premise-Dienst eingekauft und allen Behörden bereitgestellt. On-Premise heißt, dass Hard- und Software für diese Lösung in einem Rechenzentrum betrieben werden, welches unter Kontrolle der Staatskanzlei steht. Nun war dieser Videokonferenzdienst für Spezialfälle gedacht, weil man zum Zeitpunkt der Planung noch nicht an Situationen wie eine Pandemie gedacht hatte. Als im Zuge der Corona-Pandemie auch die öffentliche Verwaltung in großem Umfang auf Home-Office umsatteln musste, war die Lösung leider vollkommen unterdimensioniert. Um Abhilfe zu schaffen, hat die Staatskanzlei weitere Lizenzen für den Videokonferenzdienst erworben und den Behörden zur Verfügung gestellt.

Videokonferenzdienst in der Cloud nicht datenschutzkonform

Mein Amtsvorgänger hat nach Bereitstellung der zusätzlichen Lösung, die sich physisch in der Cloud befand, die zugrunde liegenden Verträge angefordert und musste feststellen, dass diese nicht den datenschutzrechtlichen Vorgaben entsprachen. So war nicht ausgeschlossen, dass der Hersteller Daten für eigene Zwecke verwendet, zum Beispiel zur Verbesserung der Produkte, was aber mit einer Auftragsverarbeitung nicht zu vereinbaren ist und wofür eine öffentliche Stelle schlicht keine Rechtsgrundlage hat. Weiterhin war nicht wirksam ausgeschlossen, dass Datenübermittlungen außerhalb der Europäischen Union stattfinden und Daten in sogenannten unsicheren Drittstaaten verarbeitet werden. Meine Behörde hat die Staatskanzlei auf diese Mängel hingewiesen, allerdings in Anbetracht des dringenden Erfordernisses für eine Videokonferenzlösung in der Pandemiezeit eine zeitlich befristete Duldung vereinbart.

Gleichzeitig wurde vereinbart, dass eine Unterarbeitsgruppe des Arbeitskreises SVN zur Findung einer rechtlich unbedenklichen Nachfolgelösung, die gleichzeitig alle fachlichen Anforderungen erfüllt, ins Leben gerufen wird. Diese Unterarbeitsgruppe wurde vom SID im Auftrag der Staatskanzlei geleitet und war mit Vertretern der Technikbereiche einzelner Ministerien sowie mit Vertretern der Barrierefreiheit, der Informationssicherheit und eben des Datenschutzes besetzt. Als ausdrückliches Ziel der Arbeit wurde seitens der Staatskanzlei auch die Stärkung der digitalen Souveränität des Freistaates Sachsen benannt, ein Ziel, welches auch meinen Vorstellungen entspricht.

Entscheidung für freie Software

Die Unterarbeitsgruppe nahm ihre Arbeit zügig auf. Ein Kriterienkatalog mit rechtlichen, technischen und fachlichen Anforderungen wurde erstellt und zahlreiche infrage kommende Produkte wurden im Rahmen von Teststellungen untersucht. Im Ergebnis hat die Unterarbeitsgruppe eine Empfehlung für ein Produkt ausgesprochen, welches auf freier Software ba-

siert und vom Freistaat Sachsen in eigener Verantwortung betrieben werden kann. Dabei wurde deutlich, dass auch fachliche und technische Anforderungen nicht nur, wie oft behauptet, durch namhafte Hersteller erfüllt werden können. Mein Amtsvorgänger hat sich auch für dieses Produkt ausgesprochen, sowohl aus Gründen der rechtlichen Kontrollierbarkeit als auch aus wirtschaftlichen Erwägungen heraus. Für die ebenfalls in der Bewertung enthaltenen Cloud-Dienste großer internationaler Hersteller hatte sich meine Behörde ausdrücklich nicht ausgesprochen. Eine solche Datenverarbeitung weist hohe Risiken für einen rechtssicheren Betrieb auf, da umfangreiche Vertragsunterlagen, komplexe Datenflüsse und sich häufig ändernde Bedingungen schwer mit den Anforderungen an Transparenz, Informiertheit und Betroffenenrechte zu vereinbaren sind. Das Ergebnis wurde der Staatskanzlei inzwischen vorgelegt, ich hoffe auf eine entsprechende Reaktion, werde allerdings die oben dargestellten Mängel in Zukunft nicht mehr dulden.

Was ist zu tun?
Die Behörden des Freistaats Sachsen sind pflichtig, Videokonferenzdienste zum Einsatz zu bringen, die Art. 25 und 32 DSGVO genügen. Entsprechendes gilt für die Inanspruchnahme von Cloud-Diensten. Autark und in eigener Verantwortung betriebenen Systemen ist der Vorzug zu geben.

4.2 Auftragsverarbeitung

4.2.1 Verarbeitung personenbezogener Daten bei der Untersuchung von Vorgängen durch „unabhängige" Expertenkommissionen

↗ § 3 SächsDSDG; §§ 4, 17 SächsVwOrgG; Art. 28 DSGVO

Im Zuge der Aufarbeitung öffentlich bekannt gewordenen verwaltungsinternen Fehlverhaltens mit Skandalisierungspotenzial erfreut sich in den letzten Jahren die Beauftragung eines externen Experten beziehungsweise einer aus nicht der Verwaltung des Freistaates angehörigen Experten bestehenden Kommission mit der unabhängigen Untersuchung der Vorfälle zunehmender Beliebtheit. Zumeist erteilt das Staatsministerium, in dessen Zuständigkeitsbereich die zu untersuchenden Vorgänge stattgefunden haben, dem beziehungsweise den Experten im Wege eines zivilrechtlichen Vertrages den Auftrag zur Untersuchung und zur Vorlage eines Abschlussberichts. Besonders betont werden bei der Information der Öffentlichkeit über die Einsetzung einer Experten-

kommission regelmäßig die Unabhängigkeit der Experten und der Umstand, dass ihnen bei der Erfüllung ihres Auftrages keine Weisungen erteilt werden. Zivilvertraglich wird den Experten Zugang zu behördlichen Unterlagen und Unterstützung durch Beschäftigte des Freistaates zugesichert.
Ich kritisiere diese Praxis seit Langem. Ist einerseits der Einsatz von Personen des Privatrechts etwa bei Organisationsuntersuchungen, in deren Verlauf keine personenbezogenen Daten verarbeitet werden und nicht in Grundrechte von Personen eingegriffen wird, unproblematisch und angesichts besonderer Fachkenntnisse Externer für den erstrebten Zweck oftmals förderlich, begegnet andererseits die Beauftragung privater Personen mit Untersuchungen konkreter Vorfälle, die ohne die Verarbeitung personenbezogener Daten schlechterdings nicht geführt werden können und für die der Gesetzgeber zuständige staatliche Stellen und Verfahrensregelungen festgelegt hat, größten rechtsstaatlichen Bedenken.

Keine Auftragsverarbeitung bei Beauftragung einer weisungsfreien Stelle

Die unbestreitbare Befugnis einer (Aufsichts-)Behörde, sich umfassend über Vorgänge in ihrem Zuständigkeitsbereich zu informieren und diese im Rahmen ihrer Selbstkontrolle zu untersuchen, kann aus verfassungs- und staatsorganisationsrechtlichen Gründen nicht die Beauftragung „unabhängiger" dritter Personen oder Stellen außerhalb der Staatsverwaltung mit Tätigkeiten umfassen, die mit Grundrechtseingriffen einhergehen. Die Zuschreibung einer Aufgabe allein befugt die zuständige staatliche Stelle nicht, die mit Grundrechtseingriffen verbundene Ausführung dieser Aufgabe zivilvertraglich auf eine außerhalb der staatlichen Verwaltung stehende, weisungsfrei und unabhängig agierende Stelle zu übertragen. Eine zivil-vertragliche „Bestellung" kann die erforderliche gesetzliche Übertragung einer grundrechtsbeeinträchtigenden Aufgabenwahrnehmung nicht ersetzen. Sie ist in datenschutzrechtlicher Hinsicht auch keine Auftragsverarbeitung (Art. 28 DSGVO), deren zentrales Element die Weisungsgebundenheit des Auftragsverarbeiters ist.

Externen, unabhängigen Experten fehlt verfassungsgemäße Legitimation

Für die staatlich initiierte Verarbeitung personenbezogener Daten – ein Grundrechtseingriff – durch eine unabhängige, nicht weisungsgebundene Expertenkommission, die „freihändig" zivilvertraglich beauftragt wird und deren Mitglieder nicht dienstrechtlich in die Verwaltungsstruktur der für entsprechende Untersuchungen zuständigen Aufsichtsbehörde eingebunden sind, gibt es schlicht keine Rechtsgrundlage. Eine solche wäre aber zwingend erforderlich und findet sich etwa bezüglich der Einbindung anderer Privater in förmliche staatliche Verfahren – nämlich die Sachverständigen, die im Fall ihrer Ernennung einer öffentlich-rechtlichen Gutachterpflicht nachkommen und nach gesetzlichen Vorschriften vergütet werden – in detaillierter Form in den Verfahrensgesetzen.

So nachvollziehbar der Gedanke, ein nichtstaatliches, unabhängiges Gremium behördliche Vorgänge und Vorfälle „besonders objektiv" prüfen zu lassen, auch ist, so wenig ist die Beauftragung unabhängiger, weisungsfreier Privater mit der eigenmächtigen Verarbeitung personenbezogener Daten, die öffentliche sächsische Stellen in ihrer gesetzlichen Zuständigkeit hoheitlich erhoben haben und speichern, mit essenziellen rechtsstaatlichen Grundsätzen vereinbar. Dies gilt erst recht in Vorgängen, in denen disziplinar- und/oder strafrechtlich relevante Verfehlungen im Raum stehen, deren Verfolgung eine Kerntätigkeit des hoheitlich agierenden Staates darstellt und die detailliert gesetzlich geregelt ist. Dass Untersuchungen externer Experten parallel zu anhängigen disziplinarrechtlichen und/oder strafprozessualen Ermittlungen gesetzlich festgelegte Zuständigkeiten und vor allem Schutzvorschriften auszuhebeln drohen, liegt auf der Hand. Strenge gesetzliche Regeln binden die zuständigen staatlichen Stellen als Normadressaten, nicht aber den zivilvertraglich bestellten externen Experten. Letzterem fehlt es nicht nur an einer verfassungsgemäßen Legitimation für seine Tätigkeit, er unterliegt im Gegensatz zur Staatsverwaltung auch nicht der Kontrolle durch das Parlament.

In aller Regel findet der Abschlussbericht des Experten oder der Expertenkommission den Weg in die Öffentlichkeit, insbesondere, wenn nach dem Untersuchungsergebnis keine oder nur geringe Anhaltspunkte für fehlerhaftes Vorgehen des Staatsministeriums vorliegen, das die Untersuchung in Auftrag gegeben hat. Und natürlich ist ein solcher Abschlussbericht ohne personenbeziehbare Daten von Beschäftigten des Freistaates oder Dritten kaum denkbar.

Möglichkeiten der Einbindung externer Dritter

Im Berichtszeitraum gab die Einsetzung einer unabhängigen Untersuchungskommission zur Aufklärung des sogenannten Munitionsskandals im Landeskriminalamt Anlass, sich zu diesen Fragen mit dem Sächsischen Staatsministerium des Innern (SMI) auseinanderzusetzen.

Im Ergebnis des Austauschs bestand Einigkeit darüber, dass die Verarbeitung personenbezogener Daten im Rahmen der Ausübung der Fach- und Dienstaufsicht durch die oberste Aufsichtsbehörde – das Staatsministerium – auf § 3 Sächsisches Datenschutzdurchführungsgesetz (SächsDSDG) in Verbindung mit §§ 4, 17 Sächsisches Verwaltungsorganisationsgesetz (SächsVwOrgG) gestützt werden kann.

Dabei ist für die aufsichtführende Behörde auch die Möglichkeit eröffnet, mit bestimmten Verarbeitungen personenbezogener Daten Auftragsverarbeiter zu betrauen, wobei die Vorgaben von Art. 28 DSGVO einzuhalten sind. Eine Funktionsübertragung dergestalt, dass dem Staatsministerium obliegende Aufgaben und zustehende Befugnisse Dritten zur weisungsfreien Behandlung nach eigenem Ermessen übertragen werden, ist ausgeschlossen.

Eine umfassende (Erst-)Erhebung von Daten durch Externe wäre im aktuell maßgeblichen Rechtsrahmen unzulässig; erst recht gälte dies für eine Beauftragung Dritter mit Aufgaben, deren Erfüllung der Gesetzgeber bestimmten staatlichen Stellen zugewiesen hat (etwa der Staatsanwaltschaft oder dem Landesamt für Verfassungsschutz).

Daraus folgt auch, dass externen Personen keine Weisungsbefugnisse gegenüber Beschäftigten öffentlicher Stellen des Freistaates zustehen. Diesen Personen gegenüber unterliegen Beschäftigte öffentlicher Stellen dementsprechend auch keinerlei Auskunftspflichten. Eventuelle anderslautende zivilvertragliche Absprachen sind unwirksam.

In diesem Punkt bestand zwischen meiner Behörde und dem Staatsministerium Einigkeit; ebenso zum Bestehen von Verschwiegenheitspflichten des Auftragsverarbeiters sowie zu dessen Pflicht zur Herausgabe sämtlicher Daten spätestens nach Beendigung der Tätigkeit.

Bei einer eventuellen Beauftragung externer Personen in künftigen Fällen sollte sich – wenn im Rahmen des Auftrags personenbezogene Daten verarbeitet werden (sollen) – das Vorgehen der einen Dritten beauftragenden verantwortlichen Stelle an diesen Grundsätzen orientieren.

Was ist zu tun?
Öffentliche Stellen dürfen eigene Aufgaben und Eingriffsbefugnisse nicht zur weisungsfreien Erledigung zivilvertraglich an Dritte übertragen. Die Einbindung Dritter in die behördliche Aufgabenerfüllung ist allenfalls im Wege und unter den engen Voraussetzungen der – weisungsgebundenen – Auftragsverarbeitung nach Art. 28 DSGVO zulässig.

4.2.2 Einsatz von Chatbots durch öffentliche Stellen

↗ Art. 6 und 28 DSGVO

Im Berichtsjahr gab es erstmals Anfragen von Kommunen, die für einfach gelagerte Anfragen von Bürgern sogenannte Chatbots einsetzen wollten oder sich zumindest mit der Frage des Einsatzes näher befasst haben. Ein Chatbot ist zunächst einmal eine neutrale Technologie, die schriftlich oder auch mithilfe von Spracherkennungssoftware mündlich gestellte Fragen einfacher Art analysiert und aus einem Fundus von standardisierten Antworten eine schnelle Hilfe für den Fragenden ermöglichen soll. Um einen solchen Chatbot sinnvoll betreiben zu können, ist es meist erforderlich, die Eingaben von Nutzern im laufenden Betrieb zu erheben und auszuwerten, damit die daraus gewonnenen Erkenntnisse in die Ergänzung, Erweiterung und Verbesserung der angebotenen Dienstleistung einfließen können. Diese Verarbeitung kann maschinell mit einer Form der künstlichen Intelligenz, meist sogenanntem „machine learning" oder auch manuell durch menschliche Bearbeiter erfolgen. In den allermeisten

Fällen wird aber eine maschinelle Komponente mit verwendet werden. Klar ist, dass sowohl Betrieb als auch Daten für die Verbesserung des Systems eine Verarbeitung personenbezogener Daten zur Folge hat und damit eine oder mehrere Rechtsgrundlagen erfordert.

Zunächst bedarf es einer informierten und transparenten Einwilligung in klarer Sprache für eine Nutzung des Chatbots. Einer weiteren Einwilligung bedarf es, wenn Daten von Nutzern für weitere Zwecke, zum Beispiel zur Verbesserung des Dienstes oder der Messung des Nutzungsverhaltens, verwendet werden sollen. Diese Einwilligung ist so zu gestalten, dass eine Nutzung des Chatbots auch ohne die Verarbeitung zu diesen Zwecken möglich ist. Sonderfälle der Einwilligung, wie die von Kindern, bei denen eine Einwilligung der Erziehungsberechtigten erforderlich ist, sind dabei zu berücksichtigen. Speicherdauer und Verarbeitungen müssen für alle Zwecke genau bezeichnet werden und sich ergebende Betroffenenrechte gewährleistet werden.

Werden besonders schutzwürdige Daten (beispielsweise automatisierte Auskünfte durch Gesundheitsämter zu Quarantänebestimmungen) verarbeitet, ist durch technisch-organisatorische Maßnahmen eine wirksame Verringerung der Risiken herbeizuführen, zum Beispiel durch schnellstmögliche Löschung oder Anonymisierung, Einschränkung von Zugriffsrechten, Verschlüsselung von Datenbanken oder andere geeignete Maßnahmen.

Wird ein solcher Dienst im Rahmen einer Auftragsverarbeitung eingesetzt, muss eine sorgfältige Prüfung des beauftragten Dienstleisters erfolgen. Insbesondere ist sicherzustellen, dass der Dienstleister die verarbeiteten Daten nur im Rahmen des Auftrags und nicht für eigene Zwecke verarbeitet. Für öffentliche Stellen ist eine solche Weitergabe von Daten für die Nutzung aufgrund des berechtigten Interesses Dritter ausdrücklich untersagt. Eine Datenverarbeitung „zur Verbesserung des Produktes" zugunsten des Herstellers muss klar ausgeschlossen sein. Ebenso muss die Verarbeitung innerhalb der Europäischen Union stattfinden. Dies gilt vor allem für eingesetzte Unterauftragsverarbeiter eines

Was ist zu tun?
Öffentliche Stellen bzw. durch diese verpflichtete Auftragnehmer müssen beim Einsatz von Chatbots oder ähnlicher Techniken sicherstellen, dass die Anforderungen der DSGVO eingehalten werden.

Auftragsverarbeiters. Nicht selten zeigt sich in der Praxis, dass der Auftragsverarbeiter seinen Sitz zwar in Europa hat, sich aber für die Auslieferung einzelner Komponenten eines global agierenden Content-Delivery-Networks bedient und damit eine Übermittlung von Nutzungsdaten in eine Cloud mit außereuropäischer Datenverarbeitung nicht wirksam ausgeschlossen ist.

4.2.3 Einsatz der Corona-Warn-App (CWA) durch öffentliche Stellen

↗ SächsCoronaNotVO

Von einer Hochschule wurde die Frage gestellt, ob für den Einsatz der Corona-Warn-App (CWA) ein Vertrag zur Auftragsverarbeitung erforderlich sei, wenn diese bei der Zutrittskontrolle von Lehr- und sonstigen Veranstaltungen der Hochschule im Rahmen der jeweils geltenden Corona-Schutzmaßnahmen Verwendung findet.
Die Frage ist insoweit zu verneinen, als dass ein solcher Vertrag gar nicht geschlossen werden kann, da es zu gar keiner Datenverarbeitung durch die Hochschule kommt. Die öffentliche Stelle erstellt über die Homepage der Corona-Warn-App lediglich die QR-Codes mit den Daten der jeweiligen Veranstaltung, mit deren Hilfe sich Nutzerinnen und Nutzer der App einchecken können und damit einer Kontakterfassung nach Sächsischer Corona-Notfall-Verordnung genügen. Der Freistaat Sachsen war das erste Bundesland, welches dieses datensparsame und auf Eigenverantwortung der Nutzerinnen und Nutzer basierende System in der Corona-Notfall-Verordnung des Landes als Ersatz für eine eigene Kontaktnachverfolgung normiert hat.
Bei der weiterhin parallel angebotenen manuellen Kontakterfassung oder bei Nutzung eigener Systeme, in denen Kontaktdaten von Besuchern von Veranstaltungen erfasst werden, sind die datenschutzrechtlichen Anforderungen in eigener Verantwortung sicherzustellen.

4.2.4 Videodolmetschen

↗ Art. 28 DSGVO

Im Berichtszeitraum erhielt mein Amtsvorgänger eine Anfrage eines behördlichen Datenschutzbeauftragten einer Kommune zum Einsatz von Videodolmetschern. Bei kurzfristigem Bedarf oder fehlender Verfügbarkeit von Dolmetschern, zum Beispiel in einer bestimmten Sprache, werden Videodolmetscher eingesetzt.

Er bat um Stellungnahme, ob es sich beim Einsatz von Videodolmetschern um Auftragsverarbeitung im Sinne des Art. 28 Datenschutz-Grundverordnung (DSGVO) handelt. Ein Referat der Kommune, das immer wieder kurzfristig Dolmetscher einsetzt, vertritt die Auffassung, dass keine Auftragsverarbeitung vorliege, weil es sich hier um eine freiberufliche Tätigkeit handele.

Im Bereich der Justiz wird das Videodolmetschen als Auftragsverarbeitung angesehen und wird in Abstimmung mit meiner Behörde in Justizvollzugsanstalten eingesetzt.

Nach meiner Auffassung ist die Inanspruchnahme von Videodolmetschern im Rahmen einer Auftragsverarbeitung möglich. Eine Auftragsverarbeitung liegt vor, da der Dolmetscher das Gesprochene in eine andere Sprache übersetzt. Anders ist es bei einem Gutachter, der eine eigene Wertung vornimmt. Letzteres ist hier jedoch nicht der Fall. Nicht erheblich für die Frage, ob es sich um eine Auftragsverarbeitung handelt, ist der Einwand, dass es sich beim Dolmetschen um eine freiberufliche Tätigkeit handelt.

Es sind die Anforderungen des Art. 28 DSGVO zu beachten. Werden von der Firma freie Mitarbeiter eingeschaltet, liegt ein Unterauftragsverhältnis vor, das ebenfalls den Anforderungen des Art. 28 DSGVO genügen muss.

4.3 Sicherheit der Verarbeitung

4.3.1 Nutzung von LernSax

↗ Art. 32 DSGVO

Tätigkeitsbericht 2020:
↗ sdb.de/tb2020

Im Tätigkeitsbericht 2020 hatte sich mein Amtsvorgänger unter „2.3.2 LernSax – die sächsische Schulcloud" (Seite 90f.) zur einwilligungsfreien Nutzung des LernSax geäußert. In einer Petition wurde ich nun darüber informiert, dass eine Lehrerin über LernSax einer Schülerin eine Nachricht geschickt hätte, wonach sie auf 4,5 stehen würde und gespickt hätte. Diese Nachricht sei an die gesamte Klasse geschickt worden. Die um Stellungnahme gebetene Schule räumte den Datenschutzverstoß ein. Dieser resultiere aus einem Versehen der Lehrerin. Diese hatte in LernSax auf eine Nachricht der Schülerin geantwortet und nicht bemerkt, dass diese Nachricht zwar von dieser persönlich gesendet wurde, dies aber aus der Klassengruppe heraus. Die Antwort der Lehrerin wurde dadurch automatisch für die ganze Gruppe und nicht nur die Schülerin sichtbar. Als sie dies bemerkte, wandte sie sich unverzüglich an den Support von LernSax, um die Nachricht löschen zu lassen. Schließlich entschuldigte sie sich in einem Gespräch bei der Schülerin und ihren Eltern. Vor diesem Hintergrund hat meine Behörde von weiteren Maßnahmen abgesehen.

4.4 Meldung von Datenschutzverletzungen

4.4.1 Zuwachs bei gemeldeten Datenpannen

↗ Art. 28, 32, 34, 83 DSGVO

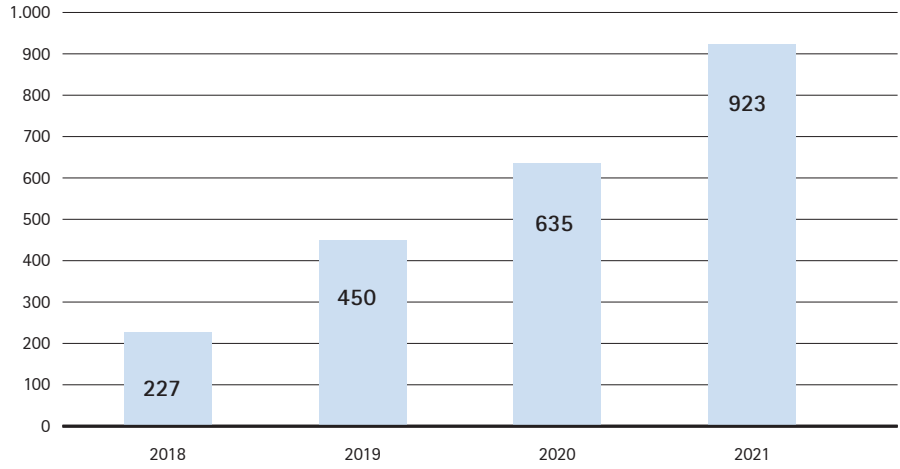
Nach Art. 33 Datenschutz-Grundverordnung (DSGVO) sind Verantwortliche verpflichtet, im Falle der Verletzung des Schutzes personenbezogener Daten unverzüglich und möglichst binnen 72 Stunden nach Bekanntwerden der Verletzung diese der Aufsichtsbehörde zu melden, es sei denn, dass die Verletzung des Schutzes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

aussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.
Im Berichtszeitraum sind 923 solcher Meldungen eingegangen. Im Vergleich zum vorjährigen Berichtszeitraum (635 Meldungen) entspricht dies einer Steigerung um rund 45 Prozent. Damit ist erneut eine erhebliche Zunahme der Meldungen von Datenschutzverletzungen zu verzeichnen.
Die folgenden Fallgruppen sind im Berichtszeitraum besonders häufig gemeldet worden:

Fehlversand

Wie bereits im vorjährigen Berichtszeitraum ist der Fehlversand eine der häufigsten Fallgruppen der gemeldeten Datenschutzverletzungen und macht rund 35 Prozent aller Meldungen aus. Ursachen für diese Vorfälle sind falsche Zuordnung von Unterlagen, fehlerhafte Kuvertierung oder schlicht Flüchtigkeitsfehler. In der Regel wird der fehlerhafte Versand dem Absender vom falschen Empfänger mitgeteilt und die Unterlagen vernichtet oder zurückgesandt, sodass in diesen Fällen zumeist nicht von einem hohen Risiko für die Betroffenen auszugehen ist.

Abbildung 1:
Meldungen von Datenschutzverletzungen



Offener E-Mail-Verteiler

Ein sehr wichtiger Aspekt des Datenschutzes ist die Sorgfalt. Insbesondere beim Versenden von E-Mails an größere Empfängergruppen wird diese oftmals vernachlässigt. Daher ist nach wie vor häufig der Versand von E-Mails (zum Beispiel Newsletter) über erkennbare E-Mail-Adressen im Kopie-Modus (Cc), anstatt im Blindkopie-Modus (Bcc) eine gemeldete Datenschutzverletzung, die in der Regel auf schlichte Unachtsamkeit des Absenders zurückzuführen ist. Auch wenn hierbei das Risiko für die Betroffenen oftmals als gering eingeschätzt werden kann, ist eine solche Datenschutzverletzung nach Art. 33 DSGVO meldepflichtig.

Verlust auf dem Postweg

Neben dem Fehlversand aufgrund des Verschuldens des Absenders gingen auch wieder zahlreiche Meldungen wegen des Verlustes von Postsendungen ein. Auch dies stellt eine meldepflichtige Datenschutzverletzung gem. Art. 33 DSGVO dar, soweit der Absender über den Verlust der Postsendung informiert wurde, was in der Regel durch den angegebenen Empfänger angestoßen wird, indem er sich über den Verbleib der erwarteten Postsendung informiert.

Verlust von Datenträgern

Ebenso kam es im Berichtszeitraum wieder zu Diebstählen oder dem Verlust von Datenträgern mit zum Teil sensiblen Daten. Besonders ärgerlich – weil vermeidbar – ist, dass die Datenträger in der Regel unverschlüsselt waren, sodass Angreifer oder Finder direkten Zugriff auf die Daten hatten. Um die Folgen so gering wie möglich zu halten, ist eine zwingende technisch-organisatorische Maßnahme bezogen auf Datenträger unter anderem die Verschlüsselung. Entsprechende Funktionen stellen bereits gängige Betriebssysteme oder frei zugängliche Software zur Verfügung. Wichtig ist bei der Verschlüsselung die Verwendung eines sicheren Passwortes. Neben der Verschlüsselung der Datenträger sind diese stets ordnungsgemäß zu verwahren bzw. zu transportieren,

Hinweise des BSI zum Generieren sicherer Passwörter:
↗ sdb.de/tb2112

und es sollten stets regelmäßige Backups durchgeführt werden, um die Verfügbarkeit der Daten zu gewährleisten. Häufig werden auf Speichermedien Datensicherungen vorgehalten oder Fotodokumentationen angelegt. Dies sind zum Beispiel in Kindertageseinrichtungen oder Arztpraxen besonders sensible Daten, sodass mit dem Verlust in der Regel ein hohes Risiko und damit verbunden ein erheblicher Schaden für die Betroffenen entstehen kann. Folge einer solchen Datenschutzverletzung mit hohem Risiko für die Betroffenen ist dann stets, dass der Verantwortliche neben der Meldung nach Art. 33 DSGVO zusätzlich die Betroffenen nach Art. 34 DSGVO zu benachrichtigen hat.

Datenschutzverletzungen durch Auftragsverarbeiter

In diesem Jahr gab es auch gehäuft Vorfälle, bei denen Auftragsverarbeiter von einem Datenschutzvorfall betroffen waren, welche im Rahmen des Auftragsverhältnisses Zugriff auf personenbezogene Daten hatten. Dies ist häufig der Fall, wenn Fremdunternehmen Software pflegen, Abrechnungen von Leistungen von externen Firmen übernehmen oder der Druck und Versand ausgelagert ist. Der Auftragsverarbeiter hat hier keine Entscheidungsbefugnis über die Daten und verfolgt mit den Daten auch keinen eigenen Geschäftszweck. Bei Datenschutzvorfällen bei einem Auftragsverarbeiter ist dieser gemäß Art. 33 Abs. 2 DSGVO dem Verantwortlichen gegenüber verpflichtet, dies unverzüglich zu melden, damit der Verantwortliche seiner Meldepflicht gegenüber der Aufsichtsbehörde gemäß Art. 33 Abs. 1 DSGVO oder möglicherweise sogar seiner Benachrichtigungspflicht nach Art. 34 Abs. 1 DSGVO überhaupt nachkommen kann.

So ging ein meldepflichtiger Vorfall eines Dienstleisters in meiner Behörde ein, bei welchem sächsische Unternehmen betroffen waren und benannt wurden. Aufgrund eines Missverständnisses einiger betroffener Unternehmen setzten diese als Verantwortliche keine eigene Meldung gegenüber meiner Behörde ab, sodass dem Meldeerfordernis erst infolge unserer Nachfrage nachgekommen wurde.

Cyberkriminalität

Rund ein Drittel der Meldungen von Datenschutzverletzungen, die im Jahr 2021 eingingen, sind auf die Fallgruppe der Cyberkriminalität zurückzuführen. Dieser unspezifische Begriff umfasst sämtliche Handlungen/Straftaten, die durch die Nutzung von Kommunikations- und Informationstechniken begangen werden.

Zu den besonderen Vorfällen im Bereich Cyberkriminalität zählten die Sicherheitslücken in Microsoft Exchange-Servern. Zahlreiche Meldungen gingen dazu zum Jahresanfang 2021 in meiner Behörde ein. Anfang März 2021 veröffentlichte Microsoft Sicherheitsupdates für diese Schwachstellen. Zugleich gab das Unternehmen bekannt, dass die Lücke bereits seit geraumer Zeit bestand und auch aktiv ausgenutzt wurde. Somit hatten Nutzer keine Garantie, dass allein durch eine unverzügliche Installation der Sicherheitsupdates jegliche Gefahr gebannt war. Darüber hinaus war es erforderlich zu überprüfen, ob eine Kompromittierung des Exchange-Servers möglicherweise bereits stattgefunden hatte.

Vorbeugende Maßnahmen

Prävention und Vorsorge sind die richtigen Mittel, um einer Datenschutzverletzung und damit verbundenen Risiken für Betroffene sowie der Meldepflicht gemäß Art. 33 DSGVO entgegenzuwirken. Folgende Vorkehrungen empfehle ich:

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

Im Zusammenhang mit der Meldepflicht von Datenschutzverletzungen nach 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 auf die für Meldefälle bestehende Dokumentationspflicht gemäß Art. 33 Abs. 5 DSGVO sowie auf die mögliche Pflicht der Benachrichtigung der betroffenen Person nach Art. 34 DSGVO hin.
Im Rahmen der Verpflichtung nach Art. 32 DSGVO hat der Verantwortliche grundsätzlich dafür Sorge zu tragen, dass die erforderlichen technischen und organisatorischen Maßnahmen umgesetzt und regelmäßig zu überprüfen sind, damit Datenschutzverletzungen, soweit es möglich ist, vermieden werden. Verstöße gegen Art. 32 DSGVO wären beispielsweise nicht installierte Sicherheitsupdates, fehlende Backups, fehlende Verschlüsselung, aber auch fehlende Sensibilisierungsmaßnahmen gegenüber Beteiligten.

Verstöße sowohl gegen Schutzmaßnahmen nach Art. 32 DSGVO als auch gegen formelle Anforderungen der Meldung bzw. Benachrichtigung gemäß Art. 33, 34 DSGVO können Gegenstand eines bußgeldrechtlichen Verfahrens nach 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 genannten Vorkehrungen zu prüfen und stets auf aktuellem Stand zu halten.

4.5 Datenschutzbeauftragter

4.5.1 Datenschutzbeauftragter als Beauftragter für Informationssicherheit

↗ Art. 37 DSGVO, SächsISichG

Das Sächsische Informationssicherheitsgesetz (SächsISichG) von 2019 verpflichtet staatliche Stellen, einen Beauftragten für Informationssicherheit zu ernennen; zum Teil sogar hauptamtlich. Aber auch nichtstaatliche öffentliche Stellen, wie beispielsweise Kommunen, sollen eine derartige Ernennung vornehmen. Eine kleinere sächsische Kommune wandte sich mit der Frage an meine Behörde, ob für eine entsprechende Ernennung auch der nach Art. 37 Datenschutz-Grundverordnung (DSGVO) benannte Datenschutzbeauftragte infrage käme.

Die Bestellung verschiedener anderer Beauftragter in Personalunion zum Datenschutzbeauftragten ist grundsätzlich problematisch. Der Beauftragte für Informationssicherheit ist dabei jedoch weniger kritisch zu betrachten, da Informationssicherheit und Datenschutz meist parallel laufen. Dies gilt auch vor dem Hintergrund, dass für die Informationssicherheit umfassende Sammlungen personenbezogener Daten verarbeiten werden, um Missbrauch zu entdecken. Auch Art. 32 DSGVO adressiert die Sicherheit der Verarbeitung und zudem in Absatz 1 Buchst. c) ausdrücklich die Verfügbarkeit. Anders stellt sich dies jedoch dar, wenn der Informationssicherheitsbeauftragte auch noch Aufgaben der Umsetzung, gar mit Budgetverantwortung, hat.

5 Internationaler Datenverkehr

5.1 Neue Standardvertragsklauseln

↗ Art. 28 DSGVO

Als Konsequenz aus dem Urteil des Europäischen Gerichtshofs vom 16. Juli 2020 – C-311/18 – („Schrems II") hat die Europäische Kommission neue Standardvertragsklauseln erlassen. Alte Standardvertragsklauseln dürfen für Neuverträge keine Verwendung mehr finden. Bis zum 27. Dezember 2022 haben Altverträge auf Grundlage der bisherigen Standardvertragsklauseln geändert zu sein. Zusätzlich sind Altverträge in Bezug auf die Rechtslage und Rechtspraxis in dem Drittland und das gewährleistete Schutzniveau zu überprüfen.

Zu den neuen Standardvertragsklauseln hat die Europäische Kommission einen Durchführungsbeschluss erlassen, Durchführungsbeschluss (EU) 2021/914 der EU Kommission vom 4. Juli 2021, Aktenzeichen C (2021) 3972, Amtsblatt EU Nr. L 199/31 vom 7. Juni 2021.

Die neuen Standardvertragsklauseln berücksichtigen die gebräuchlichen Datenübermittlungen an Verantwortliche in Drittländer und die Inanspruchnahme von Auftragsverarbeitern und Sub-Auftragsverarbeitern. Es bleibt aber weiterhin erforderlich, die Rechtslage und Rechtspraxis des Drittlands zu prüfen und gegebenenfalls zusätzliche Schutzmaßnahmen zu ergreifen. Soweit eine Gewährleistung des Schutzniveaus nicht erreicht werden kann, ist von einer Übermittlung in das Drittland Abstand zu nehmen.

Kommen Auftragsverarbeitungsverträge zum Einsatz, berücksichtigen die neuen Standardvertragsklauseln die Anforderungen gemäß Art. 28 Datenschutz-Grundverordnung (DSGVO).

EUR-Lex:
↗ sdb.de/tb2113

Was ist zu tun?
Die neuen Standardvertragsklauseln sind unverändert, gegebenenfalls als Teil eines Vertragswerks, zu verwenden. Nur dann tritt Genehmigungsfreiheit ein.

6 Sächsische Datenschutzbeauftragte

6.1 Zuständigkeit und Anforderungen an Beschwerden

6.1.1 Modellprojekte nach der Sächsischen Corona-Schutz-Verordnung

↗ §§ 8g, 36 SächsCoronaSchVO; Art. 51 Abs. 1 DSGVO, Art. 57 DSGVO

Nachdem sich der Freistaat Sachsen seit Dezember 2020 im Lockdown befunden hatte und das gesellschaftliche öffentliche Leben nur noch eingeschränkt möglich war, sollten mit der Sächsischen Corona-Schutz-Verordnung (SächsCoronaSchVO) vom 5. März 2021 Lockerungen ermöglicht werden.

Idee der Modellprojekte

Dazu sollten unter anderem sogenannte Modellprojekte beitragen. Gemäß § 8g der SächsCoronaSchVO vom 5. März 2021 konnte der zuständige Landkreis oder die zuständige kreisfreie Stadt für das Gebiet oder ein Teilgebiet einer Gemeinde Abweichungen von den einschränkenden Regelungen der SächsCoronaSchVO im Rahmen von Modellprojekten zulassen. Diese Modellprojekte sollten gemäß der Verordnung der Untersuchung und der Entwicklung des Infektionsgeschehens, der diskriminierungsfreien Erprobung von Corona-Testkonzepten und von digitalen Systemen zur datenschutzkonformen Verarbeitung von personenbezogenen Daten und ihre Übermittlung an das Gesundheitsamt zur kurzfristigen und vollständigen Kontaktnachverfolgung dienen.

Anfangs sah die Genehmigung der Modellprojekte durch die zuständigen Landkreise und kreisfreien Städte die Zustimmung meiner Behörde vor. In späteren Fassungen der SächsCoronaSchVO sollte zunächst noch das Einvernehmen und später nur noch das Benehmen mit meiner Dienststelle hergestellt werden. Neben der Beteiligung meiner Behörde hatte die zuständige Genehmigungsbehörde, das heißt der Landkreis oder die kreisfreie Stadt, in diesem mehrstufigen Verwaltungsverfahren auch die oberste Landesgesundheitsbehörde zu beteiligen. Auch diese Beteiligten wurden im Laufe der Anpassungen der SächsCoronaSchVO geändert. So musste zum Beispiel laut der SächsCoronaSchVO vom 29. März 2021 (in der konsolidierten Fassung vom 16. April 2021) das Sächsische Staatsministerium für Soziales und Gesellschaftlichen Zusammenhalt und die bei der Staatsministerin für Kultur und Tourismus im Staatsministerium für Wissenschaft, Kultur und Tourismus eingerichtete Fachkommission beteiligt werden.

Schwierigkeiten bei den Verfahren und den Projekten

Diese Regelung stellte meine Behörde vor große Herausforderungen, insbesondere in personeller Hinsicht, aber auch in Bezug auf die nichtabgestimmte Verfahrensweise zwischen den unterschiedlichen Verfahrensbeteiligten, wegen der unklaren Antragsvoraussetzungen, aber auch in Bezug auf die Vielgestaltigkeit der Projekte, die eine umfangreiche und sorgfältige Einzelfallprüfung erforderlich machten. Dabei hatte sich meine Dienststelle mit einer Antragsflut, größeren Fallmengen, auseinanderzusetzen.

Die Beschränkungen der Gewerbebetriebe durch die Corona-Maßnahmen, wie zum Beispiel die Schließung der Hotel- und Gastbetriebe sowie Restaurants und auch das Verbot von Veranstaltungen, führten nach meiner Beobachtung dazu, dass die Modellprojekte als ein Instrument zur Umgehung der Schutzmaßnahmen bzw. deren Öffnung und nur sekundär der Erprobung von digitalen Systemen zur datenschutzkonformen Verarbeitung personenbezogener Daten genutzt werden sollten.

Dies belegt eine Vielzahl von Modellprojektanträgen von Vereinen, Unternehmen und Veranstaltern, insbesondere zum Beispiel aus dem von Einschränkungen stark betroffenen Veranstaltungsbereich, sowie der geplante Einsatz von digitalen Systemen, die häufig weit entfernt von datenschutzrechtlichen Standards, kurzfristig entwickelt und in Betrieb genommen werden sollten. Regelmäßig waren notwendige Verfahrensbeschreibungen, die die Datenverarbeitungsprozesse darstellen – insbesondere wer zu welchem Zweck und Zeitpunkt welche Daten genau erhebt, wer Daten zu welchem Zweck weitergibt, wann die Daten gelöscht werden, wie betroffene Personen informiert werden, welche technischen und organisatorischen Maßnahmen zum Schutz der Daten ergriffen wurden – gar nicht vorhanden oder unzureichend, zum Teil rudimentär.

Konstruktive Mängel bei der Rechtssetzung

Aufgrund der fehlenden Beteiligung meiner Behörde bei der Einführung dieser Regelung sowie der Kurzfristigkeit, mit der diese Regelung in Kraft trat, waren weder die Antragsvoraussetzungen noch das Verfahren zwischen den zu beteiligenden Genehmigungsbehörden abgestimmt und prozedural strukturiert.

Meine Behörde vertritt die Auffassung, dass es sich bei der Frage der Durchführung der Modellprojekte primär um infektionsschutzrechtliche und nicht um datenschutzrechtliche Angelegenheiten handelte, die grundsätzlich von der jeweiligen zuständigen Gesundheits- oder Genehmigungsbehörde zu entscheiden wäre. Auch wenn die Modellprojekte regelmäßig datenschutzrechtliche Problemstellungen aufwiesen, ist eine Beteiligung meiner Behörde nach der Datenschutz-Grundverordnung (DSGVO) in dieser Form nicht vorgesehen. Inwieweit eine derartige Aufgabenzuweisung an meine Behörde durch den sächsischen Verordnungsgeber europarechtskonform ist, vgl. Art. 51 Abs. 1, Art. 57 DSGVO, hätte durch den Sächsischen Verordnungsgeber vertieft geprüft werden müssen.

Die Aufgaben meiner Behörde werden durch die Datenschutz-Grundverordnung bzw. formelles Recht abschließend geregelt. Eine Prüfung der Modellprojektanträge erfolgte seitens meiner Behörde gleichwohl.

Die Vorschriften der SächsCoronaSchVO zu den Modellprojekten bezüglich der Beteiligung meiner Behörde waren dabei nicht systemgerecht bzw. nicht mit der europarechtlichen Verordnung abgestimmt, da meine Behörde örtlich nur gegenüber den in Sachsen gelegenen Verantwortlichen und Auftragsverarbeitern aufsichtsbefugt ist. Auch eine sachliche Zuständigkeit meiner Behörde gegenüber Modellprojektantragstellern, die selbst keine datenverarbeitenden Stellen sind, ist nicht gegeben. Diese sind gegenüber meiner Behörde nicht pflichtig, können nicht beauflagt und kontrolliert werden. Hinzu kommt noch eine mögliche Kollision aufsichtlicher Zuständigkeiten mit spezifischen Aufsichtsbehörden, zum Beispiel bei kirchlichen Stellen, für die meine Behörde ebenso nicht zuständig ist. Die Implikationen sind jedenfalls seitens des Verordnungsgebers unberücksichtigt geblieben, hatten sich jedoch in der Bearbeitung der Modellprojektanträge sehr schnell gezeigt und erhebliche Auswirkungen auf das Verfahren gehabt, insbesondere bezüglich der Beteiligung weiterer Datenschutzaufsichtsbehörden und der Bearbeitungsdauer. Festzuhalten blieb zudem, dass neben den europarechtlich zugewiesenen Aufgaben für eine Beteiligung in formellen gestuften Verwaltungsverfahren personell und sachlich die Ressourcen in meiner Behörde fehlten.

Was ist zu tun?
Soweit der sächsische Gesetz- oder Verordnungsgeber beabsichtigt, automatisierte Verfahren in Projekten zu erproben, kann der Sächsischen Datenschutzbeauftragten das angezeigt werden. Auf diese Weise kann auch eine Beteiligung erfolgen. Eine datenschutzrechtliche und informationssicherheitsrechtliche Qualität automatisierter Verfahren ist hingegen primär seitens der Projektverantwortlichen abzusichern.

Resümee

Ende April 2021 wurde das Infektionsschutzgesetz geändert. Aufgrund der darin festgelegten Beschränkungen (sogenannte „Bundesnotbremse“) war die Realisierung der Modellprojekte aufgrund der hohen Inzidenzzahlen ohnehin nicht mehr durchführbar. Nach dem Auslaufen der Bundesnotbremse konnten aufgrund der zuvor beschriebenen Problematik nur vereinzelt Modellprojekte durchgeführt werden. Nach meiner Überzeugung wurde aufgrund der zuvor beschriebenen Umstände das mit den Modellprojekten ver-

knüpfte Ziel verfehlt. Das betraf sowohl die Entwicklung von digitalen Systemen zur datenschutzkonformen Verarbeitung von personenbezogenen Daten als auch ihre Übermittlung an das Gesundheitsamt zur kurzfristigen und vollständigen Kontaktnachverfolgung.

6.1.2 Datenverarbeitung eines Jugendamts im Rahmen eines familiengerichtlichen Verfahrens

↗ DSGVO, SGB VIII

Das Verfahren der vorläufigen Aufnahme und Unterbringung eines Kindes oder Jugendlichen in einer Notsituation durch das Jugendamt ist in § 42 Achtes Buch Sozialgesetzbuch (SGB VIII) geregelt. Widersprechen die Personensorge- oder Erziehungsberechtigten einer solchen Inobhutnahme oder sind sie nicht erreichbar, so hat das Jugendamt eine Entscheidung des Familiengerichts über die erforderlichen Maßnahmen zum Wohl des Kindes oder des Jugendlichen herbeizuführen.
§ 42 SGB VIII regelt dabei auch die Möglichkeit, ein Kind/einen Jugendlichen bei einer geeigneten Person vorläufig unterzubringen.
Die Mitwirkung in Verfahren vor dem Familiengericht nach § 50 SGB VIII gehört nach § 2 Abs. 3 u. 6 SGB VIII zu den Aufgaben der Kinder- und Jugendhilfe. Insoweit ist das Jugendamt berechtigt, in Verfahren des Familiengerichts zur Entscheidung einer Inobhutnahme mitzuwirken, also auch zu der Frage, wer konkret als geeignete Person für eine angedachte Inobhutnahme im Einzelfall angesehen werden kann. Das Jugendamt ist daher berechtigt, hinsichtlich der Frage der Geeignetheit eine konkrete, personenbezogene Stellungnahme zu der fraglichen Person gegenüber dem Familiengericht abzugeben. Eines Zustimmungserfordernisses der betroffenen Person bedarf es dazu nicht.
Welche fachlichen Anforderungen für eine Inobhutnahme bei einer geeigneten Person im Einzelnen vorausgesetzt werden und ob diese in Bezug auf ihre Person konkret und sachlich

richtig gewertet worden sind, ist in der Sache eine fachrechtliche, jedoch keine datenschutzrechtliche Frage, sodass dies einer Überprüfung durch meine Behörde entzogen ist.

6.1.3 Verstoß gegen die Impressumspflicht

↗ § 1 Abs. 2 Sätze 2 und 3 Sächsisches Gesetz zur Durchführung des Medienstaatsvertrages und des Rundfunkbeitragsstaatsvertrages, § 106 MStV

Immer wieder beinhalten bei mir eingehende Beschwerden (auch) einen Verweis auf ein fehlendes, unvollständiges oder falsches Impressum auf einer Internetseite. So trat in einem Fall ein Hauseigentümer an mich heran und schilderte, dass fälschlicherweise auf der Facebook-Fanpage eines Gewerbebetriebs die Adresse seines Mietshauses als Geschäftsadresse angegeben sei. Der Hauseigentümer sah darin die Gefahr, dass mögliche Mietinteressenten darauf aufmerksam und dadurch verprellt werden könnten. Wie sich herausstellte, hatte der Firmeninhaber bis vor ein paar Jahren in dem Mietshaus seine private Wohnung.
Zunächst begehrte der Hauseigentümer ein Eingreifen meiner Behörde auf datenschutzrechtlicher Grundlage, was mein Amtsvorgänger unter Verweis auf die fehlende Anwendbarkeit der Datenschutzvorschriften ablehnen musste. In der Folge machte der Hauseigentümer wegen der unrichtigen Adressangabe einen Verstoß gegen die Impressumspflicht geltend und wollte wissen, wohin er sich diesbezüglich wenden müsse.

Zuständigkeit neu geregelt

Mein Amtsvorgänger hatte sich in seinem Tätigkeitsbericht für den Berichtszeitraum 1. April 2017 bis 31. Dezember 2018 (6.1.2, Seite 230f.) bereits mit der Impressumspflicht und der Frage der zuständigen Behörde beschäftigt. Damals verwies er bei möglichen Verstößen gegen die Anbieterkennzeichnungspflicht an die Landesdirektion Sachsen. Der Sächsische Gesetzgeber hat die Zuständigkeitsfrage für alle Telemedien betreffenden Sachverhalte jedoch zwischenzeitlich neu geregelt. Der den damaligen Ausführungen zugrunde liegende

Rundfunkstaatsvertrag wurde im November 2020 vom Medienstaatsvertrag abgelöst. Nach diesem liegt die Zuständigkeit für bundesweit ausgerichtete Angebote bei der Landesmedienanstalt des jeweiligen Bundeslandes (§ 106 Medienstaatsvertrag). Im Freistaat Sachsen ist die Sächsische Landesanstalt für privaten Rundfunk und neue Medien, Ferdinand-Lassalle-Straße 21, 04109 Leipzig, als Landesmedienanstalt die zuständige Aufsichts- sowie auch Verwaltungsbehörde bei Ordnungswidrigkeiten (§ 1 Abs. 2 Sätze 2 und 3 Sächsisches Gesetz zur Durchführung des Medienstaatsvertrages und des Rundfunkbeitragsstaatsvertrages). Ob in dem geschilderten Fall ein Bußgeldtatbestand erfüllt ist, lässt sich wegen fehlender Zuständigkeit meiner Behörde nicht beurteilen. Dem betroffenen Hauseigentümer dürfte es aber in erster Linie darum gehen, dass sein Mietobjekt nicht in Zusammenhang mit einem Gewerbebetrieb gebracht wird, was die Attraktivität seines Wohnungsangebots zu schmälern geeignet gewesen sein könnte.

Was ist zu tun?
Für die Einhaltung der Impressumpflicht bei Telemedien ist in Sachsen die Sächsische Landesanstalt für privaten Rundfunk und neue Medien aufsichtlich und als Bußgeldbehörde zuständig. Die Sächsische Datenschutzbeauftragte prüft die Anbieterkennzeichnungspflicht hingegen nicht, ist aber für die Erfüllung der Informationspflicht nach Art. 13 und 14 DSGVO zuständig.

6.1.4 Private Rechtsdurchsetzung und Schadensersatz bei Datenschutzverstößen

↗ §§ 3, 3a, 8 UWG; Art. 12ff., 15, 20, 57, 82 DSGVO

Datenschutzkonformes Verhalten (Datenschutz-Compliance) ist eine zentrale Pflicht jedes datenschutzrechtlich Verantwortlichen. Dieser kennt die Umstände der konkreten Datenverarbeitung am besten und hat direkten Einfluss darauf. Dies ist die wichtigste Ebene der Rechtsdurchsetzung. Auf eine Compliance durch die Verantwortlichen in der Fläche, Breite und Tiefe ist die Rechtsgemeinschaft angewiesen. Entsprechend stellt die Rechtsordnung ein breites Spektrum von Durchsetzungsmechanismen zur Verfügung. Entscheidend sind dabei die so generierten Anreize für die Verantwortlichen, die Datenschutzregeln einzuhalten. Praktisch bedeutsam ist dabei, dass die Sanktionen für Datenschutzverstöße schwerer wiegen müssen als die zusätzlichen Gewinne, die der Verantwortliche durch die Außerachtlassung seiner datenschutzrechtlichen Pflichten erzielen kann.

Bei Verstößen gegen das Datenschutzrecht drohen daher empfindliche Sanktionen – Bußgelder bis zu 20 Millionen Euro bzw. 4 Prozent des weltweiten Jahresumsatzes und bis zu drei Jahren Freiheitsstrafe.

Parallel zu derartigen hoheitlichen Sanktionsmöglichkeiten bestehen Ansprüche der von der rechtswidrigen Datenverarbeitung Betroffenen auf Ersatz ihrer materiellen und immateriellen Schäden daraus, Art. 82 Datenschutz-Grundverordnung (DSGVO).

Unabhängig von Schaden und Sanktionen bestehen auch direkte Ansprüche des Betroffenen und – hinsichtlich Datenschutznormen, die gleichzeitig eine Marktverhaltensregelung im Sinne des § 3a des Gesetzes gegen den unlauteren Wettbewerb (UWG) darstellen – auch von Wettbewerbern und anderen zur Rechtsdurchsetzung Zugelassenen.

Teilweise sind erste eigene Schritte des Betroffenen schon Voraussetzung für ein behördliches Verfahren.

Daneben hat die private Rechtssetzung verschiedene Vorzüge, nicht zuletzt hinsichtlich Schnelligkeit, Reichweite der Anspruchsdurchsetzung und Breitenwirkung auf die Compliance in der Fläche. Insoweit komplementiert die private Rechtsdurchsetzung die behördliche.

In verwandten Rechtsgebieten weist die private Rechtsdurchsetzung eine substanzielle, vielfach zunehmende Bedeutung auf. Im Datenschutzrecht zeichnet sich bereits heute ab, dass die DSGVO Grundlage einer ähnlichen Entwicklung werden dürfte. Auf diese Art vervielfachen sich die Mittel zur Durchsetzung des Datenschutzrechts, was wiederum den Schutzzwecken des Datenschutzrechts zugutekommt.

(Beweisbare) Geltendmachung der Betroffenenrechte als Verfahrens-Vorbedingung

Häufig fordern Betroffene von mir, ihre Betroffenenrechte gegenüber den tatsächlichen Verantwortlichen geltend zu machen bzw. ihre entsprechenden Ansprüche direkt zu erfüllen.

Die DSGVO sieht jedoch für die Mehrzahl der Betroffenenrechte nach Art. 12ff. zunächst eine Geltendmachung der Ansprüche direkt gegenüber dem Verantwortlichen vor; dies gilt insbesondere für das Recht auf Auskunft und Kopie, Art. 15, 20 DSGVO. Entsprechend kann ich regelmäßig erst tätig werden, wenn der Verantwortliche beweisbar (oder zumindest plausibel belegt) entsprechende Anfragen des Betroffenen nicht (oder nicht fristgemäß) erfüllt.

In einer Vielzahl derartiger Beschwerdefälle erledigt sich der Beschwerdegegenstand, wenn der Betroffene auf das Erfordernis einer (beweisbaren) Geltendmachung seiner Rechte gegenüber dem Verantwortlichen hingewiesen wird und dies nachholt.

Das falsche Abstreiten durch einen Verantwortlichen, entsprechende Anfragen erhalten zu haben, stellt demgegenüber einen eigenständigen schweren, bußgeld- bzw. strafbewehrten Datenschutzverstoß dar, zusätzlich zu dem damit regelmäßig ebenfalls vorliegenden Fristversäumnis.

Die falsche Behauptung von Tatsachen gegenüber der Aufsichtsbehörde greift die Aufsicht in ihren Wurzeln an. Entsprechend fänden derartige (Verdachts-)Fälle meine besondere Aufmerksamkeit und würden besondere Verfolgungspriorität genießen.

Soweit in Bezug auf einen Verantwortlichen die Beschwerdelage den Verdacht aufdrängt, dass dieser empfangene Anfragen unbeantwortet lässt bzw. unterschlägt, bin ich zu entsprechenden Durchsuchungen befugt.

Bei (vorsätzlichen) Falschbehauptungen gegenüber der Behörde durch (angeblich) Betroffene oder Hinweisgeber liegt regelmäßig eine nach § 164 Strafgesetzbuch strafbare Falsche Verdächtigung vor. Falsche Angaben seitens des Verantwortlichen sind bußgeldbewehrte Verstöße gegen das Kooperationsgebot und die Auskunftspflicht und können unter anderem nach § 42 Bundesdatenschutzgesetz (BDSG) strafbar sein. Soweit sich der Verdacht erhärtet, gebietet die Bedeutung wahrheitsgemäßer Auskünfte an die Aufsichtsbehörde für die Aufsicht, entsprechende Strafverfolgung zu veranlassen.

Vorzüge privater Rechtsdurchsetzung

Sämtliche individuellen Rechte aus dem Datenschutzrecht stehen dem Betroffenen direkt zu, können also unmittelbar vor den Zivilgerichten geltend gemacht werden. Daneben stehen unter anderem Wettbewerbern direkte Unterlassungsansprüche gegen Verantwortliche zu, die im Wettbewerb gegen marktverhaltensregelnde Vorschriften des Datenschutzrechts verstoßen.

Eine derartige private Rechtsdurchsetzung weist eine Reihe von Vorzügen auf.

Das ist besonders augenfällig in Bereichen, in denen die Behördenzuständigkeit und die Reichweite des Datenschutzrechts den problematischen Sachverhalt nicht oder nur teilweise umfasst.

Dafür spricht insbesondere die teilweise erheblich schneller mögliche Rechtsdurchsetzung durch Zivilrechtsmittel wie einstweilige Anordnungen und Abmahnungen für eine private Rechtsdurchsetzung.

Auch ist meist meine Behörde räumlich weiter von dem Ort vermuteter Datenschutzverstöße entfernt als der Betroffene und die örtlich zuständigen Zivilgerichte, was die Ermittlung des Sachverhalts und möglicher Lösungsmöglichkeiten erleichtern kann.

Ein durch Datenschutzverstöße beeinträchtigter Betroffener ist in der Lage, den Verantwortlichen vor dem für seinen eigenen Wohnsitz zuständigen Gericht in Anspruch zu nehmen, ohne eine Entscheidung der möglicherweise zurückhaltenden Aufsichtsbehörde am Hauptsitz des Verantwortlichen abzuwarten.

Schließlich kann die belastbare gerichtliche Feststellung, dass für bestimmte Datenschutzverstöße ein Schadensersatz geschuldet ist, entsprechende Praktiken schnell und wirksam auch in der Breite abstellen. Zwar wirkt ein entsprechendes Urteil nur zwischen den Parteien. Allerdings ist die Reichweite eines gut begründeten Schadensersatzurteils nicht auf die Parteien oder den Zuständigkeitsbereich des erkennenden Gerichts beschränkt. Vielmehr kann ein solches Ausstrahlungswirkungen entfalten, die mit behördlichen

Entscheidungen nur begrenzt bewirkt werden können. Denn die begrenzten Ressourcen der Aufsichtsbehörden sind bekannt und beeinflussen teilweise Standortentscheidungen von datenverarbeitenden Unternehmen.
Zusätzlich haben Schadensersatzurteile den Vorzug, dass der Geschädigte direkt einen Ausgleich für den erlittenen Schaden erhält, während Behördenentscheidungen für den Betroffenen hinsichtlich in der Vergangenheit liegender Verstöße allenfalls immaterielle Genugtuung und Grundlage einer Schadensersatzforderung sein können.

Beispiel: Videoüberwachung durch Nachbarn

Beschwerden über Videoüberwachung seitens des Nachbarn scheitern häufig daran, dass ein Datenschutzverstoß nicht ermittelbar ist. Denn die Anwendung der Datenschutzgesetze setzt eine konkrete ungerechtfertigte Verarbeitung personenbezogener Daten voraus. Die datenschutzrechtlichen Grenzen zulässiger Videoüberwachung über das eigene Grundstück hinaus sind zwar eng; eine Überwachung des Nachbarn ist insoweit unzulässig (vgl. auch 2.2.52.2.5).
Die Ermittlungsbefugnisse meiner Behörde sind in Bezug auf Wohnräume jedoch begrenzt. Insbesondere bei fernsteuerbaren Videokameras und sogenannten Domekameras kann eine meinerseits überprüfte, datenschutzrechtlich zulässige Videografie auch ohne besonderen Aufwand so verändert werden, dass nach Veränderung des Aufnahmefeldes Datenschutzverstöße stattfinden. Für Kamera-Attrappen bin ich schließlich mangels Datenverarbeitung schon unzuständig.
Ein nachbarschaftsrechtlicher Unterlassungsanspruch hingegen kann auch dann bestehen, wenn Dritte eine Überwachung durch Überwachungskameras nur objektiv ernsthaft befürchten müssen („Überwachungsdruck"). Dies schließt insbesondere auch Attrappen mit ein.
Dabei ist zwar der genaue Einzelfall zu würdigen. In Verwaltungs- und Ordnungswidrigkeitenverfahren muss jedoch im Kern die Behörde den Nachweis eines Datenschutzverstoßes führen. Demgegenüber ist im Nachbarschaftsrechtsstreit der-

jenige in erheblichem Maße darlegungs- und beweisbelastet, der die Kamera oder Kamera-Attrappe einsetzt.
Die etablierten nachbarschaftsrechtlichen Vorgaben der Zivilgerichte sind insoweit stringent:

> „Die Befürchtung, durch vorhandene Überwachungsgeräte überwacht zu werden, ist dann gerechtfertigt, wenn sie aufgrund konkreter Umstände als nachvollziehbar und verständlich erscheint, etwa im Hinblick auf einen eskalierenden Nachbarstreit oder aufgrund objektiv Verdacht erregender Umstände. Liegen solche Umstände vor, kann das Persönlichkeitsrecht des (vermeintlich) Überwachten schon aufgrund der Verdachtssituation beeinträchtigt sein. Allein die hypothetische Möglichkeit einer Überwachung durch Videokameras und ähnliche Überwachungsgeräte beeinträchtigt hingegen das allgemeine Persönlichkeitsrecht derjenigen, die dadurch betroffen sein könnten, nicht. Deshalb ist die Installation einer Überwachungsanlage auf einem privaten Grundstück nicht rechtswidrig, wenn objektiv feststeht, dass dadurch öffentliche und fremde private Flächen nicht erfasst werden, wenn eine solche Erfassung nur durch eine äußerlich wahrnehmbare technische Veränderung der Anlage möglich ist und wenn auch sonst Rechte Dritter nicht beeinträchtigt werden."
>
> Bundesgerichtshof (BGH), Urteil vom 16.03.2010 - VI ZR 176/09; vgl. etwa auch Landgericht Frankenthal (Pfalz), Urteil vom 16.12.2020 - 2 S 195/19

> „Bei der Installation von Videoüberwachungsanlagen auf einem Privatgrundstück muss sichergestellt sein, dass weder angrenzende öffentliche Bereiche noch benachbarte Privatgrundstücke von den Kameras erfasst werden. Etwas anderes gilt in Einzelfällen lediglich dann, wenn bei einer Abwägung mit dem Persönlichkeitsrecht ein überwiegendes Interesse des Betreibers der Anlage angenommen werden kann."
>
> Landgericht Koblenz, Beschluss vom 5.09.2019 - 13 S 17/19

Entlang dieser etablierten Rechtsprechungslinien kann der (möglicherweise datenschutzrechtlich nicht) betroffene Nachbar im einstweiligen Verfügungsverfahren innerhalb weniger Tage vom lokal zuständigen Gericht einen sofort durchsetzbaren Titel erlangen und nötigenfalls mit Unterstützung des Gerichtsvollziehers zeitnah vollstrecken lassen, ohne dass es auf Datenschutzverstöße und deren Nachweis ankäme.
Soweit Betroffene den Beschwerdeweg vor meine Behörde wählen, ist andererseits häufig schon die – umfangreicher erforderliche – Sachverhaltsermittlung deutlich zeitintensiver. Falls kein Datenschutzverstoß festgestellt werden kann, bleibt die private Rechtsdurchsetzung nach Durchführung eines behördlichen Verfahrens die einzige Möglichkeit für Nachbarn, die sich gegen Kameras bzw. Attrappen und den davon ausgehenden Überwachungsdruck wehren möchten.
Letztlich wird angesichts der weitreichenden nachbarschaftsrechtlichen Vorgaben für Videografie eine gerichtliche Auseinandersetzung oftmals unnötig sein. Die direkte Ansprache des videografierenden Nachbarn kann die (weitere) Verschlechterung des Nachbarschaftsverhältnisses vermeiden helfen, die aus der Beschwerde bei der Aufsichtsbehörde oder einem Gang vors Gericht folgen kann. Daneben ist für sächsische Sachverhalte insbesondere auf das Verfahren vor dem Friedensrichter hinzuweisen, der für solche Nachbarschaftsstreitigkeiten eine niederschwellige und konsensuale Konfliktlösungsmöglichkeit bietet.

Beispiel: Datenschutz im Bereich des Presse- und Medienrechts

Meine Aufsichts- und Eingriffsbefugnisse im Bereich journalistischer Tätigkeiten sind durch § 11a Satz 4 Sächsisches Gesetz über die Presse (SächsPresseG) in Verbindung mit Art. 85 DSGVO ganz erheblich eingeschränkt.
Danach bin ich nicht befugt, Unternehmen und Hilfsunternehmen der Presse datenschutzaufsichtlich zu kontrollieren, soweit diese personenbezogene Daten zu journalistischen oder literarischen Zwecken verarbeiten. Wegen der Bedeutung des Medienprivilegs für den öffentlichen Diskurs und

die Funktionsfähigkeit der Demokratie ist diese Ausnahme weit auszulegen und grundsätzlich unabhängig von journalistischer Qualität oder Unabhängigkeit.

Durch jene Norm sind auch die Betroffenenrechte aus der DSGVO insoweit stark eingeschränkt. Allerdings besteht eine Reihe presse- bzw. medienrechtlicher Ansprüche, die Betroffenen teilweise verwandte Ansprüche verleihen, wenn auch angesichts der Bedeutung der Presse-, Informations- und Meinungsfreiheit in eingeschränktem Maße.

Die presse- und medienrechtlichen Ansprüche auf Unterlassung, Gegendarstellung, Widerruf und Berichtigung einer bestimmten Berichterstattung sowie Schadensersatz haben teilweise ähnliche Wirkungen wie die entsprechenden datenschutzrechtlichen Ansprüche.

Sie sind jedoch vollkommen unabhängig vom Datenschutzrecht und können ausschließlich privat durchgesetzt werden. Wenn es sich hier auch nicht um eine Durchsetzung des Datenschutzrechts handelt, so dienen diese Ansprüche jedoch eng verwandten Schutzzwecken und füllen insoweit eine durch die Ausnahmeregelung entstehende Schutzlücke.

Beispiel: Unlauterer Wettbewerb durch Datenschutzverstöße

Verstöße gegen das Datenschutzrecht können unlautere Handlungen im Wettbewerb darstellen. Mitbewerber, entsprechende rechtsfähige Verbände, qualifizierte Einrichtungen im Sinne des Unterlassungsklagengesetzes sowie die Industrie-/Handels-/Handwerkskammern können gegen den Verantwortlichen für derartige Rechtsverstöße grundsätzlich selbstständig und aus eigenem Recht vorgehen, §§ 3, 3a, 8 UWG. Eine datenschutzrechtliche Selbstbetroffenheit ist nicht erforderlich.

Insoweit ist zwar umstritten, ob und welche datenschutzrechtlichen Regeln eine sogenannte Marktverhaltensregelung darstellen und entsprechende lauterkeitsrechtliche Unterlassungs- und Schadensersatzansprüche begründen. Allerdings hat sich hier eine recht weitreichende Rechtsprechungslinie der Gerichte etabliert, die weitgehend auf unter der alten

Rechtslage entwickelten Judikatur aufbaut. So hat etwa eine Reihe von Obergerichten entsprechende Ansprüche bestätigt (vgl. etwa OLG Hamburg, Urteil vom 25.10.2018 – 3 U 66/17; OLG München, Urteil vom 21.03.2019 – 6 U 3377/18; OLG Naumburg, Urteile vom 7.11.2019 – 9 U 6/19 und 9 U 39/18; OLG Stuttgart, Urteil vom 27.02.2020 – 2 U 257/19).

Unter der alten Rechtslage hatte der Europäische Gerichtshof (EuGH) die vorgelagerte Frage nach der sogenannten Sperrwirkung datenschutzrechtlicher Rechtsbehelfe verneint (EuGH, Urteil vom 29.07.2019, Az. C-40/17). Im Berichtszeitraum hat der Bundesgerichtshof diese Frage unter der neuen Rechtslage erneut dem EuGH vorgelegt (BGH, Beschluss vom 28. Mai 2020 - I ZR 186/17; am EuGH registriert unter C-319/20, Facebook Ireland Limited gegen Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband e.V.). Entsprechend steht eine verbindliche höchstgerichtliche Entscheidung an, die die bestehende Unsicherheit beseitigen könnte.

Die lauterkeitsrechtliche Durchsetzung der Datenschutzregeln ohne Selbstbetroffenheit hat eine Reihe erheblicher Vorteile gegenüber behördlichem Vorgehen. Maßnahmen und Sanktionen der Datenschutzaufsichtsbehörden können jedoch durchaus auf entsprechenden Feststellungen aufbauen.

Auf diese Weise stellen Wettbewerber und andere Klageberechtigte ohne datenschutzrechtliche Selbstbetroffenheit zusätzliche Ressourcen zur Verfügung, die marktbezogene Einhaltung der Datenschutzregeln zu kontrollieren, und dienen so dem Datenschutz.

Zudem sind Marktteilnehmer mitunter aus ihrer eigenen Vorbeschäftigung mit den konkreten Datenschutzproblemen in ihrer Branche enger vertraut als möglicherweise nicht vorbefasste Aufsichtsbehörden.

Schließlich ist die übliche Durchsetzungsform in diesem Bereich die Abmahnung, die regelmäßig innerhalb weniger Tage zur Abstellung abgemahnter datenschutzwidriger Praktiken führen kann, was in behördlichen Verfahren nur selten gelingt.

Auch wenn die vollständige Entwicklung der privaten Rechtsdurchsetzung in diesem Bereich noch von einer – absehbaren –

endgültigen Klärung einiger Rechtsfragen abhängt, kann doch bereits heute konstatiert werden, dass es sich um eine wertvolle Ergänzung des datenschutzrechtlichen Durchsetzungsinstrumentariums handelt.

Breitenwirkung und Schadensersatz für Datenschutzverstöße

Die aus Datenschutzverstößen folgenden Schäden sind in der Regel immaterieller Natur. Deutsche Gerichte sind in der Regel zwar sehr zurückhaltend beim Zuspruch von Schadensersatz für immaterielle Schäden. Die DSGVO hat hier allerdings mit Art. 82 eine vollkommen neue Rechtsgrundlage eingeführt, deren Wirksamkeit sich freilich erst entwickeln muss.

Unionsrechtlich ist der erlittene Schaden vollständig und wirksam zu ersetzen (Erwägungsgrund 146 DSGVO). Insoweit kann auf eine umfangreich entwickelte unionsrechtliche Judikatur zum Schadensersatzrecht, insbesondere nach Kartellrechtsverstößen, zurückgegriffen werden.

Denn die Mitgliedsstaaten – auch die mit Schadensersatzforderungen befassten Gerichte – sind nach dem Gedanken des Art. 4 Abs. 3 des Vertrags über die Europäische Union (EUV) verpflichtet, der Datenschutz-Grundverordnung zur Wirkung zu verhelfen (Arbeitsgericht Dresden, Urteil vom 26.08.2020 – 13 Ca 1046/20).

Nach anfänglichem Zögern haben deutsche Gerichte zunehmend eine Judikatur entwickelt, deren zugesprochene Schadensersatzsummen teils ausdrücklich „abschreckende Wirkung" haben sollen. Demgegenüber wird mitunter auch dann ein Ausgleich in Geld abgelehnt, wenn vorsätzliche Datenschutzverstöße nicht unerhebliche Schäden verursacht haben. Illustriert wird dieses Widerspiel von unionsrechtlichen Vorgaben und deutscher Justiztradition durch eine datenschutzbezogene Entscheidung des Bundesverfassungsgerichts: Ein Amtsgericht hatte die Schadensersatzforderung eines von einer rechtswidrigen Werbe-E-Mail Betroffenen abgelehnt: Hier liege lediglich eine bagatellartige Beeinträchtigung vor, die einen Schadensersatz nicht begründen könne. Das Bundesverfassungsgericht hob diese Entscheidung auf, da das

Amtsgericht nicht ohne Weiteres von einer nirgends festgelegten Erheblichkeitsschwelle ausgehen dürfe. Vor einer Ablehnung des Schadensersatzanspruchs sei daher die zugrunde liegende Auslegungsfrage dem Europäischen Gerichtshof vorzulegen (Bundesverfassungsgericht, Beschluss vom 14. Januar 2021 – 1 BvR 28531/19).

Mitunter wird vorgetragen, die Verantwortlichen würden durch die Pflicht zum Ersatz des verursachten immateriellen Schadens über Gebühr und jenseits konkreter Vorwerfbarkeiten belastet. Dies stellt eine abstrakte Gefahr dar, die von interessierter Seite immer wieder vorgebracht wird. Aus konkreten Urteilen ist eine derartige Unverhältnismäßigkeit allerdings nicht erkennbar und würde auch im Gegensatz zu den Grundprägungen und sonstigen Schadensersatzgewichtungen deutscher Gerichte stehen. Vielmehr sollte sich der Verantwortliche, der seinen Sorgfalts- und Dokumentationspflichten nachgekommen ist, regelmäßig ohne Weiteres exkulpieren können, Art. 82 Abs. 3 DSGVO.

Bei einer Betrachtung der Handlungsanreize stellen schließlich Bußgelder, Schadensersatzforderungen und Reputationsschäden, multipliziert mit der Wahrscheinlichkeit einer Aufdeckung, Sanktionierung und Verurteilung, die „Kosten" eines Verstoßes dar. Solange diese Kosten geringer sind als die Kosten einer Datenschutz-Compliance, ist es betriebswirtschaftlich rational, suboptimale Compliance-Anstrengungen zu unternehmen. Dies gilt besonders, wenn diese „Kosten" erst nach der Amtszeit der Zuständigen innerhalb der Unternehmen drohen, während entsprechende Boni zeitnah realisiert werden.

Die Datenschutzbehörden können kapazitätsbedingt Bußgelder nur in einem Bruchteil der sanktionswürdigen Verstöße verhängen. Verantwortlichen für Datenschutzverstöße den vollständigen und wirksamen Ersatz der so verursachten (immateriellen) Schäden aufzuerlegen erscheint vor diesem Hintergrund dringend komplementär erforderlich, um ausreichende Anreize zur angemessenen Sorgfalt bei der Verarbeitung personenbezogener Daten zu geben.

Die Verpflichtung zum Schadensersatz hat auch direkt aufmerksamkeitslenkende Wirkung: Denn dadurch muss der Verantwortliche gewärtig sein, Schäden konkret ausgleichen zu müssen, die durch eine Verwirklichung des durch eine Datenverarbeitung bedingten Risikos entstehen. Erst durch eine wirksame und vollständige Ersatzpflicht ist die datenschutzrechtliche Risikobetrachtung nicht nur abstrakt, sondern steht in angemessenem Verhältnis zum dadurch gesetzten Risiko für die Betroffenen.

In der Fläche sind bereits eine Vielzahl von Urteilen ergangen, in denen dem Betroffenen nicht unerhebliche Schadensersatzsummen für Datenschutzverstöße zugesprochen wurden. Gegenstand der haftungsauslösenden Rechtsverletzung waren etwa die unberechtigte Kundgabe (teils falscher) personenbezogener Daten an Dritte oder deren Veröffentlichung, die Verweigerung oder verspätete Erteilung datenschutzrechtlich geschuldeter Auskünfte.

Auf der anderen Seite haben Gerichte entsprechende Forderungen abgelehnt, weil kein Schaden entstanden oder dargelegt worden sei, es an einer substanziierten Darlegung bzw. dem Beweis eines Datenschutzverstoßes, dessen Kausalität oder eines Verschuldens des Verantwortlichen fehlte. Die nicht wenigen abweisenden Urteilen zugrunde gelegte Voraussetzung einer Erheblichkeit des Schadens unterliegt aktuell einer Beurteilung durch den EuGH (siehe oben).

Zwar fällt dem Betroffenen mitunter schwer, den Datenschutzverstoß, den daraus folgenden Schaden und die Kausalität zwischen Verstoß und Schaden zu beweisen. Allerdings stellt Art. 82 Abs. 3 DSGVO eine Vermutungsregel hinsichtlich des Verschuldens des Verantwortlichen auf, deren Reichweite umstritten ist. Daneben unterliegt aktuell der höchstgerichtlichen Klärung, welche Auswirkungen die allgemeine Rechenschaftspflicht der Art. 5 Abs. 2, 24 Abs. 1 DSGVO im Rahmen der zivilrechtlichen Darlegungs- und Beweislast haben (OLG Stuttgart, Urteil vom 31.03.2021 – 9 U 34/21; Rechtsmittel sind beim Bundesgerichtshof anhängig). Ich hoffe für die Betroffenen, dass bald eine Klärung zu ihren Gunsten herbeigeführt wird.

Unternehmen haben häufig ein erhebliches Interesse, Schadensersatzansprüche abzuwehren, um ähnlich Betroffene von der Geltendmachung ihrer Rechte abzuhalten. Entsprechend sind vor Gericht aufseiten der Verantwortlichen hochqualifizierte Rechtsanwälte tätig, deren kostenintensiver Einsatz allein durch das Interesse an einer Vermeidung von Präzedenzentscheidungen zu erklären ist. Aufseiten der Betroffenen sind erst zögerlich Prozessfinanzierer und spezialisierte Verbraucheranwälte zu beobachten, was sicher auch in der zurückhaltenden Haltung der deutschen Gerichte begründet liegt, Ersatz für immateriellen Schaden zuzusprechen.
Insgesamt entwickelt sich mit dem Schadensersatz für Datenschutzverstöße ein neues Rechtsgebiet, das erhebliches Potenzial aufweist, dezentrale Anreize für die Einhaltung des Datenschutzrechts zu bieten. Dies ist uneingeschränkt zu begrüßen, unterstützt es die Aufsichtsbehörden in ihren Zielen, den Datenschutz zu stärken.

Effektive Klärung offener Grundsatzfragen durch den Europäischen Gerichtshof

Die Effektivierung des datenschutzrechtlichen Betroffenenschutzes durch Schadensersatzansprüche bedarf jedoch noch der Klärung einiger Grundfragen. Ein Vergleich mit den insoweit ähnlichen Entwicklungen im Kartellrecht legt nahe, dass die Wirksamkeit der Schadensersatzansprüche aus Art. 82 DSGVO erst nach jahrzehntelangen justiziellen Klärungen dem Anspruch der DSGVO und des Unionsrechts entsprechen wird. Eine grundlegende Lehre aus jenem und verwandten Bereichen ist, dass in durch Unionsrecht determinierten Fragen allein der Europäische Gerichtshof Rechtsklarheit bringen kann. Eine entsprechende Vorlage bietet schon erstinstanzgerichtlichen Verfahren die Möglichkeit, nach Art. 267 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) Fragen des Datenschutz- und des Schadensersatzrechts verbindlich sowie relativ günstig und zeitnah klären zu lassen. Eine Vielzahl sowohl deutscher Gerichte als auch Gerichte anderer Mitgliedsstaaten der EU haben von dieser Vorlagepflicht bzw. -möglichkeit im Bereich des

Datenschutz-Schadensersatzrechts bereits Gebrauch gemacht. Auf Basis dieser Verfahren ist bereits die verbindliche Klärung vieler offener Rechtsfragen in nächster Zukunft zu erwarten.

Vorlagerecht und Vorlagepflicht deutscher Gerichte

Vorabentscheidungen des Europäischen Gerichtshofs führen für alle Rechtsanwender im Geltungsbereich der DSGVO unmittelbar zu Rechtsklarheit. Bislang findet in Deutschland die Klärung offener Rechtsfragen v. a. im Rahmen langwieriger Prozesse durch die Gerichtsinstanzen statt. Dies führt faktisch oft zu langjähriger Wirkung paralleler, vielfach inhaltlich widersprechender unter- und obergerichtlicher Entscheidungslinien mit entsprechenden Rechtsunsicherheiten, Prozessrisiken und weiteren Problemen. Das Bundesverfassungsgericht hat demgegenüber auch für den Bereich der DSGVO ausdrücklich darauf hingewiesen, dass insbesondere der Geldentschädigungsanspruch für Datenschutzverletzungen in der Rechtsprechung des Gerichtshofs der Europäischen Union nicht erschöpfend geklärt ist und entsprechend Vorlagepflichten der entscheidenden Fachgerichte bestehen, konkret des Amtsgerichts Goslar (Bundesverfassungsgericht, Beschluss vom 14. Januar 2021 - 1 BvR 2853/19).

Viele Gerichte haben diese Vorlagemöglichkeit im Datenschutzrecht bereits genutzt, sodass dazu eine Vielzahl teils inhaltlich überlappender Vorabentscheidungsverfahren in Luxemburg anhängig sind. So lassen unter anderem das Landgericht Saarbrücken und der österreichische Oberste Gerichtshof die Frage klären, ob Ersatzansprüche für immaterielle Schäden aus Datenschutzverstößen eine Mindestschwelle oder einen nachweisbaren Schaden voraussetzen (Landgericht Saarbrücken Beschluss vom 22.11.2021 – 5 O 151/19 = EuGH C-741/21 sowie Oberster Gerichtshof der Republik Österreich, Beschluss vom 15. April 2021 – 6 Ob 35/21x = EuGH C-154/21). Viele andere deutsche (Ober-)Gerichte haben demgegenüber ohne Rücksicht auf die Besonderheiten und die Autonomie des Unionsrechts deutschrechtliche Grundsätze angewandt, und so faktisch Rechtsschutz

erschwert oder gar vereitelt. Vor diesem Hintergrund sei mit dem Bundesverfassungsgericht an die Vorlagepflicht letztinstanzlicher Gerichte erinnert, und die Vorlagemöglichkeit für alle Gerichte einschließlich der Amts- und Landgerichte hervorgehoben.

Die Sächsische Datenschutzbeauftragte regt die zuständigen Gerichte dringend an, in Zweifelsfragen die Vorlagemöglichkeit an den Europäischen Gerichtshof zu nutzen und so zur Erhöhung der Rechtsklarheit beizutragen. Dadurch, und durch die Aussetzung von Verfahren bis zur Entscheidung des EuGH in problemidentischen Vorlageverfahren, können unnötige Instanzenzüge und viele weitere Prozesse vermieden werden. Nicht zuletzt kann die so erreichbare Rechtsklarheit auch die Einhaltung des Datenschutzrechts für alle Rechtsanwender, einschließlich der Verantwortlichen, wesentlich erleichtern.

Beratungsmandat der Sächsischen Datenschutzbeauftragten und Breitenwirkung

Meine Behörde ist weder für die Beurteilung von datenschutzrechtlichen Schadensersatz- noch von nachbar-, presse- oder lauterkeitsrechtlichen Unterlassungsansprüchen zuständig. Im Rahmen meines Beratungs- und Aufklärungsmandats aus Art. 57 Abs. 1 Buchst. b, e, i, v DSGVO bin ich allerdings gehalten, Betroffene, Verantwortliche und die Öffentlichkeit über den Datenschutz zu informieren und die entsprechenden Entwicklungen zu beobachten.

Durch konkrete oder allgemeine Hinweise auf die Möglichkeiten privater Rechtsdurchsetzung können externe Ressourcen, etwa der Betroffenen und Verantwortlichen, aber auch entsprechender Berater und zuständiger Zivilgerichte für die Durchsetzung des Datenschutzrechts nutzbar gemacht werden.

Nicht nur in den beispielhaft aufgeführten Bereichen kann der Einzelne, gegebenenfalls mit Unterstützung entsprechender Interessenvertretungen wie der Verbraucherzentralen, nicht allein sein Recht durchsetzen, sondern auch an der Klärung offener Fragen mitwirken und Datenschutzverstöße wirksam und nachhaltig abstellen.

Was ist zu tun?

Die direkte Durchsetzung des Datenschutzrechts kann eine Reihe von Vorzügen insbesondere für die Betroffenen aufweisen. Für manche Rechte sieht das Datenschutzrecht schon eine primäre Pflicht des Betroffenen vor, diese direkt gegenüber dem Verantwortlichen geltend zu machen.

Im Nachbarrecht sind zivilprozessuale Mittel teils deutlich schärfer und effektiver als aufsichtsrechtliche Ermittlungs- und Abstellungsbefugnisse.

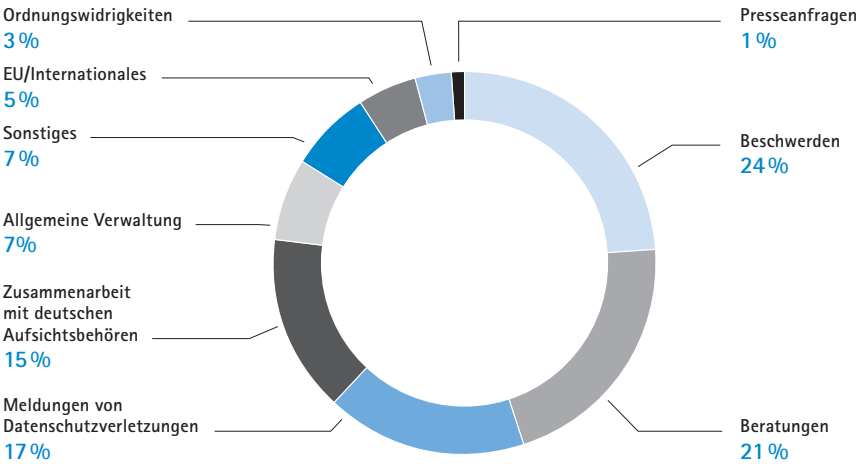
Insbesondere in Fallkonstellationen, in denen breitenwirksame Praktiken nicht datenschutzkonform sind, während die zuständige Aufsichtsbehörde untätig bleibt, empfiehlt sich die private Rechtsdurchsetzung als wirksameres Mittel, dem Datenschutzrecht zur praktischen Geltung zu verhelfen. Diese Datenschutz-Compliance wiederum ist ein zentrales Ziel meiner Tätigkeit.

6.2 Zahlen und Daten zu den Tätigkeiten 2021

6.2.1 Überblick zu den Arbeitsschwerpunkten

Wie im vorherigen Berichtszeitraum verzeichnete meine Dienststelle bei Beschwerdeeingaben und Beratungsanfragen wiederum die meisten Vorgänge – zusammen rund 45 Prozent. Weiterhin bildete die Zusammenarbeit mit den deutschen Aufsichtsbehörden einen Schwerpunkt. Der rege Austausch zu Datenschutzthemen setzt sich fort, ebenso der Anstieg bei Meldungen von Datenschutzverletzungen nach Artikel 33 der Datenschutz-Grundverordnung.

Abbildung 2:
Arbeitsschwerpunkte nach Anzahl der Vorgänge



6.2.2 Beschwerden und Hinweise

Das Beschwerdeaufkommen lag im Berichtszeitraum auf dem hohen Niveau des Vorjahres. Seit Wirksamwerden der Datenschutz-Grundverordnung im Jahr 2018 haben sich die jährlich eingehenden Beschwerden und Hinweise mehr als verdoppelt. Sanken 2021 die Eingaben im öffentlichen Bereich, legten sie im nichtöffentlichen Sektor gegenüber 2020 zu.

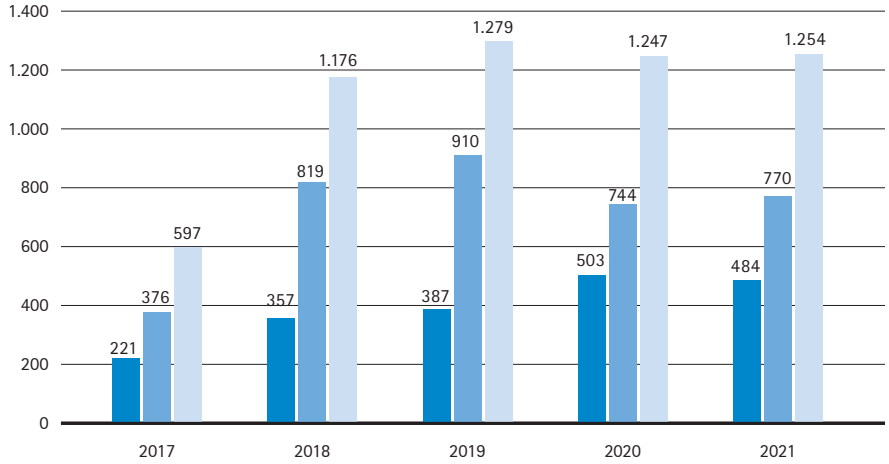


Abbildung 3:
Beschwerden und Hinweise

- öffentlicher Bereich
- nichtöffentlicher Bereich
- Beschwerden gesamt

Beschwerdeaufkommen bei Telemedien

Auch in diesem Berichtszeitraum gab es ein beständig hohes Aufkommen an Beschwerden im Bereich Telemedien. Insgesamt sind über 80 Beschwerden eingegangen, die zum überwiegenden Teil berechtigt waren. Die meisten Beschwerden richteten sich gegen sächsische Betreiber von Websites, die Cookies und Tracking-Elemente ohne eine Einwilligung in ihre Websites eingebunden hatten oder Daten der Besucher in Drittländern wie die USA übermitteln. Weitaus weniger Beschwerden wurden 2021 aufgrund fehlender Verschlüsselung auf Websites eingereicht; hier ist davon auszugehen, dass ein Großteil der Website-Betreiber mittlerweile eine zuverlässige Transportverschlüsselung einsetzt. Die

Tätigkeitsbericht 2020:
↗ sdb.de/tb2020

Bearbeitung der Beschwerden ist trotz der im letzten Jahr gestarteten Bemühungen um eine Automatisierung (siehe TB 2020; 4.1.1 Prüfwerkzeuge für Websites und Anforderungen an Betreiber von Websites, Seite 115f.) immer noch aufwendig in der Vorbereitung und im Verfahren mit den jeweiligen Verantwortlichen. Im Vorfeld müssen alle auf einer Website stattfindenden Datenverarbeitungen (Einbindungen von Dritt-Ressourcen, Cookies und andere Technologien) sowie die Datenschutzerklärung der Website analysiert und bewertet werden, was aufgrund der schieren Masse an eingesetzten Techniken oft sehr aufwendig ist. So ist es nicht ungewöhnlich, wenn beim Aufruf der Startseite einer einzelnen Website bereits mehr als 20 Cookies gesetzt werden und Verbindungen zu bis zu 40 fremden Servern stattfinden, die alle Daten der Besucher erhalten. Im Verfahren mit dem Verantwortlichen werden dann oft umfangreiche Unterlagen wie Auftragsdatenverarbeitungsverträge und andere Vereinbarungen beigebracht, die wiederum bewertet werden müssen. Über die jeweiligen Verfahrensstände werden die Betroffenen regelmäßig informiert bzw. können sich bei Fragen auch jederzeit an meine Behörde wenden.

6.2.3 Beratungen

Die Digitalisierung nahezu aller Lebensbereiche setzt sich fort. Folglich werden auch immer mehr personenbezogene Daten verarbeitet. Was hierbei erlaubt ist und wie die Daten von Bürgerinnen und Bürgern zu schützen sind, war 2021 vielmals Thema in Gesprächen mit Verantwortlichen. Insgesamt stieg die Anzahl der Beratungsvorgänge im Vergleich zum vorherigen Berichtszeitraum um über 9 Prozent auf 1.112. Das waren fast so viele wie im Jahr 2018, als die Datenschutz-Grundverordnung wirksam wurde. Der Zuwachs geht sowohl auf Auskünfte gegenüber dem öffentlichen als auch dem nichtöffentlichen Bereich zurück. Viele Anfragen standen im Zusammenhang mit der Coronavirus-Pandemie und sind exemplarisch auch in diesem Tätigkeitsbericht aufgeführt (siehe 1.1, 2.2.10, 2.4.1).

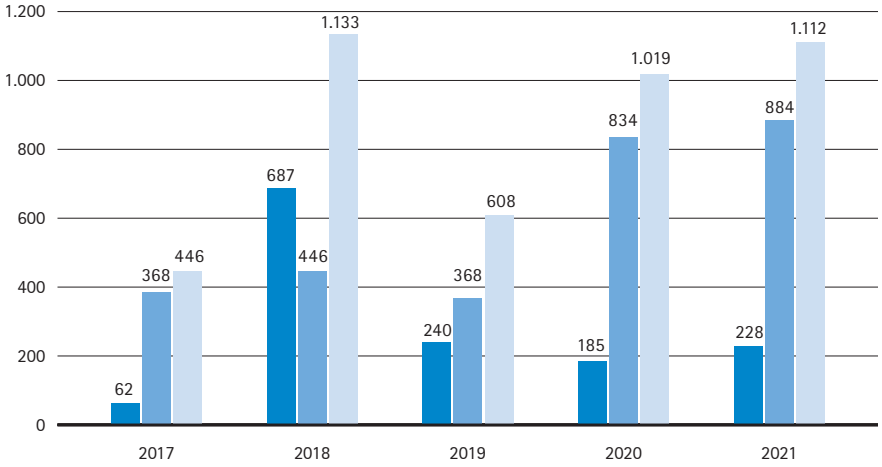


Abbildung 4:
Beratungen

- öffentlicher Bereich
- nichtöffentlicher Bereich
- Beratungen gesamt

6.2.4 Datenschutzverletzungen

↗ Art. 33 DSGVO

Die Meldung von Datenschutzverletzungen gemäß Art. 33 der Datenschutz-Grundverordnung steigt seit der Anwendbarkeit der Datenschutz-Grundverordnung ab dem 25. Mai 2018 stetig an. Neben der Registrierung sind die Meldungen auszuwerten und gegebenenfalls für eine aufsichtliche Nacharbeit zu kategorisieren. Einen Überblick zu den inhaltlichen Vorgängen liefert der Beitrag 4.4.1.

6.2.5 Zusammenarbeit mit europäischen Aufsichtsbehörden – Internal Market Information System

↗ Art. 56, 60, 61, 64 DSGVO; Verordnung (EU) 1024/2012

Die Datenschutzaufsichtsbehörden in der Europäischen Union koordinieren in grenzüberschreitenden Fällen ihre Zusammenarbeit nach den Artikeln 60 bis 67 der Datenschutz-Grundverordnung durch das sogenannte Binnenmarkt-Informationssystem (Internal Market Information System – IMI). Es handelt sich dabei um ein webbasiertes Netzwerk zum Informationsaustausch und für die Zusammenarbeit der

Tätigkeitsbericht 2020:
↗ sdb.de/tb2020

öffentlichen Stellen, welches durch die Kommission der Europäischen Union bereitgestellt wird (vgl. auch Tätigkeitsbericht 2020, Punkt 6.2.5, Seite 144). Einzelheiten dieser Verwaltungszusammenarbeit sind in der Verordnung (EU) Nr. 1024/2012 (IMI-Verordnung) geregelt.

Im IMI werden jeden Tag Informationen zu den dort eingestellten Verfahren, die sogenannten IMI-Notifications, auch an mich versandt. Mich erreichen täglich etwa zwischen zehn und 20 solcher Mitteilungen. Ich prüfe dabei, ob ich federführende oder lediglich (mit-)betroffene Aufsichtsbehörde bin, und – wenn ich betroffene Aufsichtsbehörde bin – ob ich mich bei Verfahren anderer Aufsichtsbehörden zum Sachstand oder zu Entscheidungen äußern möchte. Auch werde ich darüber informiert, wie andere Aufsichtsbehörden mit bestimmten Fällen umgehen.

Insgesamt wurden im IMI-System 2021 unter Beteiligung deutscher (federführender oder lediglich betroffener) Aufsichtsbehörden 2.367 Verfahren eingestellt. Davon wurden 128 wieder eingestellt (Statistische Angabe vom 04.11.2021). Auch ich war in einer Vielzahl von Verfahren als betroffene Aufsichtsbehörde beteiligt. Als federführende Aufsichtsbehörde habe ich im Berichtszeitraum zwei Verfahren übernommen, da die jeweiligen Unternehmen ihre Hauptniederlassung in Sachsen haben. Sachsen ist damit in sechs Verfahren federführend. Einen Fall habe ich an die federführende Aufsichtsbehörde eines anderen Mitgliedsstaats in einem Verfahren nach Art. 56 DSGVO abgegeben.

Seit Juli 2021 nutzen die deutschen Aufsichtsbehörden auch das IMI-Modul „Internal Written Procedure" (IWP) für ihre interne Abstimmung bei schriftlichen Verfahren des Europäischen Datenschutzausschusses (EDSA). Auf diese Weise stellen sie gemeinsame Standpunkte gemäß § 18 Bundesdatenschutzgesetz (BDSG) her. In diesem Rahmen gab ich unter anderem mein Votum für Stellungnahmen des EDSA zu verbindlichen internen Vorschriften von Unternehmen („Binding Corporate Rules"), zu Anforderungen an die Akkreditierung von Zertifizierungsstellen (Art. 64 Abs. 1 Satz 2 Buchst. c der Datenschutz-Grundverordnung) oder für Ant-

wortschreiben an verschiedene Einrichtungen der Europäischen Union ab. Ich gehe davon aus, dass künftig die Anzahl der Beschwerden betroffener Personen in der Europäischen Union und auch in Sachsen und damit auch die Anzahl der grenzüberschreitenden Verfahren im IMI weiter steigen wird.

6.2.6 Register der benannten Datenschutzbeauftragten

↗ Art. 37 Abs. 1 und 7 DSGVO

Im Berichtszeitraum gingen 1.015 Meldungen zu benannten Datenschutzbeauftragten in meiner Dienststelle ein. Diese Meldungen umfassten Mitteilungen zur Benennung von behördlichen und betrieblichen Datenschutzbeauftragten (DSB), 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 Bedingungen) die Pflicht vor, einen Datenschutzbeauftragten zu benennen. Nach Art. 37 Abs. 7 der DSGVO hat ein Verantwortlicher oder ein Auftragsverarbeiter die Kontaktdaten 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.

6.2.7 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 Rechtsverordnungs-

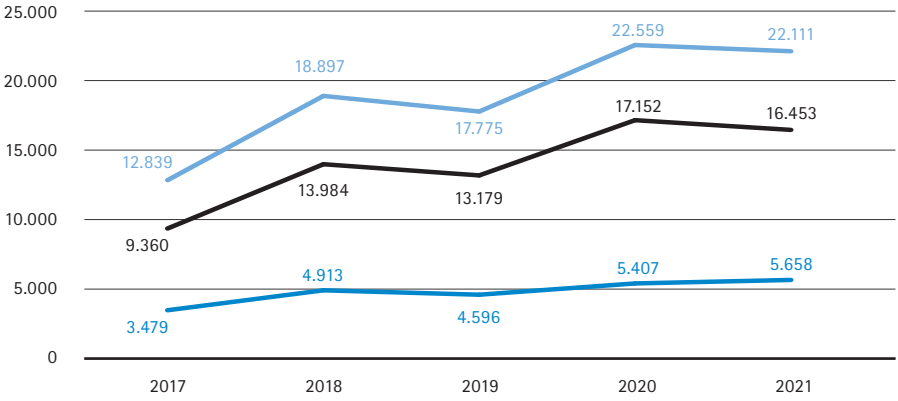
entwurfs, die die Verarbeitung personenbezogener Daten betreffen, zu konsultieren. Im Berichtszeitraum hat sich meine Behörde verfahrensbegleitend bei Rechtsetzungsvorhaben eingebracht. Dabei handelte es sich beispielsweise in Sachsen um Stellungnahmen zum Gesetz zur Fortentwicklung des Kommunalrechts, zum Transparenzgesetz, zur Novellierung des Hochschulfreiheitsgesetzes und zur Verordnung auf Grundlage des Informationssicherheitsgesetzes und des Infektionsschutzgesetzes. Auch mit Rechtsetzungsvorhaben für Deutschland und Europa befasste sich mein Amtsvorgänger. Das betraf unter anderem das Registermodernisierungsgesetz, die Evaluierung des Bundesdatenschutzgesetzes und das Telekommunikations-Telemedien-Datenschutzgesetz (TTDSG).

6.2.8 Ressourcen

Tätigkeitsbericht 2020:
↗ sdb.de/tb2020

Seit Anwendbarkeit der Datenschutz-Grundverordnung sehe ich einen kontinuierlichen Anstieg beim Arbeitsaufkommen in meiner Dienststelle. Auf die Gründe ist mein Amtsvorgänger bereits mehrfach eingegangen (vgl. Tätigkeitsbericht 2020, 6.3, Seite 145f.).
Seit der Covid-19-Pandemie hat sich das Pensum noch mal deutlich erhöht. Im Berichtszeitraum wurden 16.453 Posteingänge und 22.111 Postausgänge registriert. Damit lag das Schriftgutaufkommen nahezu auf dem Rekordstand von 2020.

Abbildung 5:
Schriftgutaufkommen

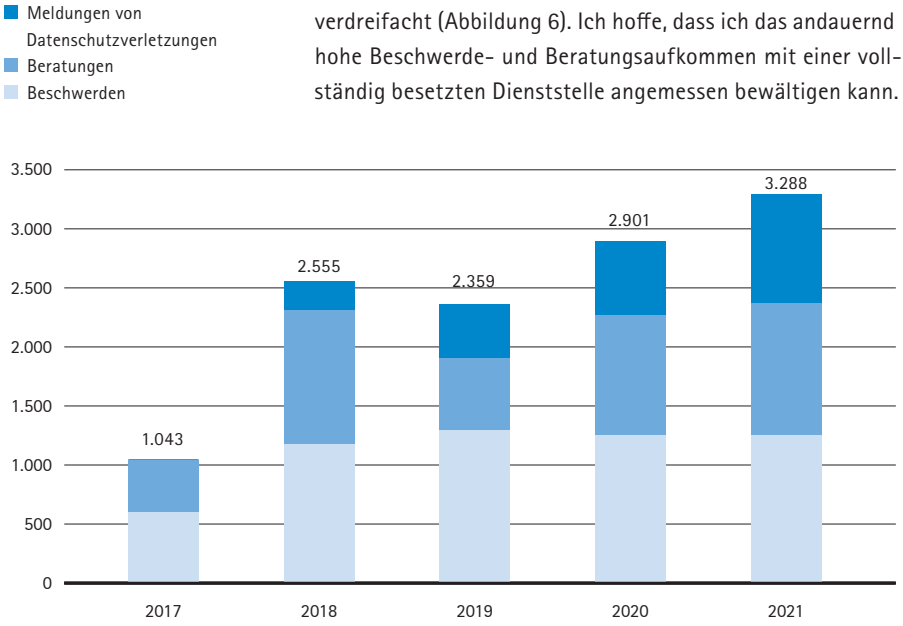


Wie in den Vorjahren konnte meine Behörde die gesetzlichen Aufgaben nicht voll umfänglich erfüllen. Zwar hat sich die Personallage in meiner Behörde durch die mir im Berichtszeitraum zugewiesenen acht neuen Stellen entspannt. Dafür danke ich den Abgeordneten des Sächsischen Landtages. Jedoch konnte ich – wegen der Verabschiedung des Doppelhaushaltes 2021/22 erst im Juni 2021 – erst in der zweiten Hälfte des Berichtszeitraums tatsächlich mit Stellenbesetzungsverfahren beginnen. Die Personalentwicklung der vergangenen Jahre, jeweils zum 31. Dezember, stellt sich wie folgt dar:

- 2017: 22 Planstellen
- 2018: 24 Planstellen
- 2019: 28 Planstellen
- 2020: 31 Planstellen
- 2021: 39 Planstellen

Von 2017 bis Ende 2021 haben sich die jährlich neu eingehenden Vorgänge in wichtigen Tätigkeitsbereichen mehr als verdreifacht (Abbildung 6). Ich hoffe, dass ich das andauernd hohe Beschwerde- und Beratungsaufkommen mit einer vollständig besetzten Dienststelle angemessen bewältigen kann.

Abbildung 6:
Zuwächse in wichtigen Tätigkeitsbereichen



In wichtigen Tätigkeitsbereichen wie der Bearbeitung von Beschwerden, Datenpannen-Meldungen und bei Beratungen hat sich die zu knapp bemessene personelle Ausstattung der Dienststelle im letzten Jahr noch offenbart. Konkret: Vorgänge konnten oftmals nur mit mehrmonatiger Verzögerung erledigt werden, anlasslose Datenschutz-Kontrollen erfolgten leider nur in geringem Maße und Referententätigkeiten bei verschiedenen Fach- und Fortbildungsveranstaltungen konnten nur in geringem Umfang wahrgenommen werden. (siehe 6.5.2). Weiterhin sind immer noch Altfälle aus den vergangenen Jahren abzuarbeiten. Vor allem für die betroffenen Personen, deren Daten gegebenenfalls deshalb über einen längeren Zeitraum unrechtmäßig verarbeitet werden, ist dies ein schwer nachvollziehbarer Zustand, zumal ich den Anspruch habe, Bürger, Wirtschaft und Verwaltung frühzeitiger und umfangreicher zu beraten. Prävention ist bekanntlich besser als Intervention.

Erfolgreiche Fortbildung von Mitarbeitern

In meiner Dienststelle verfügen nunmehr vier Bedienstete über eine Qualifizierung zum Fachbegutachter der Deutsche Akkreditierungsstelle GmbH (DAkkS), der nationalen Akkreditierungsstelle der Bundesrepublik Deutschland mit Sitz in Berlin. Sie sind damit zur Mitwirkung im Rahmen der Akkreditierung von Zertifizierungsstellen befähigt und erfüllen die Voraussetzungen zur Erteilung von Zertifikaten im Bereich des Datenschutzes nach der Datenschutz-Grundverordnung.

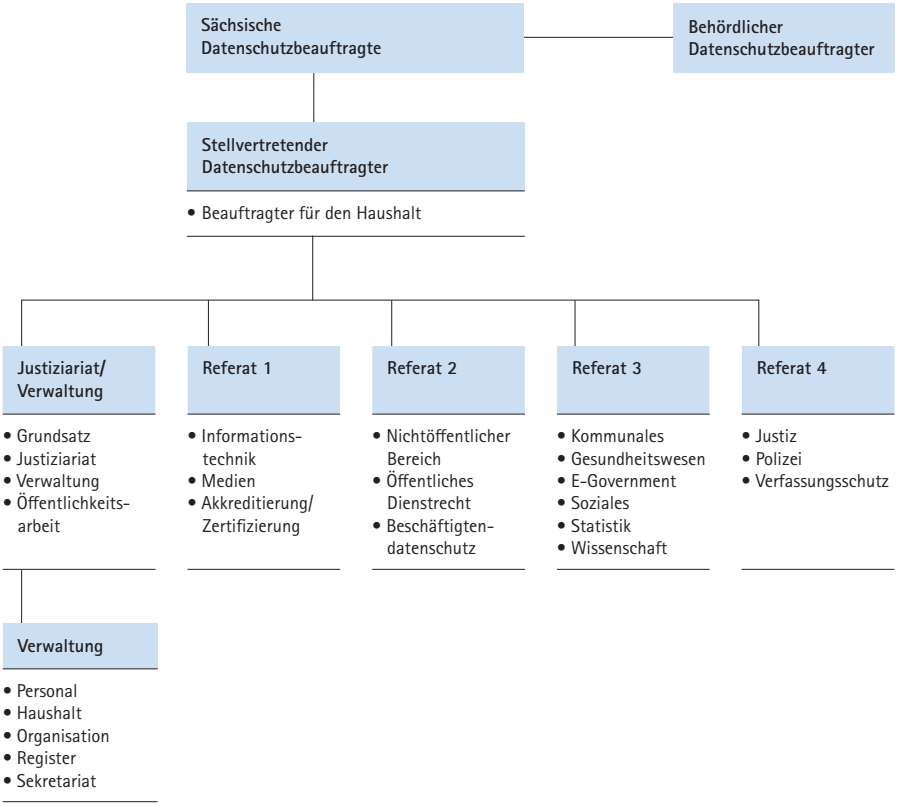


Abbildung 7:
Vereinfachtes Organigramm der Behörde

6.3 Datenschutzaufsichtliche Befugnisse, verwaltungsrechtliche Entscheidungen

6.3.1 Inanspruchnahme des Auskunftsverweigerungsrechts

↗ § 40 Abs. 4 Satz 2 BDSG, § 383 Abs. 1 Nr. 1 bis 3 ZPO, Art. 58 Abs. 1 Buchst. a und Abs. 4 DSGVO, Art. 31 DSGVO

Nach Art. 58 Abs. 1 Buchst. a Datenschutz-Grundverordnung (DSGVO) kann die Aufsichtsbehörde den Verantwortlichen anweisen, alle Informationen bereitzustellen, die für die Erfüllung ihrer Aufgaben erforderlich sind. Der Begriff

„Informationen" schließt dabei die Bereitstellung von Unterlagen oder Dateien ein. Art. 31 DSGVO korrespondiert mit dieser Vorschrift und verpflichtet den Verantwortlichen, mit der Aufsichtsbehörde zusammenzuarbeiten und sie bei der Erfüllung ihrer Aufgaben zu unterstützen. Allerdings kann sich der Verantwortliche aufgrund der Rechtsstaatlichkeitsklausel in Art. 58 Abs. 4 DSGVO auf sein Auskunftsverweigerungsrecht berufen, soweit er sich durch die Bereitstellung der Informationen selbst belasten würde. Dieses Auskunftsverweigerungsrecht findet sich – insoweit zunächst beschränkt auf die Fälle der reinen Auskunftserteilung – in § 40 Abs. 4 Satz 2 Bundesdatenschutzgesetz (BDSG), wonach der Auskunftspflichtige die Auskunft auf solche Fragen verweigern kann, deren Beantwortung ihn selbst oder einen der in § 383 Abs. 1 Nr. 1 bis 3 der Zivilprozessordnung (ZPO) bezeichneten Angehörigen der Gefahr strafgerichtlicher Verfolgung oder eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten aussetzen würde, folgt darüber hinaus – mithin auch bezogen auf die generelle Informationsbereitstellung – aber auch aus den allgemeinen verfassungsrechtlichen und strafverfahrensrechtlichen Grundsätzen. Voraussetzung für die Inanspruchnahme des Auskunftsverweigerungsrechts ist, dass sich das Auskunfts- oder Informationsbereitstellungsverlangen auf ein Verhalten bezieht, das den Tatbestand einer Straftat oder Ordnungswidrigkeit erfüllen kann. Fragt die Aufsichtsbehörde verschiedene Sachverhalte ab, muss dabei entsprechend differenziert werden.

Aus der Praxis: Kooperation besser als Auskunftsverweigerung

So weit die Theorie. Offensichtlich verleitet die Möglichkeit dieses Auskunftsverweigerungsrechtes in der Praxis gelegentlich aber auch dazu, sich der – eher aufwendig erscheinenden – Informationsbereitstellung an die Aufsichtsbehörde zu entziehen, oder aber man verbindet damit die Hoffnung, dass sich die Aufsichtsbehörde damit zufriedengibt und man auf diese Weise der Ahndung eines im Raum stehenden Verstoßes entgehen kann.

Dass diese Hoffnung trügerisch sein kann und man dadurch letztendlich noch größeren Ärger und Aufwand bekommen kann, zeigt das folgende Beispiel:

Ein Petent hatte der Aufsichtsbehörde zwei Dome-Kameras auf einem zu Wohnzwecken genutzten Privatgrundstück angezeigt. Eine Kamera war an der Vorderfront neben dem Hauseingang platziert und auf diesen sowie möglicherweise auch auf die wenige Meter davor befindliche Straße gerichtet; die zweite Kamera befand sich auf dem rückwärtigen Balkon in einer exponierten Lage an einem dort wohl extra deswegen errichteten Mast. Direkt hinter der durch einen Zaun markierten Grundstücksgrenze führte ein Wanderweg entlang.

Der – anwaltlich vertretene – Verantwortliche hatte auf Aufforderung der Aufsichtsbehörde lediglich behauptet, dass weder fremde Grundstücke noch öffentliche Verkehrsflächen videoüberwacht würden. Die darüberhinausgehend geforderten Auskünfte hatte er ebenso wenig erteilt, wie er auch keine diesbezüglich abgeforderten Nachweise/Unterlagen, insbesondere auch keine Screenshots der Kamerabilder vorgelegt hat. Stattdessen hatte er nach nochmaliger Aufforderung von seinem Auskunftsverweigerungsrecht Gebrauch gemacht. Eine örtliche Überprüfung des Sachverhalts schied aus, da mangels geschäftlicher Nutzung kein Betretungsrecht für die Aufsichtsbehörde bestand.

Soweit man unterstellte, dass die Behauptung des Verantwortlichen, keine Bereiche außerhalb des eigenen Grundstücks zu überwachen, der Wahrheit entsprach, wäre die Berufung auf das Auskunftsverweigerungsrecht unrechtmäßig gewesen. Denn wenn sich die Videoüberwachung tatsächlich auf das eigene Grundstück beschränkte, hätte er sich mit der Beantwortung der Fragen der Aufsichtsbehörde nicht der Gefahr straf- oder ordnungswidrigkeitenrechtlicher Verfolgung ausgesetzt.

Angesichts dessen kam grundsätzlich die weitere – dann förmliche – Inanspruchnahme des Verantwortlichen zur Auskunftserteilung/Informationsbereitstellung in Betracht. Jedoch war dabei abzusehen, dass – wegen der zu erwartenden gerichtlichen Klärung – jedenfalls zeitnah keine belastbaren

und den tatsächlichen Verhältnissen entsprechende Ergebnisse erzielt werden konnten. Der Verantwortliche wäre zudem jederzeit in der Lage gewesen, nachträglich rechtskonforme Zustände herzustellen und dann erst der Aufsichtsbehörde zu antworten.

Ordnungswidrigkeitenverfahren und Durchsuchungsbeschluss

Effektiver erschien vorliegend die Überleitung ins Ordnungswidrigkeitenverfahren. Angesichts der Inanspruchnahme des Auskunftsverweigerungsrechts bestanden Anhaltspunkte dafür, dass tatsächlich auch Bereiche außerhalb des eigenen Grundstücks videoüberwacht wurden. Innerhalb eines Ordnungswidrigkeitenverfahrens könnte dies dann mit einem entsprechenden Durchsuchungsbeschluss kurzfristig überprüft und gegebenenfalls nachgewiesen und auch geahndet werden. Tatsächlich hat der Ermittlungsrichter beim zuständigen Amtsgericht dann auch einen diesbezüglichen Durchsuchungs- und Beschlagnahmebeschluss erlassen, den die Aufsichtsbehörde schließlich gemeinsam mit der örtlichen Polizei wenige Wochen später in den frühen Morgenstunden vollstreckt hat. Der sichtlich überraschte Hauseigentümer zeigte sich dabei – wohl auch zur Vermeidung weitgehender (aber dennoch zulässiger) Eingriffe und Einblicke in seine Privatsphäre – kooperativ. Auch wenn die Kameras zum Durchsuchungszeitpunkt nicht mehr aktiv waren, war der Hauseigentümer mit der Sicherstellung der zuvor für Videoaufzeichnungen genutzten Speichermedien einverstanden, sodass es einer Beschlagnahme nicht bedurfte. Der Ausgang des Verfahrens war zum Redaktionsschluss dieses Berichts wegen der ausstehenden Auswertung der Datenträger noch offen.

Gleichwohl sollte aus der Schilderung dieses Aufsichtsfalls die Schlussfolgerung gezogen werden, dass auch eine Inanspruchnahme des Auskunftsverweigerungsrechts wohl überlegt sein will. Zwar wird nicht jeder Sachverhalt derart drastische Ermittlungsmaßnahmen rechtfertigen können, tatsächlich kann aber auch nicht davon ausgegangen werden, dass sich ein Aufsichtsverfahren einfach mit der Inan-

Was ist zu tun?
Eine Inanspruchnahme des Auskunftsverweigerungsrechts im aufsichtlichen Verfahren ist seitens der Berechtigten gut abzuwägen. Anmerkung: Bei besonders tiefgreifenden Verstößen kann aber auch bei Kooperation mit der Aufsichtsbehörde ein Bußgeld nicht ausgeschlossen werden.

spruchnahme des Auskunftsverweigerungsrechtes erledigen lässt. Wer stattdessen – zumal als Privatperson – von Anfang an mit der Aufsichtsbehörde kooperiert und ein Aufsichtsverfahren auch als Chance sieht, seine Videoüberwachung rechtssicher zu gestalten, wird kaum Gefahr laufen, deswegen mit einem Bußgeld belegt zu werden.

6.3.2 Zwangsgeld bei Auskunftsverweigerung

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

Eine sächsische Kommune veröffentlichte in ihrem Gemeindespiegel ein Schreiben der Landesdirektion Sachsen (LDS), ohne eine Schwärzung des Namens und der Kontaktdaten der Ansprechpartnerin in der LDS vorzunehmen. Nachdem ich auf die Veröffentlichung hingewiesen wurde, forderte meine Behörde die Kommune auf, eine Rechtsgrundlage zu benennen oder anderenfalls bei einer Veröffentlichung im Internet beispielsweise eine entsprechende Schwärzung vorzunehmen und ihre Mitarbeiter für künftige Veröffentlichungen entsprechend zu sensibilisieren. Mein Amtsvorgänger musste mehrfach an sein Schreiben erinnern.
Schließlich bestritt die Kommune zunächst die Notwendigkeit, meiner Behörde eine Rechtsgrundlage für die Verarbeitung personenbezogener Daten benennen zu müssen und ließ später durch einen beauftragten Rechtsanwalt mitteilen, dass diese zum einen im Sächsischen Datenschutzgesetz (SächsDSG) zu finden sei, es zum anderen einer Ermächtigungsgrundlage für Eingriffe in individuelle Rechte von Amtswaltern ohnehin nicht bedürfe, da es einen solchen Eingriff mangels individueller Rechte nicht geben könne. Meine Behörde antwortete, dass weder das SächsDSG zum Zeitpunkt der Veröffentlichung anwendbar war (vielmehr wurde es wegen der Datenschutz-Grundverordnung (DSGVO) durch das SächsDSDG mit deutlich abweichenden Regelungen ersetzt), noch die Darstellung im Übrigen der aktuellen Rechtsprechung entspricht. Vielmehr gelten Grundrechte für Beamte im Rahmen des Dienstverhältnisses in gleicher und nicht lediglich abgeschwächter Weise.

Meine Behörde kündigte daraufhin an, die Gemeinde mittels Bescheid förmlich zur Auskunft heranzuziehen und den entsprechenden Verwaltungsakt mithilfe von Zwangsmitteln in Form eines Zwangsgeldes in Höhe von 500 Euro gemäß § 19 Abs. 2 Satz 1 Verwaltungsvollstreckungsgesetz für den Freistaat Sachsen (SächsVwVG) durchzusetzen. Diese Ankündigung bewirkte schließlich, dass durch die Kommune eingeräumt wurde, dass die unterlassene Schwärzung von Namen in dem veröffentlichten Schreiben der LDS versehentlich erfolgte und diese bei einer (bisher nicht erfolgten) Veröffentlichung im Internet vorgenommen wird.

6.4 Geldbußen und Sanktionen, Strafanträge

6.4.1 Ordnungswidrigkeitenverfahren im öffentlichen Bereich

Die Sächsische Datenschutzbeauftragte war im Berichtszeitraum im öffentlichen Bereich zuständig für die Verfolgung und Ahndung von Ordnungswidrigkeiten 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 des Zehnten Buches 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 93 Bußgeldverfahren anhängig. Davon wurden 15 mit einem Bußgeld abgeschlossen. 3 Verfahren sind nach eingelegtem

Einspruch gegen den Bußgeldbescheid dem zuständigen Amtsgericht vorgelegt worden. Eine Entscheidung steht noch aus. In 22 Verfahren erfolgte eine Einstellung bzw. wurde von der Verfolgung abgesehen. 56 Verfahren befanden sich zum Ende des Berichtszeitraumes noch in Bearbeitung.

Berichtszeitraum		**01.01.–31.12.2021**
anhängig gesamt		**93**
davon	Verfahren aus vorherigem Berichtszeitraum	55
	neu eingegangene Verfahren	38
abgeschlossen		**37**
davon	mit Bußgeld	15
	mit Verwarnungsgeld	0
	eingestellt/von Verfolgung abgesehen	22
noch in Bearbeitung		**56**
Summe festgesetzter Buß- und Verwarnungsgelder in Euro		**8.250**

Tabelle 1:
Ordnungswidrigkeitenverfahren im öffentlichen Bereich

Die Summe der festgesetzten Buß- und Verwarngelder belief sich auf 8.250 Euro, die der rechtskräftigen auf 6.920 Euro. Gegenüber dem vergangenen Berichtszeitraum hat sich die Anzahl der neu eingegangenen Ordnungswidrigkeitenverfahren nahezu verdoppelt. Dennoch konnten – vor allem aufgrund eines personellen Zuwachses – im Vergleich zum Berichtszeitraum 2020 doppelt so viele Verfahren abgeschlossen werden, was wiederum zu einer höheren Summe der festgesetzten Geldbußen führte.
Die im Berichtszeitraum andauernde Corona-Pandemie und die damit einhergehende zeitweise eingeschränkte Funktionsfähigkeit der Behörde sowie der stetig steigende Bearbeitungsaufwand im Bereich der Ordnungswidrigkeiten wirkten sich allerdings auch weiterhin negativ auf die Dauer der Verfahren aus.

Verfahren vor allem gegen Polizeibedienstete

Erneut standen/stehen in einem Großteil (ca. 75 Prozent) der Ordnungswidrigkeitenverfahren Bedienstete der sächsischen Polizei in Verdacht, unbefugt personenbezogene 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 durchweg um unbefugte Abrufe nicht offenkundiger personenbezogener Daten aus den polizeilichen Datenbanken (§ 38 Abs. 1 Nr. 1a SächsDSG alte Fassung), und/oder unbefugte Verarbeitungen nicht offenkundiger personenbezogener Daten (§ 38 Abs. 1 Nr. 1a SächsDSG alte Fassung) durch Polizeivollzugsbedienstete.

Ganz überwiegend privat motivierte Datenabrufe

Die anhaltend große Anzahl an Ordnungswidrigkeitenverfahren gegen sächsische Polizeibedienstete resultiert dabei einerseits aus einem überdurchschnittlichen Anzeigeverhalten der Polizeidienststellen, welche datenschutzrechtliche Verstöße – auch dienstrechtlich – konsequent verfolgen, deutet aber auch 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 Freunden, Kollegen, Nachbarn oder anderen Bekannten, aber auch um Recherchen zur eigenen Person. Wie bereits in vorangegangenen Tätigkeitsberichten ausführlich erläutert, darf der gesamte Polizeivollzugsdienst nur die personenbezogenen Daten verarbeiten, die zur Erfüllung seiner Aufgaben erforderlich sind (§ 53 Sächsisches Polizeivollzugsdienstgesetz (SächsPVDG) in Verbindung mit § 3 SächsDSUG). Somit ist auch der einzelne Polizeibedienstete nur berechtigt,

die zur Erfüllung 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 Freunde, Bekannte oder auch sie selbst in polizeilichen Verfahren erfasst sind, nur weil derartige Recherchen in den polizeilichen Datenbanken technisch möglich sind. Persönliche Neugier bzw. eine private Motivation ersetzen die zum Verarbeiten und/oder Abrufen nicht offenkundiger personenbezogener Daten erforderliche Befugnis demnach nicht.

Bereits durch bloße Unkorrektheiten im Umgang mit personenbezogenen Daten durch öffentliche Stellen kann das Vertrauen der Allgemeinheit in die Zuverlässigkeit der Behörden empfindlich geschädigt werden. Um die Bediensteten der Behörden und sonstigen öffentlichen Stellen in Sachsen auch zukünftig zu ihrer besonderen Pflichtenwahrung sowie Vorbildwirkung zu ermahnen und ihnen die Bedeutung und Reichweite des Datenschutzes zu verdeutlichen, bleibt die Ahndung von Ordnungswidrigkeiten im öffentlichen Bereich unabdingbar.

6.4.2 Ordnungswidrigkeitenverfahren im nichtöffentlichen Bereich

Im Berichtszeitraum verzeichnete meine Behörde 81 neue Ordnungswidrigkeitenanzeigen – die Anzahl bewegte sich damit im Wesentlichen auf dem Niveau des Vorjahres. Fast zwei Drittel der Anzeigen (52) bezogen sich auf die Anfertigung von Videoaufnahmen: stationäre Kameras (34), Dashcams (12), Handy- und Fotoaufnahmen (6). Damit liegt der Schwerpunkt (64 Prozent) der bei mir eingehenden Ordnungswidrigkeitenanzeigen auch weiterhin klar bei der Videoüberwachung (Vorjahr: 56 Prozent).

Insgesamt waren damit im Berichtszeitraum 207 Ordnungswidrigkeitenverfahren anhängig. Von diesen konnte mein Amtsvorgänger 73 Fälle abschließen und dabei 23 Bußgelder festsetzen.

Berichtszeitraum		01.01.–31.12.2021
anhängig gesamt		207
davon	Verfahren aus vorherigem Berichtszeitraum	126
	neu eingegangene Verfahren	81
abgeschlossen		73
davon	mit Bußgeld	23
	eingestellt/von Verfolgung abgesehen	50
noch in Bearbeitung		134
Summe festgesetzte Bußgelder in Euro		7.550

Tabelle 2:
Ordnungswidrigkeitenverfahren im nichtöffentlichen Bereich

Dashcams

19 Bußgelder betrafen den rechtswidrigen Einsatz von Dashcams durch Privatpersonen; ihre Höhe bewegte sich wiederum zwischen 100 und 1.000 Euro (insgesamt 6.250 Euro). Soweit es sich bei Dashcams nur um geringfügige Verstöße gehandelt hat bzw. auf eine Verfolgung des unzulässigen Dashcam-Einsatzes aus anderen Gründen verzichtet worden ist, habe ich die Bußgeldverfahren eingestellt und stattdessen eine Verwarnung nach Art. 58 Abs. 2 Buchst. b Datenschutz-Grundverordnung (DSGVO) ausgesprochen oder einen entsprechenden Hinweis (Art. 58 Abs. 1 Buchst. d DSGVO) erteilt.

Videografie von Privatpersonen

Die verbleibenden vier Bußgelder (insgesamt 1.300 Euro) betrafen gleichfalls Privatpersonen. In drei Fällen ahndete meine Behörde unzulässige Videoaufnahmen. In einem dieser Fälle hatte die Betroffene eine Wildkamera auf ihrem Grundstück installiert, um damit einen Dritten, der sie ihren Aussagen

nach stalkte, zu überführen. Allerdings war die Kamera so ausgerichtet, dass sie auch den öffentlichen Verkehrsraum vor dem Grundstück erfasst und zugleich die Gespräche auf dem unmittelbar daneben befindlichen Nachbargrundstück mit aufgenommen hatte. Die betroffenen Nachbarn bzw. ihre Gäste waren zwar nicht per Bild, dafür aber per Audio erfasst worden und konnten insoweit auch zweifelsfrei identifiziert werden. Da sie keinen Strafantrag gestellt hatten, wurde dieser Sachverhalt als Ordnungswidrigkeit verfolgt. Die beiden anderen Video-Fälle betrafen Videoaufnahmen eines Mieters mit einem Fotoapparat in den Innenhof eines großen Wohngrundstückes sowie heimliche Videoaufnahmen mit einem Mobiltelefon während einer Gerichtsverhandlung. Das vierte Verfahren schließlich richtete sich gegen den ehemaligen Inhaber eines Fitnessstudios, 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.

Durchsuchungs- und Beschlagnahmebeschlüsse

In den Tätigkeitsberichten 2019 (Seite 126ff.) und 2020 (Seite 154ff.) hatte mein Amtsvorgänger von einer Hausdurchsuchung im Zusammenhang mit einem sehr extensiven Einsatz von Dashcams berichtet. Auch im Berichtszeitraum erwirkte meine Behörde in einem Dashcam-Fall einen Durchsuchungs- und Beschlagnahmebeschluss, allerdings war die Ausgangslage hier eine vollkommen andere:
Ausgangspunkt waren verbale, vom Grundsatz her strafbare Beleidigungen des Betroffenen gegen die in einem anderweitigen Einsatz befindliche Besatzung eines Funkstreifenwagens. Im Rahmen der daraufhin vorgenommenen Kontrolle hatte der Betroffene angegeben, dass er mit seiner – permanent im Betrieb befindlichen – Dashcam alles aufgezeichnet habe. Es sei sein gutes Recht, mit der Dashcam im Straßenverkehr zu filmen, und er dürfe dies jederzeit tun. Nachdem infolge des Auftretens des Betroffenen absehbar war,

dass eine Sicherstellung bzw. Beschlagnahme der Dashcam nur unter erheblichem Widerstand und mutmaßlich unter Anwendung unmittelbaren Zwangs erfolgen könnte und zugleich die dringende Abarbeitung des ursprünglichen Einsatzauftrages anstand, wurde von einer Beschlagnahme der Kamera zunächst abgesehen, gleichwohl aber eine diesbezügliche Anzeige erstellt.

Es handelte sich hier also um eine Ordnungswidrigkeitenanzeige, der nicht wie sonst das Beweismittel (Speicherkarte der Dashcam) schon beigefügt war. Stattdessen bestanden aber anderweitig starke Anhaltspunkte für einen unrechtmäßigen Dashcam-Einsatz. Eine Anhörung des Betroffenen hätte sehr wahrscheinlich dazu geführt, dass der Betroffene den Tatvorwurf für die Verwaltungsbehörde unüberprüfbar abstreitet oder dass er die Speicherkarte vor einer Übergabe an die Verwaltungsbehörde löscht oder gleich einen anderen Datenträger übergibt. Eine alternative Ermittlungsmaßnahme war nicht ersichtlich; der Tatvorwurf aber immerhin so schwerwiegend, dass auch eine Einstellung nicht in Betracht kam. Das Ergebnis der Durchsuchung, die sich infolge der Anwesenheit und Kooperationsbereitschaft des Betroffenen auf dessen Fahrzeug und die dort befindliche Dashcam beschränkte, war dann insoweit überraschend, als dass tatsächlich keine relevanten Videoaufnahmen auf der Speicherkarte enthalten waren. Der Betroffene gab an, gegenüber dem Polizisten nur geblufft und die Dashcam lediglich für den Einsatz im Ausland angeschafft zu haben. Das Beispiel zeigt zum einen, dass Durchsuchungen nicht ausschließlich mit dem Ziel des Auffindens belastender Beweismittel durchgeführt werden, sondern natürlich auch dazu führen können, den Betroffenen zu entlasten. Zum anderen wird an diesem Fall deutlich, dass vorschnell geäußerte Behauptungen auch und gerade gegenüber polizeilichen Einsatzkräften mit dem Ziel, diese entsprechend einzuschüchtern, wenig erfolgversprechend sind und schnell ins Gegenteil umschlagen können.

Der zweite Fall, in dem ich einen Durchsuchungs- und Beschlagnahmebeschluss beantragt und vollzogen habe, betraf eine stationäre Videoüberwachung, bei der der Betroffene

der Auffassung war, sich des auskunftsbehördlichen Zugriffs durch die Berufung auf sein Auskunftsverweigerungsrecht entziehen zu können, und in dem ich im Ergebnis wegen fehlender weiterer Aufklärungsmöglichkeiten und fehlender Zutrittsbefugnisse keine andere Wahl hatte, als vom Aufsichts- in das Ordnungswidrigkeitenverfahren überzugehen, vgl. dazu die Ausführungen unter 6.3.1 zur Inanspruchnahme des Auskunftsverweigerungsrechts.

6.4.3 Sanktionierung sogenannter Mitarbeiterexzesse

↗ Art. 25, 83 DSGVO; § 48 SächsDSDG

Mein Amtsvorgänger hatte sich zu den Verfahren bei der Verfolgung Beschäftigter bei Verstößen nach Art. 83 Abs. 5 Datenschutz-Grundverordnung (DSGVO) geäußert, siehe Tätigkeitsbericht 1. April 2017 bis 31. Dezember 2018, Seite 252ff.

Tätigkeitsbericht 2017/2018:
↗ sdb.de/tb2109

Keine Strafe ohne normenklare gesetzliche Grundlage

Sanktioniert werden können nach Art. 83 DSGVO lediglich Verantwortliche, Art. 4 Nr. 7 DSGVO, oder Personen in den Fällen, in denen bereichsspezifische Vorschriften – zum Beispiel landesrechtliche Bußgeldvorschriften – dies bestimmen und für die die Vorschriften des Ordnungswidrigkeitengesetzes (OWiG) dann sinngemäß gelten.
Eine Sanktionierung bedarf jeweils einer normenklaren gesetzlichen Grundlage, die dem Bestimmtheitsgrundsatz genügt.

Voraussetzungen einer Anwendbarkeit von Art. 83 Datenschutz-Grundverordnung

Die nicht zweckgemäße Sichtung oder der Abruf von Informationen in der Infrastruktur des Arbeitgebers oder des Dienstherrn genügt nicht für die Annahme einer Verantwortlichkeit nach der DSGVO. Kumulativ hinzukommen muss, dass die abrufende Person auch über die Mittel der Datenverarbeitung verfügt. Der Beschäftigte ist nicht schon bereits dann Verantwortlicher, wenn er eine gewisse Eigenverantwortung

übertragen bekommen hat, die es ihm gestattet, personenbezogene Daten aus automatisierten Verfahren selbstständig zu sichten bzw. abzurufen, jedenfalls dann nicht, wenn Eigenmacht einer einzelnen Person, die dem Verantwortlichen zuzuordnen ist, nicht ausdrücklich gesetzlich sanktioniert ist, vgl. unten zur Anwendungspraxis. Erforderlich ist also vielmehr auch die Befugnis, über das Mittel zu verfügen, das heißt die dem Verantwortlichen – der Behörde oder dem Unternehmen – obliegende Einhaltung der Datenschutzvorschriften zu organisieren, datenschutzorganisatorische Maßnahmen, Berücksichtigung der Betroffenenrechte etc.

Mitarbeiterexzesse, die ein gewisses Ausmaß erreichen, werden regelmäßig auch im Hinblick auf Art. 25 DSGVO und ungenügende technische und organisatorische Maßnahmen des Verantwortlichen, der dem Beschäftigten den Datenzugang ermöglichte, zu betrachten sein.

Hinzu kommen dürfte in der Praxis, dass die Verfolgbarkeit besonders häufig auftretender reiner „Neugieranfragen" regelmäßig an Art. 2 Abs. 2 Buchst. c DSGVO scheitern sollte.

Der Mitarbeiterexzess kann aber wiederum dann sanktionierbar sein, wenn der die Informationen abrufende Beschäftigte diese mit seinen Datenverarbeitungsgeräten weiterverarbeitet, das heißt, weitere Datenverarbeitungsphasen außerhalb der Arbeitgebersphäre hinzutreten.

Beispiel: Ein Beschäftigter eines Verantwortlichen ruft Namens- und Adressdaten auf, speichert diese auf einem eigenen Datenträger und verarbeitet diese zu Zwecken seiner nebenberuflichen Tätigkeit – Vertrieb von Finanzprodukten – zu Hause auf seinem Heimrechner weiter.

Bisherige gerichtliche Entscheidungen

Mit dem Verwaltungsgericht Dresden und der in seiner Entscheidung vom 5. Februar 2020 (VG Dresden, Urteil vom 05. Februar 2020 – 10 K 372/16.D –, Rdnr. 83 - 85, juris) in Bezug genommenen ständigen Rechtsprechung des Bundesverwaltungsgerichts geht meine Behörde bei der Nutzung dienstlicher Informationssysteme – selbst für dienstfremde, private Zwecke – von einer innerdienstlichen Handlung aus. Dies, insbesondere die Einbindung eines solchen pflichtwidrigen Verhaltens in das Amt und in die damit verbundene dienstliche Tätigkeit (BVerwG, Urteil vom 19. August 2010 – 2 C 5.10 –, juris Rdnr. 9), steht der Annahme entgegen, dass die oder der Beschäftigte als Privatperson und eigener Verantwortlicher

im Sinne von Art. 4 Nr. 7 DSGVO zu behandeln wäre. Dies gilt erst recht für Handlungen, die ausschließlich dienstlichen Zwecken dienen.

Bisher waren zwei andere Gerichtsentscheidungen nach Wirksamwerden der Datenschutz-Grundverordnung bekannt geworden, die zumindest am Rande dazu tendieren, eine eigene Verantwortlichkeit exzessiv handelnder Mitarbeiter anzunehmen, LG Freiburg und VG Mainz. Gerichtsentscheidungen, nach denen bei Mitarbeiterexzessen Art. 83 Datenschutz-Grundverordnung keine Anwendung findet, sind nicht bekannt. Das OLG Dresden vertrat zusätzlich in einer Entscheidung vom 30.11.2021 – 4 U 1158/21 – die Ansicht, dass ein Geschäftsführer eines Verantwortlichen neben dem Verantwortlichen selbst als eigener Verantwortlicher zu betrachten sei.

Anwendungspraxis

Meine Behörde wendet im Hinblick auf Ordnungswidrigkeiten bei öffentlichen sächsischen Stellen ausschließlich landesrechtliche Bußgeldvorschriften an, so die Vorschrift des § 48 Sächsisches Datenschutzumsetzungsgesetz im Richtlinienbereich.

Eine Anwendung von Art. 83 DSGVO auf Mitarbeiter, die bei Gelegenheit der Ausübung ihrer beruflichen Tätigkeit unbefugt nicht offenkundige Daten verarbeitet haben, erfolgt, sofern keine weiteren Verarbeitungsschritte hinzukommen, seitens meiner Behörde aus oben dargestellten Gründen generell nicht. Weitergehendes zu regeln obläge allein dem Verordnungs- bzw. Gesetzgeber.

6.5 Öffentlichkeitsarbeit

6.5.1 Pressearbeit und Online-Kommunikation

Die Presse- und Medienarbeit bleibt ein wichtiges Kommunikationsinstrument für meine Behörde. Dazu gehörte im Berichtszeitraum nicht nur die Beantwortung von Medienanfragen, sondern auch die Veröffentlichung von Pressemitteilungen, beispielsweise zum Registermodernisierungs-

gesetz, Safer Internet Day, Datenschutz in der Schule, zur Prüfung von Medienunternehmen und zu den Gefahren von Cyberattacken.

Seit Juni 2021 können Medieninformationen meiner Behörde über den Medienservice des Freistaates Sachsen kostenfrei abonniert werden.

Pressemitteilungen der SDB:
↗ medienservice.sachsen.de

Journalisten wendeten sich zudem mit ganz unterschiedlichen Fragen an meine Behörde. Vieles stand im Zusammenhang mit der Pandemie und der Digitalisierung. Es ging unter anderem um Datenlecks bei Testzentren, digitale Gesundheitsanwendungen, Bonusprogramme für Geimpfte, Modellprojekte, die Schüler-App Scoolio, die Datenschutzkonformität von Faxgeräten, Videoüberwachung in Chemnitz und vieles mehr.

Ein weiteres wichtiges Kommunikationsinstrument ist meine Website. Im Berichtszeitraum begannen die Vorbereitungen zur Neugestaltung. Parallel stellten die Mitarbeiter meiner Dienststelle regelmäßig auf der bisherigen Plattform Informationen zu aktuellen Themen ein. Einen Schwerpunkt bildete wiederholt der Datenschutz in der Corona-Pandemie. Aber auch Informationen zum Einsatz von Consent-Layern und dem Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) sowie zu vielen anderen datenschutzrechtlichen Fragestellungen wurden veröffentlicht.

Weitere Unterstützung und Hinweise erhielten Interessenten beim Virtuellen Datenschutzbüro, an dem ich mich ebenfalls beteiligte. Dabei handelt es sich um ein Informationsportal für Bürger, das von deutschsprachigen staatlichen, kirchlichen und Rundfunk-Datenschutzbeauftragten betrieben wird.

Virtuelles Datenschutzbüro:
↗ www.datenschutz.de

6.5.2 Schulungen und Vorträge

Im Berichtszeitraum haben Mitarbeiterinnen und Mitarbeiter aus meiner Dienststelle 21 Fortbildungsseminare gehalten, unter anderem an der Sächsischen Verwaltungs- und Wirtschafts-Akademie Dresden, am Fortbildungszentrum des Freistaates Sachsen, beim Landesamt für Schule und Bildung und an einer Schule in Dresden. Hinzu kamen kürzere Vorträge, beispielsweise bei einer Veranstaltung mit der Säch-

sischen Jugendstiftung im November. 35 FSJler (Freiwilliges Soziales Jahr) nahmen daran teil.

Im Vergleich zum Vorjahr war ein leichter Anstieg der Dozententätigkeit zu verzeichnen, begünstigt durch die zunehmende Digitalisierung und ein breiteres Online-Seminarangebot. In der Gesamtschau zu den länger zurückliegenden Jahren ist dennoch ein Rückgang bei der Dozententätigkeit festzustellen. Zu den Ursachen zählen auch die Infektionsschutzmaßnahmen im Zusammenhang mit der Coronavirus-Pandemie, weshalb etliche Veranstaltungen abgesagt wurden. Des Weiteren ist der Rückgang dem hohen Arbeitsaufkommen in der Dienststelle geschuldet.

In den Vorträgen im Berichtszeitraum wurden insbesondere Grundlagen und aktuelle Fragen zur Datenschutz-Grundverordnung behandelt. Auch Datenschutz in Schulen und der Kommunalverwaltung war Thema. Darüber hinaus wurden im Berichtszeitraum verstärkt Grundlagen im Bereich des Beschäftigtendatenschutzes vermittelt.

7 Zusammenarbeit der Datenschutzaufsichtsbehörden, Datenschutzkonferenz

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.

- Chancen der Corona-Warn-App 2.0 nutzen (29.04.2021)
- Impfnachweis, Nachweis negativen Testergebnisses und Genesungsnachweis in der Privatwirtschaft und im Beschäftigungsverhältnis gehören gesetzlich geregelt! (29.03.2021)

7.2 Materialien der Datenschutzkonferenz – Beschlüsse

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

- Zur Möglichkeit der Nichtanwendung technischer und organisatorischer Maßnahmen nach Art. 32 DSGVO auf ausdrücklichen Wunsch betroffener Personen (24.11.2021)

- Verarbeitungen des Datums „Impfstatus“ von Beschäftigten durch die Arbeitgeberin oder den Arbeitgeber (19.10.2021)
- Verarbeitung von Positivdaten von Privatpersonen aus Verträgen über Mobilfunkdienste und Dauerhandelskonten durch Auskunfteien (22.09.2021)
- Energieversorgerpool darf nicht zu gläsernen Verbraucher*innen führen (15.03.2021)

7.3 Materialien der Datenschutzkonferenz – Orientierungshilfen

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

- Häufige Fragestellungen nebst Antworten zur Verarbeitung von Beschäftigtendaten im Zusammenhang mit der Corona-Pandemie (20.12.2021)
- Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von Telemedien ab dem 1. Dezember 2021 (20.12.2021)
- Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail (16.06.2021)
- Einsatz von digitalen Diensten zur Kontaktnachverfolgung anlässlich von Veranstaltungs-, Einrichtungs-, Restaurant- und Geschäftsbesuchen zur Verhinderung der Verbreitung von Covid-19 (29.04.2021)

7.4 Materialien der Datenschutzkonferenz – Stellungnahmen

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

- Verantwortlichkeit bei der Nutzung von Kontaktnachverfolgungssystemen wie der Luca App (21.05.2021)

- Technische Datenschutzanforderungen an Messenger-Dienste im Krankenhausbereich (29.04.2021)
- Kontaktnachverfolgungssysteme – insbesondere zu „Luca" der culture4life GmbH (29.04.2021)
- Kontaktnachverfolgung in Zeiten der Corona-Pandemie – praxistaugliche Lösungen mit einem hohen Schutz personenbezogener Daten verbinden (26.03.2021)
- Evaluierung des BDSG (02.03.2021)

7.5 Materialien der Datenschutzkonferenz – Anwendungshinweise

- Anforderungen an datenschutzrechtliche Zertifizierungsprogramme – Datenschutzrechtliche Prüfkriterien, Prüfsystematik und Prüfmethoden zur Anpassung und Anwendung der technischen Norm DIN EN ISO/IEC 17067 (Programmtyp 6)

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

Der Europäische Datenschutzausschuss verabschiedete die nachstehend aufgeführten Dokumente.

- Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR (18.11.2021)
- Guidelines 10/2020 on restrictions under Article 23 GDPR (13.10.2021)
- Leitlinien zu den Begriffen „Verantwortlicher" und „Auftragsverarbeiter" in der DSGVO (07.07.2021)
- Guidelines 04/2021 on codes of conduct as tools for transfers (07.07.2021)

- Leitlinien 02/2021 zu virtuellen Sprachassistenten – Version 2.0 (07.07.2021)
- Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (18.06.2021)
- Empfehlungen 02/2021 zur Rechtsgrundlage für die Speicherung von Kreditkartendaten ausschließlich zum Zweck der Erleichterung weiterer Online-Transaktionen (19.05.2021)
- Leitlinien 8/2020 über die gezielte Ansprache von Nutzer:innen sozialer Medien (13.04.2021)
- Guidelines 03/2021 on the application of Article 65(1)(a) GDPR (13.04.2021)
- Guidance on certification criteria assessment (Addendum to Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation) (06.04.2021)
- Leitlinien 09/2020 zum maßgeblichen und begründeten Einspruch im Sinne der Verordnung (EU) 2016/679 (09.03.2021)
- Guidelines 02/2021 on Virtual Voice Assistants – Version 1.0 (09.03.2021)
- Leitlinien 01/2020 zur Verarbeitung personenbezogener Daten im Zusammenhang mit vernetzten Fahrzeugen und mobilitätsbezogenen Anwendungen (09.03.2021)
- Empfehlungen 01/2021 zu der Referenzgrundlage für den Begriff „Angemessenheit" in der Richtlinie zum Datenschutz bei der Strafverfolgung (02.02.2021)
- Guidelines 01/2021 on Examples regarding Data Breach Notification (19.01.2021)

7.7 Gemeinsame Überprüfung von Medienunternehmen durch Datenschutzaufsichtsbehörden

↗ Art. 6, 28 DSGVO

Tätigkeitsbericht 2020:
↗ sdb.de/tb2020

Bereits im Tätigkeitsbericht 2020 (Ziffer 7.8, Seite 164) hat mein Amtsvorgänger 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 2021 wurden die Fragebögen in den verschiedenen 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 Prüfung 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: Datentransfers ins außereuropäische Ausland, einzelne Lösungen zur Herbeiführung einer Zustimmungsentscheidung sowie Drittdienste und deren Erforderlichkeit. Mein Amtsvorgänger hat deutlich gemacht, an welchen Punkten er Änderungen für erforderlich hält und dass er auch Argumente der Medienhäuser zur Finanzierung von Online-Journalismus zur Kenntnis genom-

men hat. 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 bislang Fristverlängerungen zur Umsetzung der aus technischer und geschäftsprozessualer Sicht recht komplexen Änderungen gewährt wurden, 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 befassen müssen.

Was ist zu tun?
Medienunternehmen sind gehalten, die bestehenden Geschäftsmodelle und dabei insbesondere die Weitergabe der Daten von Nutzern auf den Prüfstand zu stellen. Dies erfordert eine genaue Prüfung aller eingesetzten Dienste sowie deren Datenverwendung durch Cookies und ähnliche Techniken.

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

8.1 Aufgaben des GKDZ nach § 4 GKDZ-StV

Seit mittlerweile einigen Jahren begleite ich den Prozess der Errichtung eines Gemeinsamen Kompetenz- und Dienstleistungszentrums der Polizeien der Länder Berlin, Brandenburg, Sachsen, Sachsen-Anhalt und Thüringen auf dem Gebiet der polizeilichen Telekommunikationsüberwachung als rechtsfähige Anstalt öffentlichen Rechts (GKDZ).
Das GKDZ soll künftig als zentraler Dienstleister der Trägerländer auf dem Gebiet der polizeilichen Telekommunikationsüberwachung Daten aus Telekommunikationsüberwachungsmaßnahmen nach den jeweiligen Landespolizeigesetzen sowie nach den §§ 100a ff. Strafprozessordnung (StPO) im Wege der Auftragsverarbeitung für die Polizeien der Trägerländer verarbeiten.
Die Trägerländer unterzeichneten am 8. September 2017 den Staatsvertrag über die Errichtung des GKDZ (GKDZ-StV), den die Parlamente der Trägerländer nachfolgend bestätigten. Der Sächsische Landtag stimmte dem Staatsvertrag per Gesetz vom 13. Dezember 2017 zu.

Position der Landesdatenschutzbeauftragten der Trägerländer

Im Zuge der Beteiligung der Landesdatenschutzbeauftragten der Trägerländer an der Planung des GKDZ zeichnete sich bereits im Jahr 2019 ein Dissens zwischen dem GKDZ und den Landesdatenschutzbeauftragten hinsichtlich der dem GKDZ per Staatsvertrag übertragenen Aufgaben ab, der auch im

Berichtszeitraum nicht aufgelöst werden konnte und meinen Amtsvorgänger sowie meine Amtskollegen veranlasste, die Innenressorts der Trägerländer als Inhaber der Rechtsaufsicht über das GKDZ über unsere Position zu informieren:
Maßgeblich für die Bestimmung der Aufgaben, deren Erfüllung dem GKDZ als einer hoheitlich tätigen Anstalt öffentlichen Rechts zugewiesen ist, ist § 4 GKDZ-StV. Danach benutzen die Trägerländer die Anstalt im Wege der Auftragsverarbeitung für Daten aus polizeilichen Telekommunikationsüberwachungen nach den jeweiligen Landespolizeigesetzen sowie nach den §§ 100a ff. StPO (Kernaufgabe), § 4 Abs. 1 Satz 2 GKDZ-StV. Nachfolgend wird in § 4 Abs. 1 Satz 3 GKDZ-StV der Begriff der Telekommunikationsüberwachung definiert:

> „Telekommunikationsüberwachung ist die Verarbeitung von Nutzungs-, Inhalts-, Verkehrs-, Bestands- und Standortdaten zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten sowie des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit."

Danach ist ausgeschlossen, dass die Aufgaben des GKDZ sich auf eine Auftragsverarbeitung von Daten aus polizeilichen bzw. strafprozessualen Maßnahmen erstrecken könnten, die in keinem Zusammenhang mit Telekommunikationsvorgängen und/oder Telekommunikationsüberwachung stehen.
Daten, die etwa im Wege der Online-Durchsuchung (§ 100b StPO bzw. entsprechende landespolizeirechtliche Regelung) aus informationstechnischen Systemen erhoben werden, sind keine Telekommunikationsdaten im Sinne von § 4 Abs. 1 Satz 3 GKDZ-StV. Ebenso wenig handelt es sich bei Daten, die bei der akustischen Wohnraumüberwachung, § 100c StPO, der akustischen Überwachung außerhalb von Wohnraum, § 100f StPO, und weiteren Maßnahmen außerhalb von Wohnraum nach § 100h StPO erhoben werden, um Telekommunikationsdaten. Gleiches gilt für Daten, die im Wege der Sicherstellung bzw. Beschlagnahme nach §§ 94, 98 und 99 StPO (Postbeschlagnahme) erhoben wurden. Die nach diesen Vorschriften bzw. den entsprechenden landespolizeirecht-

lichen Befugnissen erhobenen Daten stammen nicht aus Telekommunikationsvorgängen und können daher nicht im Wege polizeilicher Telekommunikationsüberwachung gewonnen worden sein; ihre (Auftrags-)Verarbeitung durch das GKDZ ist von der Aufgabenzuweisung in § 4 GKDZ-StV nicht umfasst. Dasselbe gilt für Daten aus der Elektronischen Aufklärung der Landespolizei. Auch unter Berücksichtigung der aus Sicht des GKDZ system- und entwicklungsoffenen Ausgestaltung des § 4 Abs. 1 GKDZ-StV und der Rechtsprechung des Bundesverfassungsgerichts zum entwicklungsoffenen Fernmeldegeheimnis ist eine Qualifikation von Vorgängen und Aktivitäten, die etwa über §§ 100c, 100f und 100h StPO in einem Ermittlungsverfahren kriminalpolizeilich erfasst werden, als „Telekommunikation" unter keinem rechtlichen, tatsächlichen oder technischen Gesichtspunkt möglich. Werden Datenträger sichergestellt oder beschlagnahmt, liegt hinsichtlich der in ihnen enthaltenen Daten eine Datenerhebungsmaßnahme in Form der „Sicherstellung" oder „Beschlagnahme" vor, die auch unter Aufbietung größter Fantasie nicht als Maßnahme der Telekommunikationsüberwachung qualifiziert werden kann.

Auslegung des Begriffs der Telekommunikation

Zwar ist aus Sicht des Bundesverfassungsgerichts (BVerfG) der Begriff des Fernmeldegeheimnisses entwicklungs- und technologieoffen, zugleich betont das Gericht aber, dass nur „mit Hilfe der verfügbaren Telekommunikationstechniken erfolgende Übermittlungen von Informationen" erfasst werden (BVerfG, 9.10.2002, Az.: 1 BvR 1611/96, 1 BvR 805/98). Derartige Informationsübermittlungen finden in Sachverhalten, in denen §§ 100b, 100c, 100f, 100h und 94, 98, 99 StPO zur Anwendung kommen, schlicht nicht statt.

Eine Auslegung der Begriffe der Telekommunikation und der Telekommunikationsüberwachung völlig losgelöst vom allgemeinen Verständnis, von gesetzlichen Definitionen und von der verfassungsgerichtlichen Rechtsprechung verbietet sich für eine an Gesetz und Recht gebundene Anstalt des öffentlichen Rechts als Auftragsverarbeiter ebenso wie für

Strafverfolgungs- und Gefahrenabwehrbehörden als datenschutzrechtlich Verantwortliche, die das GKDZ im Wege der Auftragsverarbeitung nutzen.
Das Sächsische Staatsministerium der Justiz und für Demokratie, Europa und Gleichstellung teilt diese Auffassung.
Damit setzt § 4 Abs. 1 GKDZ-StV den Rahmen, in dem das GKDZ tätig werden und personenbezogene Daten der von polizeilichen Eingriffsmaßnahmen betroffenen Personen verarbeiten darf. Zugleich bestimmt § 4 Abs. 1 GKDZ-StV, dass die Erfüllung der Kernaufgabe im Wege der Auftragsverarbeitung erfolgt. Die Erfüllung anderer Aufgaben, die mit Grundrechtseingriffen verbunden sind – die Erbringung von Unterstützungs- und Beratungsleistungen nach § 4 Abs. 2 GKDZ-StV ist hiervon nicht erfasst –, ist dem GKDZ als öffentlicher Stelle mangels gesetzlicher Aufgabenzuweisung verwehrt. Dies gilt für Tätigkeiten außerhalb des in § 4 Abs. 1 GKDZ-StV bestimmten Bereichs auch dann, wenn sie ebenso wie die Kernaufgabe im Wege der Auftragsverarbeitung ausgeführt werden sollen, da die gesetzliche Vorschrift bestimmt, dass (nur) die zugewiesene Aufgabe im Wege der Auftragsverarbeitung erfüllt wird. Für das GKDZ heißt das, dass eine Auftragsverarbeitung von Daten, die nicht aus polizeilicher Telekommunikationsüberwachung stammen, gesetzlich nicht vorgesehen und mithin unzulässig ist.

Keine eigenmächtige Erweiterung des gesetzlichen Aufgabenspektrums

Es steht einer öffentlichen Stelle, der durch den Gesetzgeber genau bestimmte Aufgaben zugewiesen wurden, nicht zu, diesen – hier in § 4 GKDZ abschließend formulierten – Aufgabenkatalog eigenmächtig zu erweitern. Einer Auftragsverarbeitung außerhalb des gesetzlich festgelegten Rahmens stünde daher der klare Wille des bzw. der Gesetzgeber entgegen; auch eine Vereinbarung zwischen zwei Stellen der Exekutive vermöchte eine solche durch die Legislative bestimmte (und beschränkte) Aufgabenzuweisung nicht zu umgehen.

Was ist zu tun?
Das GKDZ hat sich bei der Verarbeitung personenbezogener Daten im Wege der Auftragsverarbeitung auf die ihm nach § 4 GKDZ-StV gesetzlich zugewiesenen Aufgaben zu beschränken.

Sollte der Wunsch der Trägerländer bestehen, dem GKDZ weitere mit Grundrechtseingriffen verbundene Aufgaben zu übertragen, stünde es ihnen und zuvörderst ihren Parlamenten selbstverständlich frei, durch eine Änderung des Staatsvertrages das Aufgabenspektrum des GKDZ zu erweitern.
Ich werde gemäß meiner gesetzlichen Aufgabe die mir zur Verfügung stehenden Befugnisse nutzen, um die Einhaltung datenschutzrechtlicher Vorschriften durch das GKDZ – hier die Verarbeitung hoheitlich erhobener Daten nur im durch den Gesetzgeber bestimmten Umfang – durchzusetzen.

8.2 Einsatz eines Programms mit Gesichtserkennung für die Strafverfolgung durch die Polizeidirektion Dresden

↗ § 48 BDSG, § 163 StPO

Durch Medienberichte wurde meine Behörde darauf aufmerksam, dass die Polizeidirektion Dresden zur strafprozessualen Aufklärung einer großen Zahl von zum Teil erheblichen Straftaten im Zusammenhang mit den Krawallen um ein Fußballspiel der Sportgemeinschaft Dynamo Dresden am 16. Mai 2021 ein Programm mit Gesichtserkennungsfunktion einsetzt.
Die hierauf abzielenden datenschutzrechtlichen Fragen beantwortete die Polizeidirektion im Rahmen eines Gesprächs und der Vorführung des Programms. Daneben wurde eine Datenschutz-Folgenabschätzung nach § 67 Bundesdatenschutzgesetz (BDSG) vorgelegt.
Die Vorgehensweise der Polizei stellt sich danach folgendermaßen dar.
Aufgrund der Ereignisse am Nachmittag des 16. Mai 2021, in deren Verlauf aus einer großen Personenmenge heraus massive Übergriffe auf Polizeibeamte und erhebliche Sachbeschädigungen verübt wurden, wurde in der Polizeidirektion Dresden eine Sonderkommission zur strafrechtlichen Aufklärung eingesetzt.

Bildaufnahmen aus verschiedenen Quellen

Während der Krawalle hatten Polizeibeamte Videoaufnahmen auf Grundlage des Sächsischen Polizeivollzugsdienstgesetzes (SächsPVDG) und der Strafprozessordnung (StPO) gefertigt. Im Nachgang sicherte die Polizei die Tatzeiträume betreffende Videoaufnahmen von an den Tatort angrenzenden Videoüberwachungsanlagen (zum Beispiel der des Rudolf-Harbig-Stadions). Des Weiteren speicherten die Ermittler Aufnahmen der Ausschreitungen in öffentlich zugänglichen Video- und Social-Media-Plattformen Youtube und Facebook. Daneben wurde ein Hinweisportal freigeschaltet, auf dem Zeugen oder sonstigen Dritten die Möglichkeit eröffnet wurde, Multimediadaten zu den Vorfällen zu hinterlegen.
Die erhobenen und gespeicherten Bilddaten werden sodann gemeinsam gespeichert und in einen Ort-Zeit-Bezug gebracht, der die Suche nach einem bestimmten (Tat-)Ort oder einer (Tat-)Zeit ermöglicht.

Software generiert biometrische Daten

Durch die eingesetzte Software werden aus den erhobenen Bilddaten automatisiert Gesichts- und Körperbilder detektiert, die im Rahmen nachfolgender – manuell auszulösender – Abgleiche verwendet werden. Im Zuge der Speicherung werden dabei die Bildaufnahmen automatisiert indiziert, indem eine Rasterung des Bildmaterials und die Bestimmung signifikanter Punkte von im Sinne der Gesichtsdetektion relevanten Mustern erfolgen, die in einem nächsten Schritt eine Identifikation bzw. den Abgleich erlauben.
Im Rahmen der Datenverarbeitung werden softwarebasierte Algorithmen für automatisierte Verarbeitungsschritte von personenbezogenen Daten zum Zwecke der Gesichtsdetektion und der Gesichtsidentifikation auf Grundlage biometrischer Daten (Gesichtsbilder) verwendet.
Automatisierte Gesichtsdetektion beschreibt das technische Verfahren, bei dem automatisiert und nicht individualisiert in einem Bild, einer Bildfolge oder einem Video nach vorhandenen Gesichtsmustern gesucht wird. Durch dieses tech-

nische Verfahren werden zum Abgleich geeignete Gesichtsbilder berechnet. Von besonderer Bedeutung sind hierbei Merkmale des Gesichtes, die auf Grund der Mimik wenigen Veränderungen unterliegen (zum Beispiel Kanten der Augenhöhlen, Seitenpartien des Mundes, ...). Das Ergebnis der Berechnung wird als „Template" bezeichnet.

Auf Gesichtsdetektion folgt Gesichtsidentifikation

Die Gesichtsdetektion ist eine erforderliche technische Vorstufe für die nachfolgende automatisierte Gesichtsidentifikation. Dieser Verarbeitungsschritt erfasst sämtliche Personen bzw. vom Programm im Bildmaterial erkannte Gesichter bzw. Gesichtsmuster; unerheblich ist dabei, ob die betroffene Person bei strafrechtlich relevanten Handlungen gezeigt wird.
Die Gesichter bzw. die daraus errechneten „Templates" werden programmintern in einer Referenzdatenbank abgelegt, mit der im Folgenden von den Ermittlern vorgelegte Referenzdaten/Identitäten im Wege der automatisierten Gesichtsidentifikation abgeglichen werden.
Automatisierte Gesichtsidentifikation beschreibt das technische Verfahren, bei dem aus Bilddaten durch Gesichtsdetektion indizierte Gesichtsbilder mit Gesichtsbildern aus Referenzdaten automatisiert abgeglichen werden. Im Ergebnis des – nach manuellem Auftrag erfolgenden – automatisierten Verfahrens der Gesichtsidentifikation wird eine Übereinstimmung der abgeglichenen Gesichtsbilder errechnet. Abhängig von der errechneten Übereinstimmung wird ein Trefferfall angezeigt.
Bilder oder Videos von den Ermittlern bekannten Personen, die am Einsatztag durch erkennungsdienstliche Behandlung oder Ähnliches identifiziert wurden, können als Referenzdaten (Identität) in dem Programm gespeichert und analysiert werden. Nach ihnen kann in der Folge gezielt gesucht werden, um be- und entlastendes Videomaterial zu finden.
Werden in den gesicherten Daten bis dahin unbekannte Personen festgestellt, bei denen aufgrund der Aufnahmen hinreichende tatsächliche Anhaltspunkte für eine verfolgbare Straftat oder Ordnungswidrigkeit vorliegen, kann das detek-

tierte Gesicht/Objekt (Körper) als Referenzdatei (Identität) angelegt werden und somit nach weiterem Videomaterial mit der Person gesucht werden.

Nach einem Abgleich der Referenzbilder mit dem gesamten Bildmaterial (Referenzdatenbank) zeigt das System in Bezug auf die gesuchte Identität Gesichter mit einer hohen mathematisch errechneten Ähnlichkeit an (Treffer). Die maximale Trefferanzahl lässt sich durch den Benutzer einstellen. Die Sortierung erfolgt anhand der errechneten Wahrscheinlichkeit, sortiert von der höchsten zur niedrigsten. Das System entscheidet nicht automatisch, dass eine Übereinstimmung vorliegt. Es handelt sich lediglich um eine Vorsortierung, um die anschließende manuelle Verifizierungsprüfung zu erleichtern.

Die Prüfung der sachlichen Richtigkeit des Trefferfalls nimmt ein Bediensteter durch vergleichende Inaugenscheinnahme der angelegten Identität mit den errechneten Abgleichbildern vor (manuelle Verifizierungsprüfung).

„Trefferbilder", bei denen die manuelle Verifizierungsprüfung den Trefferfall nicht bestätigt hat, werden automatisch nach Beendigung der Suche in der gesonderten Trefferdatei gelöscht; die Löschung betrifft allerdings nicht die Daten der Referenzdatenbank.

Technisch-organisatorischer Schutz der Daten

Die Servertechnik, auf der die Anwendung die gesicherten Daten analysiert, um einen Abgleich mit den Referenzdaten durchzuführen, wird getrennt von sonstigen Datensystemen in einem abgeschlossenen Bereich betrieben. Einsicht in die Daten haben nur die mit dem Sachverhalt betrauten Ermittler und Videoauswerter. Neben dem Zugang auf Dateiebene, der für die Ermittler des Verfahrens zugänglich ist, ist ein weiterer Zugang (Nutzername, Kennwort) zur Bearbeitung des Falls mit der Software notwendig.

Die Polizeidirektion sieht die Rechtsgrundlage für die Erhebung, die Speicherung, den Abgleich und die Löschung der Bilddaten in der Strafprozessordnung (StPO), die auch den rechtlichen Rahmen bilde, innerhalb dessen die Bilddaten im

Trefferfall weiterverarbeitet werden dürfen. Die Grundlage speziell für das Anlegen und Nutzen der Referenzdatenbank, die die Daten bzw. Bilder enthält, mit denen das gespeicherte Bildmaterial der strafrechtlich relevanten Vorgänge abgeglichen wird, liege in § 163 Abs. 1 StPO in Verbindung mit §§ 48 Abs. 1, 46 Nr. 14 Buchst. c BDSG.

Rechtlicher Rahmen

Obgleich ich die Verarbeitung biometrischer Daten, insbesondere in Form der automatisierten Gesichtserkennung und im Rahmen polizeilicher Aufgabenerfüllung, aus datenschutzrechtlicher Sicht grundsätzlich als kritisch und riskant erachte, habe ich in eng begrenzten Anwendungsfällen gegen den Einsatz einer Software, die biometrische Merkmale betroffener Personen innerhalb von rechtmäßig erlangtem Beweismaterial generiert und abgleicht, keine durchgreifenden Bedenken. Der Einsatz der Software in der konkreten, seitens der Polizeidirektion beschriebenen Art und Weise ist nicht zu beanstanden.

Das im Verfahren genutzte Bildmaterial von den Krawallen am 16. Mai 2021 dürfte auf Grundlage der §§ 161 Abs. 1, 163 Abs. 1 StPO rechtmäßig erhoben worden sein, soweit die Polizei selbst die Aufnahmen zur Beweissicherung gefertigt hat. Bildaufnahmen, die die Polizei vor Ort zur Gefahrenabwehr auf Grundlage von § 57 Abs. 2 SächsPVDG gefertigt hat, darf sie nach § 79 Abs. 2 SächsPVDG zur Verfolgung der dort begangenen Straftaten verwenden. Bildmaterial Dritter konnte sie rechtmäßig auf Grundlage von § 94 Abs. 1 StPO sicherstellen.

Die Verarbeitung dieser Daten in Form der Speicherung sowie des Auslesens, Verwendens und Abgleichens (§ 46 Nr. 2 BDSG) kann auf § 163 Abs. 1 StPO gestützt werden. Diese Vorschrift erlaubt aber nicht ohne Weiteres die Verarbeitung biometrischer Daten (§ 46 Nr. 12 BDSG), wie sie die Polizeidirektion Dresden mittels der oben beschriebenen Software vornimmt. Dienen biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person (§ 46 Nr. 14 Buchst. c BDSG), ist ihre Verarbeitung nach § 48 Abs. 1 BDSG nur zu-

lässig, wenn sie zur Aufgabenerfüllung „unbedingt erforderlich" ist (§ 48 Abs. 2 BDSG).

Eine Verarbeitung ist dann „unbedingt erforderlich", wenn sie für die Aufgabenerfüllung beinahe unverzichtbar erscheint. Diese Voraussetzung sehe ich im vorliegenden Fall als erfüllt an. Der Staat unterliegt der Verpflichtung zu einer effektiven Strafverfolgung, gleichzeitig muss sein Handeln stets verhältnismäßig sein. Liegen den Strafverfolgungsbehörden Bildaufnahmen von mutmaßlichen schwerwiegenden, auch gegen Personen gerichteten Straftaten vor, sind sie verpflichtet, diese Taten aufzuklären. Wenn wegen der Zahl der abgebildeten Rechtsverstöße und des Umfangs des Bildmaterials eine rein „menschliche" Sichtung des Materials einen unverhältnismäßig langen Zeitraum in Anspruch nehmen und damit eine effektive Strafverfolgung praktisch vereitelt würde, ist der Einsatz zur Verfügung stehender technischer Hilfsmittel zur Sichtung und Auswertung des Bildmaterials und mithin zur zeitnahen Aufklärung der Straftaten für die der Polizei und der Staatsanwaltschaft obliegenden Aufgabe der Strafverfolgung „unbedingt erforderlich" im Sinne von § 48 Abs. 1 BDSG.

Allerdings fordert § 48 Abs. 2 BDSG – parallel zum bzw. in Ausformung des stets zu beachtenden Verhältnismäßigkeitsgrundsatzes – bei der Verarbeitung besonderer Kategorien personenbezogener Daten geeignete Garantien für die Rechtsgüter der betroffenen Personen.

Die Vorgehensweise der Polizeidirektion Dresden und die ihrerseits getroffenen Vorkehrungen zur Minimierung von Risiken für auf den verwendeten Aufnahmen abgebildete, biometrisch erfasste und mithin in den systemseitig erfolgenden Abgleich einbezogene Personen begegnet insoweit keinen durchgreifenden Bedenken. Erhebliche Zweifel allerdings habe ich hinsichtlich der Geeignetheit der Vorschrift des § 48 BDSG als allgemeine Befugnisnorm für den Einsatz von Gesichtserkennungssoftware im Bereich der Strafverfolgung. Die Vorschrift gibt im Wesentlichen lediglich den Wortlaut von Art. 10 der Richtlinie (EU) 2016/680 wieder und führt mögliche Maßnahmen zum Schutz Betroffener nur beispielhaft auf. Hinsichtlich anderer Verarbeitungssituatio-

nen und mit Blick auf andere Kategorien besonders schützenswerter Daten kann das ausreichend sein; als Grundlage für das Generieren biometrischer Daten von unter Umständen Hunderten oder gar Tausenden, größtenteils an Straftaten unbeteiligten Betroffenen und deren intensive Verwendung in Form von wiederholten Abgleichen dürfte § 48 BDSG die Anforderungen an eine hinreichend bestimmte, klare und verhältnismäßige Eingriffsnorm nicht erfüllen.
Meine Bewertung kann daher nur für den konkreten Einsatz des Programms mit Gesichtserkennungsfunktion im konkreten Ermittlungsverfahren zu den Krawallen am 16. Mai 2021 am Rudolf-Harbig-Stadion in Dresden gelten.

Risiken beim Einsatz automatisierter Gesichtserkennung

Eine generelle datenschutzrechtliche Unbedenklichkeit kann der Verwendung der Software hingegen nicht attestiert werden. Ganz im Gegenteil zeigt die Beschreibung des Verfahrens, dass Programme mit automatisierter Gesichtserkennungsfunktion nur unter strenger Beachtung der Verhältnismäßigkeit eingesetzt werden dürfen. Der Grund hierfür liegt in der großen Zahl von der Verarbeitung betroffener Personen, die weder gefahrenabwehrrechtlich als Störer noch strafrechtlich als Tatverdächtige in Erscheinung treten, sondern lediglich zufällig und als Unbeteiligte im Bildmaterial auftauchen, das polizeirelevantes Verhalten Einzelner abbildet. Auch diese unbeteiligten Dritten werden – wie eben ausnahmslos alle auf den Bildern erfassten Personen – einer polizeilichen Verarbeitung ihrer Daten unterzogen, wobei diese Verarbeitung biometrische Daten und damit eine besondere, das heißt eine besonders schützenswerte Kategorie personenbezogener Daten betrifft.
Die systemimmanente Erstellung und Indizierung von Abgleichdaten, die bereits im Zuge der Speicherung ermittlungsrelevanten Bildmaterials erfolgt und ausnahmslos alle abgebildeten Personen betrifft und erst die Grundlage für Resultate in später vorzunehmenden Abgleichen ist, erzeugt eine – temporäre – Datenbank mit biometrischen Daten sämtlicher in den Aufnahmen abgebildeter Personen.

Die damit einhergehende Eingriffstiefe hinsichtlich des Grundrechts der Betroffenen auf informationelle Selbstbestimmung ist erheblich – es werden nicht allein sie betreffende Bildaufnahmen gespeichert, sondern daraus auch sie betreffende biometrische Daten gewonnen und verarbeitet –, die Risiken liegen auf der Hand. Die Technik ermöglichte bei einer nicht begrenzten Nutzung von aus Bildaufnahmen aus (zahlreichen) verschiedenen Verfahren und verschiedenen Quellen generierten biometrischen Abgleichdaten eine zügige Vergleichbarkeit und personenbezogene Recherche, die zeitlich und örtlich umso umfassender würde, je länger Bild- und Abgleichdaten aufbewahrt und verfahrensübergreifend zur Verfügung stehen würden. Die Erstellung detaillierter individueller Verhaltens- und Bewegungsprofile wäre ohne größeren Aufwand möglich.

Eine solche Verarbeitung personenbezogener Daten – hinsichtlich unbeteiligter bzw. nicht in verifizierten Trefferfällen identifizierter Personen erfolgte diese „auf Vorrat" und damit rechtswidrig – wäre klar verfassungswidrig (vgl. hierzu die Rechtsprechung des Bundesverfassungsgerichts zur automatisierten Kennzeichenerfassung und der Pflicht zur unverzüglichen, spurenlosen Löschung von „Nichttreffern", BVerfG, 18.12.2018, Az.: 1 BvR 142/15, Rdnr. 97, 98).

Die Verwendung von Abgleichdaten, die auf biometrischen Merkmalen beruhen, muss deshalb strikt auf das konkrete Ermittlungsverfahren beschränkt bleiben. Eine Löschung dieser Daten, die in aller Regel größtenteils Unbeteiligten zuzuordnen sein werden, muss spätestens mit Abschluss der Auswertung der als beweiserheblich gespeicherten Bildaufnahmen erfolgen.

Mindestanforderungen an den Einsatz von Gesichtserkennungssoftware

Folgende Anforderungen betrachte ich vor diesem Hintergrund als unabdingbar für den Einsatz von Gesichtserkennungssoftware zum Zweck der Strafverfolgung, beschränkt auf ein einzelnes Ermittlungsverfahren:

- Der Einsatz von Programmen mit automatisierter Gesichtserkennung ist auf Vorgänge von strafrechtlich erheblichem Gewicht zu beschränken, die aufgrund der Einzelumstände auf anderem Weg nicht oder nur mit unverhältnismäßig hohem zeitlichem Aufwand aufgeklärt werden könnten.
- Um Eingriffe in das Recht auf informationelle Selbstbestimmung betroffener Personen so gering wie möglich zu halten, muss bereits bei der Entscheidung, welches Bildmaterial in die Auswertung einbezogen wird, streng auf Erforderlichkeit und Verhältnismäßigkeit geachtet werden (§ 47 Nr. 3 BDSG).
- Bei der Vorauswahl des einzubeziehenden Bildmaterials ist deshalb eine enge örtliche und zeitliche Beschränkung vorzunehmen; Aufnahmen, die außerhalb des Tatortes bzw. seiner unmittelbaren Umgebung und außerhalb des Tatzeitraums erhoben wurden, müssen unberücksichtigt bleiben.
- Ein Abgleich mit Bildern, die keinen solch engen Ort- und Zeitbezug zum Tatgeschehen haben, muss unterbleiben (das betrifft insbesondere nicht tatbezogene Bilddaten aus Social-Media-Kanälen und nicht unmittelbar tatbezogene Aufnahmen behördlicher und privater Videoüberwachungsanlagen zum Beispiel auf öffentlichen Plätzen, Bahnhöfen oder im Personennahverkehr).
- Die Referenzdatenbank darf nicht mit anderen Dateien oder Erkenntnisquellen vernetzt werden (§ 48 Abs. 2 Nr. 5 BDSG).
- Die in der Referenzdatenbank gespeicherten Templates dürfen nicht für andere Zwecke als den Bildabgleich im konkreten Verfahren verwendet werden; eine verfahrensübergreifende Nutzung der Abgleichdaten aus der Referenzdatenbank ist unzulässig.
- Eine internetbasierte Anwendung („Cloud-Anwendung") ist unzulässig, die Technik ist getrennt von sonstigen Datensystemen zu betreiben.

- Eine Übermittlung/Offenlegung personenbezogener Daten gegenüber dem Hersteller des Programms oder sonstigen Dritten, auch im Rahmen von Support- oder Wartungsarbeiten, ist unzulässig.
- Der Zugriff auf die Anwendung und die Referenzdatenbank ist auf einen möglichst kleinen, klar definierten Personenkreis zu begrenzen.
- Die Referenzdatenbank ist spätestens mit Abschluss der Auswertung des Bildmaterials zu löschen.
- Bilddaten, die aufgrund vermeintlicher, tatsächlich aber nicht verifizierter Übereinstimmung (falsch positive Treffer) erstellt wurden, sind unverzüglich zu löschen.
- Maßnahmen, die Auswirkungen auf einzelne Betroffene haben, dürfen nicht aufgrund „systemseitiger" Signale, das heißt allein aufgrund eines Rechenprozesses und ohne menschliche Kontrolle und Entscheidung ergriffen werden (§ 54 BDSG).

Unter diesen Bedingungen halte ich den Einsatz einer Software mit Gesichtserkennungsfunktion für Zwecke der Strafverfolgung in einem konkreten Ermittlungsverfahren für datenschutzrechtlich vertretbar.
Angesichts der – auch bei Einhaltung der genannten hohen Anforderungen – Eingriffstiefe der Maßnahme und ihrer potenziell großen Streubreite sowie der Unbestimmtheit der Vorschrift des § 48 BDSG würde eine normenklare gesetzliche Regelung zum Einsatz von Gesichtserkennungssoftware für Rechtssicherheit bei den Strafverfolgungsbehörden sorgen und könnte gleichzeitig das Risiko unverhältnismäßiger Beeinträchtigung für betroffene Personen minimieren. Ich halte die Schaffung einer entsprechenden Rechtsgrundlage für geboten.

Was ist zu tun?
Der Einsatz von Programmen mit automatisierter Gesichtserkennung in der Strafverfolgung ist nur unter engen Grenzen und nicht verfahrensübergreifend zulässig.

9 Rechtsprechung zum Datenschutz

9.1 Schmerzensgeld für jeden Verstoß gegen die DSGVO?

↗ Art. 9 DSGVO, Art. 82 Abs. 1 DSGVO

Derzeit befasst sich der Europäische Gerichtshof nach einem Vorlagebeschluss des Bundesarbeitsgerichts (Beschluss vom 26.8.21 – 8 AZR 253/20) unter anderem mit den Fragen, ob Art. 82 Abs. 1 Datenschutz-Grundverordnung (DSGVO) spezial- beziehungsweise generalpräventiven Charakter hat. Geprüft wird auch, ob dies bei der Bemessung der Höhe eines zu ersetzenden immateriellen Schadens nach Art. 82 DSGVO zulasten des Verantwortlichen beziehungsweise Auftragsverarbeiters berücksichtigt werden muss und ob es bei der Bemessung der Höhe eines zu ersetzenden immateriellen Schadens auf den Grad des Verschuldens des Verantwortlichen beziehungsweise Auftragsverarbeiters ankommt. Das Bundesarbeitsgericht ist dabei der Auffassung, dass die betroffene Person keine Folgen von zumindest einigem Gewicht erlitten haben muss, sondern dass ein Verstoß gegen die Datenschutz-Grundverordnung selbst einen auszugleichenden immateriellen Schaden darstellt. Ähnliche Vorlagebeschlüsse haben der Österreichische Oberste Gerichtshof (Beschluss vom 15.4.2021 – 6 Ob 35/21x –; ZD 2021, 631) sowie der Oberste Verwaltungsgerichtshof Bulgariens gefasst (Europäischer Gerichtshof, Rechtssache C-340/21).

Zugrunde liegt diesen Vorlagefragen ein Fall aus dem Arbeitsrecht. Ein Mitarbeiter eines Medizinischen Dienstes einer Krankenkasse wurde sieben Monate nach Beginn einer Erkrankung im Auftrag seiner Krankenkasse wegen Zweifel

an seiner Arbeitsunfähigkeit von seinem Arbeitgeber gesundheitlich begutachtet. Eine Ärztin seines Arbeitsgebers stellte eine „schwere Depression ohne psychotische Symptome" fest. Der Kläger erfuhr von seinem behandelnden Arzt, dass dieser von der Gutachterin kontaktiert worden war. Eine Kollegin aus der IT-Abteilung bestätigte dem Kläger, dass im digitalen Archiv seines Arbeitgebers ein Gutachten über ihn gespeichert sei und fotografierte es für ihn. Dem Kläger und seiner Kollegin wurde im Laufe des Rechtsstreits gekündigt. Der Kläger verklagte seinen Arbeitgeber auf materiellen und immateriellen Schadensersatz wegen Verletzungen datenschutzrechtlicher Bestimmungen im Arbeitsverhältnis.
Die Antwort auf die Vorlagefragen wird auch für Sachsen von erheblicher Bedeutung sein. Denn würde ein bloßer Verstoß gegen die Datenschutz-Grundverordnung ohne das Vorliegen oder den Nachweis eines Schadens als Grund für Schadensersatz ausreichen, wäre dies sehr betroffenenfreundlich und könnte zu einer Klagewelle wie im sogenannten Dieselskandal führen.

Was ist zu tun?
Die Entscheidung des EuGH bleibt abzuwarten. Erst dann können die Konsequenzen für die hiesige Praxis gezogen werden.

9.2 BAG zum Auskunftsanspruch – Anspruch auf Datenkopie nach Art. 15 Abs. 3 DSGVO

↗ § 253 Abs. 2 ZPO, Art. 15 Abs. 3 DSGVO

In einem Urteil vom 27. April 2021 – 2 AZR 342/20 – entschied das Bundesarbeitsgericht (BAG) zum Auskunftsanspruch nach Art. 15 Datenschutz-Grundverordnung (DSGVO). Es ging dabei um den Anspruch auf Erteilung einer Datenkopie.
In dem zu entscheidenden Vorgang beanspruchte der Arbeitnehmer sämtliche geschäftliche E-Mails gegen seinen Arbeitgeber in Datenkopie zu erhalten, Art. 15 Abs. 3 DSGVO. In der Streitsache entschied das Gericht, dass der Anspruch nicht vollstreckbar sei, da nicht feststellbar sei, auf welche E-Mails sich das Herausgabeverlangen stütze. Eine inhaltliche datenschutzrechtliche Bewertung erfolgte damit nicht. Das Gericht bezog sich auf die zivilprozessuale Vorschrift

Was ist zu tun?
Bei der Geltendmachung von Auskunftsansprüchen ist Erwägungsgrund 63 der Datenschutz-Grundverordnung zu beachten, wonach die betroffene Person zu präzisieren hat, auf welche Informationen sie sich bezieht.

des § 253 Abs. 2 Zivilprozessordnung (ZPO) und eine Unmöglichkeit, im konkreten Fall im Vollstreckungsverfahren festzustellen, welche E-Mails als Kopien zu beauskunften sind. Die Beschränkung und Überlegung des Gerichts ist im Einklang mit Erwägungsgrund 63 Satz 7 der Datenschutz-Grundverordnung.

9.3 BGH: Inhalt und Umfang des Auskunftsanspruchs

↗ Art. 15 DSGVO

In einer Entscheidung vom 15. Juni 2021 – VI ZR 576/19 – entschied der Bundesgerichtshof (BGH) mit Urteil zum Inhalt und zum Umfang des Auskunftsanspruchs nach Art. 15 Datenschutz-Grundverordnung (DSGVO).

In dem zu entscheidenden Rechtsstreit ging es darum, dass der Inhaber einer Lebensversicherung von der Versicherung – dem Verantwortlichen – Auskünfte erhalten hatte, diese aber als für nicht vollständig erachtete. Die betroffene Person stellte sich auf den Standpunkt, dass sämtliche bei dem Unternehmen über ihn vorhandene Daten, einschließlich der Korrespondenz und interner Aufzeichnungen und Vermerke, zu beauskunften gewesen seien. Die landgerichtliche Vorinstanz hatte einen so weit gehenden Auskunftsanspruch bereits verneint.

Der Bundesgerichtshof beurteilte den Vorgang hingegen anders und betrachtete den Auskunftsanspruch nach Art. 15 Datenschutz-Grundverordnung als grundsätzlich umfassend. Damit wären auch grundsätzlich alle gespeicherten bzw. verarbeiteten auf die betroffene Person beziehbaren Daten auskunftspflichtig. Somit gehören auch interne Unterlagen und Korrespondenz, an denen die betroffene Person nicht beteiligt gewesen war, zu den beauskunftenden Informationen. Allerdings schränkte das Gericht ein, dass zu den nicht zu beauskunftenden Informationen Daten zu internen Bewertungen der Versicherung zu gemachten streitigen Ansprüchen und rechtliche Einschätzungen zählten, da diese keine Informationen über den Betroffenen und damit keine perso-

nenbezogenen Daten darstellten. Entsprechendes gelte für Provisionszahlungen an Dritte. Entsprechende Unterlagen dürften insoweit auch geschwärzt werden.

Ein zentraler Punkt der Entscheidung war zudem, dass der Auskunftsanspruch nach dem Bundesgerichtshof dann erfüllt sei, wenn der Auskunftsschuldner bei der Erteilung einer Auskunft erkläre, dass die Auskunft vollständig sei, oder wenn sich dies aus seiner Auskunft ergebe. Insoweit eröffne ein bloßer Verdacht, dass die erteilte Auskunft nicht zutreffend oder nicht vollständig sei, keinen Anspruch auf Auskunft in einem weitergehenden Umfang.

Was ist zu tun?

Der Auskunftsanspruch nach Art. 15 DSGVO ist grundsätzlich umfassend. Ist eine Auskunft seitens des Verantwortlichen erteilt worden, ist – jedenfalls bei Fehlen weiterer Anhaltspunkte – davon auszugehen, dass die Pflicht nach Art. 15 DSGVO auch erfüllt worden ist.

9.4 Gesetzliche Aufbewahrungspflichten und das Recht auf Löschung

↗ § 147 AO, Art. 17 DSGVO

Das Oberlandesgericht Dresden entschied am 14. Dezember 2021 – 4 U 1278/21 – über die Frage, ob unberechtigt gespeicherte Daten zu löschen sind, wenn die entsprechenden Dokumente gesetzlichen Aufbewahrungspflichten unterliegen.

Im Ausgangsfall hatte ein Unternehmen einen vermeintlichen Schuldner aufgefordert, eine offene Forderung zu begleichen. Aufgrund einer Namensgleichheit handelte es sich allerdings bei der so angesprochenen betroffenen Person nicht um den tatsächlichen Schuldner. Die betroffene Person forderte dann von dem Verantwortlichen die Löschung. Der Verantwortliche – das Unternehmen – führte hiergegen an, dass nach der Abgabenordnung Aufbewahrungspflichten bestünden, § 147 Abgabenordnung (AO).

Das Gericht erkannte hingegen bei gleichzeitiger Beachtung des Erhalts der aufzubewahrenden Geschäftskorrespondenz eine Löschungsverpflichtung in Bezug auf den Namen, die Anschrift und das Geburtsdatum der betroffenen Person, mithin der Informationen, die eine Identifizierung des Betroffenen in den Unterlagen zuließen. Insoweit wäre seitens des Verantwortlichen eine Prüfung der Rechtsgrundlage der Speicherung einzelner in Dokumenten enthaltener Daten

Was ist zu tun?

Selbst bei gesetzlicher Aufbewahrungspflicht sind in Bezug auf (mögliche) unrechtmäßige Datenerhebungen die Betroffenenrechte bestmöglich zu berücksichtigen.

vorzunehmen und zur Aufbewahrung der Daten verpflichtete Stellen seien pflichtig, ihren Datenbestand so zu organisieren, dass ein Zugriff auf unrechtmäßig erhobene Daten betroffener Personen nicht möglich sei, etwa durch entsprechende Schwärzungen.

Herausgeber
Sächsische Datenschutzbeauftragte
Dr. Juliane Hundert
Devrientstraße 5
01067 Dresden

Kontakt
Postfach 11 01 32, 01330 Dresden
Telefon 0351/85471-100
Telefax 0351/85471-109
saechsdsb@slt.sachsen.de
www.datenschutz.sachsen.de

Titelbild
© Tomasz Zajda/stock.adobe.com

Druck
Neue Süddeutsche Verlagsdruckerei GmbH

Auflage
1.500 Exemplare

Veröffentlichung
Mai 2022

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

Verteilerhinweis
Dieser Tätigkeitsbericht wird aufgrund der Verpflichtung nach Artikel 59 Datenschutz-Grundverordnung herausgegeben. Er darf weder von politischen Parteien noch von deren 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.