Freistaat
SACHSEN

Tätigkeitsbericht des Sächsischen Datenschutzbeauftragten

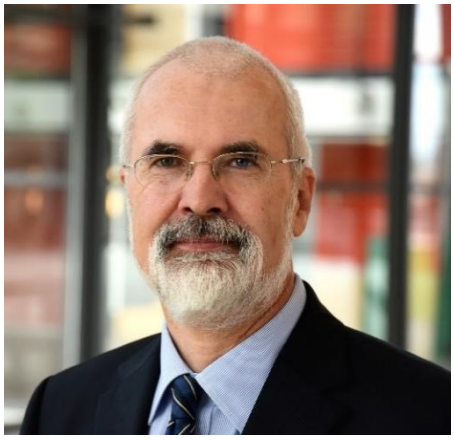
Berichtszeitraum: 1. Januar bis 31. Dezember 2020

Tätigkeitsbericht
des
Sächsischen Datenschutzbeauftragten
2020

Berichtszeitraum: 1. Januar bis 31. Dezember 2020

Rechtsstand: 31. Dezember 2020

Liebe Leserinnen und Leser,



vielleicht geht es Ihnen auch so: Es gibt Jahre, die geraten schnell in Vergessenheit. Andere brennen sich buchstäblich ins Gedächtnis ein. Das Jahr 2020 ordnen wohl die meisten von uns der Kategorie „unvergesslich“ zu. Dem schließe ich mich insbesondere mit Blick auf den Datenschutz an.

2020 – das war das Jahr in dem das analoge Leben ausgebremst wurde und das digitale rasant an Fahrt aufnahm. Passend dazu schlug eine Vielzahl von Fragen zum Datenschutz bei mir auf. Plötzlich boomten Videokonferenzen, Streaming-Plattformen und Onlineshopping. Homeoffice und Homeschooling hielten Einzug in den Alltag; Corona-Warn-Apps sollten die Pandemie stoppen.

Zur Jahresmitte sorgte eine Gerichtsentscheidung bei Verantwortlichen für Verunsicherung. Denn am 16. Juli 2020 hatte der Europäische Gerichtshof das Privacy-Shield-Abkommen zwischen der EU und den USA für unwirksam erklärt („Schrems II“). Folglich ist es US-Unternehmen nicht mehr möglich, auf der bisherigen Basis personenbezogene Daten von EU-Bürgern zu verarbeiten. Diese Entscheidung zwingt eine Vielzahl wirtschaftlicher, politischer und gesellschaftlicher Akteure zum Handeln. Vor allem Unternehmen dürften das drohende Bußgeld im Hinterkopf haben, wenn sie ihre Prozesse bei der Verarbeitung personenbezogener Daten nicht der Rechtsprechung anpassen. Auch in dieser Hinsicht entfaltet die Europäische Datenschutzgrundverordnung (DSGVO) ihre Wirkung.

Mit dem Urteil musste sich ebenso zeitnah die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder auseinandersetzen. Die Datenschutzkonferenz (DSK), deren Vorsitz ich 2020 innehatte, befasste sich intensiv mit den Folgen von „Schrems II“, beispielsweise mit der Übermittlung von Windows-10-Telemetriedaten an Microsoft oder der rechtskonformen Nutzung von Office 365. Des Weiteren wurde die Task Force „Schrems II“ eingerichtet. Sie befasst sich mit den Folgen des Urteils und dient den Aufsichtsbehörden zur Abstimmung über das weitere Vorgehen.

Neben Fragen zur datenschutzkonformen Digitalisierung und Pandemiebekämpfung erreichten mich 2020 wieder viele weitere Anliegen. Der Beratungsbedarf in Sachsen war weiterhin hoch. Datenschutz betrifft eben mehr oder weniger nahezu alle Lebensbereiche. Und so unterschiedlich die einzelnen Praxisfälle auch sein mögen, so zieht sich doch ein Aspekt wie der berühmte rote Faden hindurch: das informationelle Selbstbestimmungsrecht. Es ist ein elementares Wesensmerkmal unserer freiheitlichen demokratischen Grundordnung und daher unveräußerlich. Diesem Leitgedanke folgt auch die DSGVO, an deren Struktur sich der gemäß Artikel 59 jährlich anzufertigende Tätigkeitsbericht orientiert.

Abschließend möchte ich mich bei den Abgeordneten des Sächsischen Landtages sowie bei allen Partnern bedanken, die sich nicht nur im Berichtszeitraum für den Datenschutz und die Ausstattung meiner Behörde stark gemacht haben. Besonders danke ich meinen Mitarbeiterinnen und Mitarbeitern. Sie haben im zurückliegenden Jahr Großes geleistet. Ich denke dabei nicht nur an die Corona-bedingten Herausforderungen, sondern auch an die Bewältigung der vielen Beratungsanfragen, den DSK-Vorsitz, die Vorbereitung zum Europäischen Datenschutztag und vieles mehr.

Einzelheiten zu all diesen Ereignissen erfahren Sie, liebe Leserinnen und Leser, auf den folgenden Seiten. In diesem Sinne wünsche ich Ihnen viele neue Erkenntnisse!

Ihr

Andreas Schurig
Sächsischer Datenschutzbeauftragter

Inhaltsverzeichnis

Abbildungsverzeichnis		16
Abkürzungsverzeichnis		17
Sachgebietsregister		20
Vorbemerkung zum Sprachgebrauch		23
1	**Datenschutz im Freistaat Sachsen**	**24**
1.1	Datenschutz in Zeiten der Coronavirus-Pandemie	24
1.2	Befragung zum Datenschutz bei Kommunen	25
1.3	Vorsitz der Datenschutzkonferenz	29
1.4	Aufsichtsschwerpunkt Videoüberwachung	30
1.5	Anwendung der Datenschutz-Grundverordnung auf die parlamentarische Tätigkeit	33
1.6	Das Sächsische Datenschutzdurchführungsgesetz im Verhältnis zur Datenschutz-Grundverordnung und zum Bundesdatenschutzgesetz – Einwilligung im Beschäftigungsverhältnis	35
1.7	Konsultation bei staatlichen Rechtsetzungsvorhaben	36
1.8	Gesetz zum 23. Rundfunkänderungsstaatsvertrag	38
1.9	„Eigeninitiierte“ Öffentlichkeitsarbeit von Behörden	40
2	**Grundsätze der Datenverarbeitung**	**43**
2.1	Datenverarbeitungsgrundsätze, Begriffsbestimmungen	43
2.1.1	Betriebsarzt als eigener Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO	43
2.1.2	Datenschutzbeauftragter als eigener Verantwortlicher	43
2.1.3	MDK-Reformgesetz – Medizinischer Dienst als eigener Verantwortlicher	44
2.1.4	Verdeckte Erhebung von Fahrzeugkennzeichen – Transparenz	44

2.1.5	Geschwärzte Ausweiskopien nach Geldwäschegesetz – Datenminimierung	45
2.1.6	Datenminimierung im Sozialbereich: Umfang der bei der Verwendungsnachweisprüfung der Eingliederungshilfe zu prüfenden Unterlagen	48
2.2	Rechtmäßigkeitsvoraussetzungen der Datenverarbeitung	49
2.2.1	Was geschieht mit meinen personenbezogenen Daten bei einem Coronatest?	49
2.2.2	Führung von Besucherlisten an sächsischen Gerichten	51
2.2.3	Corona-Erfassungsbogen im Rathaus	52
2.2.4	Kontaktdatenerhebung bei Friseurbesuchen in der Coronavirus-Pandemie	52
2.2.5	Weitergabe von personenbezogenen Daten beziehungsweise Gesundheitsdaten durch die Gesundheitsämter an die Polizei	54
2.2.6	Atteste zur Befreiung von der Pflicht zum Tragen einer Mund-Nasenbedeckung in Schulen	55
2.2.7	Gesundheitsbestätigungen für Schulbesuch	57
2.2.8	Überprüfung eines bevollmächtigten Bezirksschornsteinfegers	57
2.2.9	Nachweis ausreichender Impfschutz gegen Masern	58
2.2.10	Einsatz elektronischer Wasserzähler	59
2.2.11	Luftaufnahmen von Grundstücken durch die öffentliche Hand beziehungsweise deren Beauftragte	60
2.2.12	Nutzung von Melderegisterdaten durch Ortsvorsteher	61
2.2.13	Nachbarbeteiligung bei Bauvorhaben	62
2.2.14	Offenlegung von Pfändungs- und Einziehungsverfügungen gegenüber Dritten	62
2.2.15	Adressangabe des Lebensmittelherstellers	63
2.2.16	Weitergabe von Mieterkontaktdaten an Makler und Nachmieter	63

2.2.17	Zur Frage der Übertragung der Datenbereitstellung nach dem Zensusgesetz auf die Hausverwaltung	67
2.2.18	Die Nutzung von E-Mail- und Telefonkontaktdaten bei bestehender Geschäftsbeziehung	68
2.2.19	Zulässigkeit von Business-to-Business-Marketing	69
2.2.20	Abgrenzung nicht werblicher Kundeninformationen von Werbeansprachen und Erinnerungsmails – „Nudgemails“	69
2.2.21	Inanspruchnahme eines Minderjährigen durch einen Inkassodienstleister	70
2.2.22	Richtigstellung zu „Anforderungen an Webseiten öffentlicher Stellen“	71
2.2.23	Videoüberwachung sorgt für Nachbarschaftsstreitigkeiten	72
2.2.24	Videografie: Die wertvolle Skulptur im Vorgarten	74
2.2.25	Klingelkameras als digitale Türspione	76
2.2.26	Videoüberwachung des Eingangsbereiches eines Wohnblockes – Ausnahmen bestätigen die Regel	78
2.2.27	Videoüberwachung in einer Zahnarztpraxis	81
2.2.28	Videokamera im Thai-Massage-Studio	83
2.2.29	Videoüberwachung der Mitarbeiterbereiche bei einem Autohof	84
2.2.30	Dashcams und Helmkameras	86
2.3	Einwilligungsfragen	89
2.3.1	Widerruf von gegenüber Kommunen erteilten Einwilligungen	89
2.3.2	LernSax – die sächsische Schulcloud	90
2.3.3	Erhebung von Gesundheitsdaten von Beschäftigten in der Coronavirus-Pandemie	91
2.3.4	Die obligatorische Einwilligung zur Werbung auf einem Einkaufsportal	94
2.3.5	Vorteile gegen Daten – Werbeansprache oder sonstige Datennutzung als Vertragsgegenstand	94

2.3.6	Einwilligungsformulare von Versicherungsmaklern	95
2.4	Sensible Daten, besondere Kategorien personenbezogener Daten	96
2.4.1	Datenschutzfreundliche Erhebung von Gesundheitsdaten bei Beschäftigten	96
2.4.2	Erstattung von Gewerkschaftsbeiträgen durch den Arbeitgeber	98
3	**Betroffenenrechte**	**99**
3.1	Spezifische Pflichten des Verantwortlichen	99
3.1.1	Datenschutzinformation nach Art. 13 DSGVO – One-fits-all-Lösung zulässig?	99
3.1.2	Informationspflichten von Rechtsanwälten als Berufsgeheimnisträger	100
3.2	Auskunftsrecht	101
3.2.1	Auskunftsersuchen an die Schule in einer dienstrechtlichen Angelegenheit	101
3.2.2	Verweigerte Auskunft zum Adressbezug beim Lettershop-Modell	103
3.2.3	Recht auf kostenlose Datenkopie für Kontoauszugsdaten	103
3.3	Recht auf Löschung	106
3.3.1	Verpflichtung zur Löschung von Kontoauszügen durch das Jobcenter?	106
3.3.2	Die Löschung von Kundenprofilen und -konten	107
3.3.3	Häufige Beschwerden zu unerwünschter Werbung per E-Mail	108
3.3.4	Fortwährende Verarbeitung personenbezogener Daten potenzieller Erben durch einen Verantwortlichen	110
3.3.5	Viel Lärm um nichts: Grundloser Ärger wegen alter Videokameras	111
3.4	Recht auf Datenübertragbarkeit, Sonstiges	114
3.4.1	Übermittlung der Gehaltsabrechnung	114

4	**Pflichten Verantwortlicher und Auftragsverarbeiter**	**115**
4.1	Verantwortung für die Verarbeitung, Technikgestaltung	115
4.1.1	Prüfwerkzeuge für Websites und Anforderungen an Betreiber von Websites	115
4.1.2	Standard-Datenschutzmodell (SDM)	116
4.1.3	„Autofill“-Funktion – Voreinstellung bei E-Commerce-Auftritt	117
4.1.4	Authentifizierung per IBAN bei telefonischer Zählerstandsmeldung	118
4.1.5	WhatsApp-Gruppe in Vertriebsstrukturen unter Einbindung Selbständiger	119
4.1.6	Fahrtkostenerstattung: Umgang mit Versichertendaten durch Krankenkasse	120
4.2	Gemeinsam Verantwortliche	121
4.2.1	Gemeinsam Verantwortliche bei der Videoüberwachung in Fußballstadien	121
4.2.2	Gemeinsam Verantwortliche: Eigentümer und Hausverwaltung	123
4.2.3	Lettershop-Verfahren – keine Gemeinsam Verantwortlichen	124
4.3	Auftragsverarbeitung	125
4.3.1	Beauftragung eines IT-Dienstleisters durch Kommune	125
4.4	Verzeichnis der Verarbeitungstätigkeiten, Kooperationspflicht mit der Aufsichtsbehörde	125
4.5	Sicherheit der Verarbeitung	126
4.5.1	Datenschutzgerechte Entsorgung von Geräten im medizinischen Bereich	126
4.5.2	Einsatz von privaten Messenger-Accounts und privaten Endgeräten zu beruflichen Zwecken im Beschäftigungsverhältnis	127
4.6	Meldung von Datenschutzverletzungen	128
4.6.1	Zuwachs bei gemeldeten Datenpannen	128
4.6.2	Cyberangriff auf Hochleistungsrechenzentrum	130

4.6.3	Schwachstelle in Hochschulinformationssystem	131
4.6.4	Offener Webserver	132
4.7	Datenschutzbeauftragter	132
4.8	Verhaltensregeln und Zertifizierung	132
4.8.1	Zum Stand von Akkreditierungen und Zertifizierungen	132
5	**Internationaler Datenverkehr**	**134**
5.1	Konsequenzen aus der Entscheidung des Europäischen Gerichtshofs zum internationalen Datentransfer	134
6	**Sächsischer Datenschutzbeauftragter**	**136**
6.1	Zuständigkeit und Anforderungen an Beschwerden	136
6.1.1	Zuständigkeit des Sächsischen Datenschutzbeauftragten nach der DSGVO	136
6.1.2	Sachliche Unzuständigkeit bei einem Online-Lexikon	138
6.1.3	Änderung der aufsichtsbehördlichen Zuständigkeit für Bundesautobahnen und Bundesstraßen	140
6.1.4	Inkassobereich: Mindestanforderungen an Beschwerden	141
6.2	Zahlen und Daten zu den Tätigkeiten 2020	141
6.2.1	Überblick zu den Arbeitsschwerpunkten	141
6.2.2	Beschwerden und Hinweise	142
6.2.3	Beratungen	144
6.2.4	Datenschutzverletzungen	144
6.2.5	Europäische Verfahren	144
6.2.6	Register der benannten Datenschutzbeauftragten	144
6.3	Ressourcen	145
6.4	Geldbußen und Sanktionen, Strafanträge	149

6.4.1	Ordnungswidrigkeitenverfahren im öffentlichen Bereich	149
6.4.2	Ordnungswidrigkeitenverfahren im nicht-öffentlichen Bereich	154
6.4.3	Wem gehören die Verfahrensakten in Bußgeldverfahren?	156
6.5	Öffentlichkeitsarbeit	157
6.5.1	Schulungen und Vorträge	158
7	**Zusammenarbeit der Datenschutzaufsichtsbehörden, Datenschutzkonferenz**	**159**
7.1	Konferenztätigkeit	159
7.2	Materialien der Datenschutzkonferenz – Entschließungen	159
7.3	Materialien der Datenschutzkonferenz – Beschlüsse	160
7.4	Materialien der Datenschutzkonferenz – Orientierungshilfen	160
7.5	Materialien der Datenschutzkonferenz – Anwendungshinweise	160
7.6	Dokumente des Europäischen Datenschutzausschusses: Leitlinien, Empfehlungen, bewährte Verfahren	161
7.7	Europäischer Datenschutztag zum Thema „Cross-Border Data Transfers“	162
7.8	Gemeinsame Überprüfung von Medienunternehmen durch Datenschutzaufsichtsbehörden	164
8	**Richtlinienbereich – Richtlinie (EU) 2016/680 – und sonstige Bereiche**	**165**
8.1	Nutzung von „Corona-Besucherlisten“ für Strafverfolgungszwecke	165
8.2	Einsatz von Bodycams bei der sächsischen Polizei	166
8.3	Auskunftsanspruch des Betroffenen des Bußgeldverfahrens zur Person des Anzeigeerstatters	167
9	**Rechtsprechung zum Datenschutz**	**170**
9.1	Anfechtungsklage wegen eines Kostenbescheids des Sächsischen Datenschutzbeauftragten und Antrag auf Wiedereinsetzung in den vorherigen Stand	170

9.2 Bestandsdatenauskunft: Gesetzesänderungen notwendig 171

9.3 Rechtsprechung des Europäischen Gerichtshofs zum internationalen Datentransfer, C-311/18 – „Schrems II“ 172

9.4 Entscheidung des Bundesgerichtshofs zur Einwilligung in telefonische Werbung und in Cookies zur Erstellung von Nutzungsprofilen für Zwecke der Werbung oder Marktforschung 173

9.5 Verstoß gegen Art. 32 DSGVO – Entscheidung des Landgerichts Bonn, Urteil vom 11. November 2020 – 29 OWi 1/20 174

9.6 Auskunft nach Art. 15 DSGVO durch kostenfreie (elektronische) Übermittlung der Behandlungsakte 175

9.7 Zur Speicherdauer von Kontoauszügen in Sozialleistungsakten 177

Abbildungsverzeichnis

Abbildung 1: Beginn der Umsetzung der DSGVO in sächsischen Kommunen 26

Abbildung 2: DSB-Bestellung in Kommunen 27

Abbildung 3: Schwierigkeiten im Umgang mit Einwilligungserklärungen 27

Abbildung 4: Vorkehrungen für Erteilung elektronischer Auskunftsersuche 28

Abbildung 5: Anpassung der Datenschutzerklärung auf der Website 28

Abbildung 6: Meldungen von Datenschutzverletzungen 128

Abbildung 7: Arbeitsschwerpunkte nach Anzahl der Vorgänge 142

Abbildung 8: Beschwerden und Hinweise 143

Abbildung 9: Beratungen 143

Abbildung 10: Meldungen benannter Datenschutzbeauftragter 145

Abbildung 11: Schriftgutaufkommen 146

Abbildung 12: Zuwächse in wichtigen Tätigkeitsbereichen 147

Abbildung 13: Vereinfachtes Organigramm der Behörde 148

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
BDSG	Bundesdatenschutzgesetz
BGB	Bürgerliches Gesetzbuch
BMG	Bundesmeldegesetz
BZRG	Bundeszentralregistergesetz
DSGVO	Datenschutz-Grundverordnung
HGB	Handelsgesetzbuch
JI-RL	Richtlinie (EU) 2016/680 (Justiz und Inneres)
OWiG	Gesetz über Ordnungswidrigkeiten
SächsDSG	Sächsisches Datenschutzgesetz
SächsPolG	Polizeigesetz des Freistaates Sachsen
SächsPresseG	Sächsisches Gesetz über die Presse
SächsSchulG	Sächsisches Schulgesetz
SächsVerf	Verfassung des Freistaates Sachsen
SächsVwVfZG	Gesetz zur Regelung des Verwaltungsverfahrens- und des Verwaltungszustellungsrechts für den Freistaat Sachsen und zur Änderung anderer Gesetze
SchfHwG	Schornsteinfeger-Handwerksgesetz
SGB	Sozialgesetzbuch
StPO	Strafprozessordnung
TMG	Telemediengesetz
UWG	Gesetz gegen den unlauteren Wettbewerb
VwVfG	Verwaltungsverfahrensgesetz
ZPO	Zivilprozessordnung

Sonstiges

Abs.	Absatz
Art.	Artikel
AG	Arbeitsgruppe
ASD	Allgemeiner Sozialer Dienst
Az.	Aktenzeichen
BfDI	Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BKA	Bundeskriminalamt
BMI	Bundesministerium des Innern, für Bau und Heimat
BR-Drs.	Bundesrats-Drucksache
BSG	Bundessozialgericht
BSGE	Bundessozialgerichtsentscheidung
BSI	Bundesamt für Sicherheit in der Informationstechnik
BT-Drs.	Bundestags-Drucksache
Buchst.	Buchstabe
BVerfG	Bundesverfassungsgericht
BVerfGE	Bundesverfassungsgerichtsentscheidung
BVerwG	Bundesverwaltungsgericht
BVerwGE	Bundesverwaltungsgerichtsentscheidung
DSK	Konferenz der unabhängigen Datenschutzbeauftragten des Bundes und der Länder – Datenschutzkonferenz
EGMR	Europäischer Gerichtshof für Menschenrechte
EU	Europäische Union
IVO	Integriertes Vorgangsbearbeitungssystem für die Landespolizei
JVA	Justizvollzugsanstalt
KSV	Kommunaler Sozialverband Sachsen
LaSuB	Landesamt für Schule und Bildung
LfV	Landesamt für Verfassungsschutz des Freistaates Sachsen
LG	Landgericht

LKA	Landeskriminalamt Sachsen
LT-Drs.	Landtags-Drucksache
OLG	Oberlandesgericht
OVG	Oberverwaltungsgericht
Rdnr.	Randnummer
SächsABl.	Sächsisches Amtsblatt
SächsGVBl.	Sächsisches Gesetz- und Verordnungsblatt
SächsVerfGH	Sächsischer Verfassungsgerichtshof
SID	Staatsbetrieb Sächsische Informatik Dienste
SMF	Sächsisches Staatsministerium der Finanzen
SMI	Sächsisches Staatsministerium des Innern
SMJusDEG	Staatsministerium der Justiz und für Demokratie, Europa und Gleichstellung
SMK	Sächsisches Staatsministerium für Kultus
SMS	Sächsisches Staatsministerium für Soziales und Gesellschaftlichen Zusammenhalt
SMUL	Sächsisches Staatsministerium für Energie, Klimaschutz, Umwelt und Landwirtschaft
SMWA	Sächsisches Staatsministerium für Wirtschaft, Arbeit und Verkehr
SMWK	Sächsisches Staatsministerium für Wissenschaft, Kultur und Tourismus
StA	Staatsanwaltschaft
SVN	Sächsisches Verwaltungsnetz
VVT	Verzeichnis von Verarbeitungstätigkeiten
VwV	Verwaltungsvorschrift
WEG	Wohnungseigentümergemeinschaft

Sachgebietsregister

*mit * | ausschließlich öffentlicher Bereich*
*ohne * | nicht-öffentlicher Bereich bzw. öffentlicher und nicht-öffentlicher Bereich*

Datenschutz-Grundverordnung (EU) 2016/679	**Fundstelle**
Archivwesen*	
Auftragsverarbeitung	4.3
Beliehene*	2.2.8
Beschäftigtendatenschutz (inkl. Dienstrecht*, Personalvertretungen*, Betriebsräte, sonstige Vertretungen und Beauftragte); *vgl. auch Videografie, Beschäftigte*	1.6, 2.1.1, 2.3.3, 2.4.1, 2.4.2 3.2.1, 3.4, 4.5.2
Betrieblicher Datenschutzbeauftragter, siehe *Datenschutzbeauftragter*	
Betroffenenrechte (Information, Auskunft, Löschung et cetera)	3**;** 2.1.2, vgl. 2.2.10, vgl. auch 8.3, 9.6, 9.7
Bildung und Wissenschaft	
• Hochschulen, Forschungseinrichtungen	4.6.3
• Schulen, Schulbehörden*, Bildungseinrichtungen	2.2.6, 2.2.7, 2.3.2, 2.4.1, 3.2.1
• Sonstiges, Allgemeines	
Corona, SARS-CoV-2, Pandemiemaßnahmen und damit einhergehende Datenverarbeitung	1.1, 2.2.1 bis 2.2.7, 2.3.2, 2.3.3; vgl. auch 8.1
Datenschutzbeauftragter	vgl. 1.2, 2.1.2, 6.2.6
Datenschutz-Folgenabschätzung	
Dashcam, Drohnen, siehe *Videografie*	
E-Government*	
Einwilligung	2.3**;** 1.6, 2.2.3, 2.2.16, 2.2.18, 3.3.4, 9.4
Fachverwaltung* (z. B. Bauverwaltung, Ausländerbehörden), siehe ggfs. *Registerbehörden**	2.2.8, 2.2.13, 6.1.3
Finanz-, Steuer- und Fördermittelverwaltung* (incl. kommunale Stellen)	2.4.1
Freie Berufe, siehe ggfs. auch *Gesundheitswesen*	
• Rechtsanwälte	3.1.2
• Notare	
• Steuerberater, Wirtschaftsprüfer	
• Architekten, Ingenieure	
• Sonstiges, Allgemeines	
Gemeinsam Verantwortliche	4.2
Gerichtsverwaltung*	2.2.2
Gerichtsvollzieher*	

Datenschutz-Grundverordnung (EU) 2016/679	**Fundstelle**
Gesundheitswesen	
• Behördliche Aufsicht und Überwachung*	2.2.1, 2.2.4, 2.2.5, 2.2.9, 2.2.15
• Krankenhäuser	9.6
• Pflegedienste	
• Apotheker	
• Ärzte	2.1.1, 2.2.1, 2.2.27, 2.2.9
• Heilberufe	4.5.1
• Sonstiges, Allgemeines	
Handel, Dienstleistungen, Gewerbe, Industrie	
• Auskunfteien, Inkassodienstleister, Detekteien	2.2.21, 6.1.4
• Banken, Finanzwirtschaft	2.1.5, 3.2.3, 3.3.4
• Handel, s. auch *Internet/E-Commerce*	4.1.5
• Handwerk, Gewerbe, Industrie	2.2.28, 2.2.4
• Hotel und Gastronomie, Freizeit, Tourismus, Sport	2.2.4; vgl. auch 8.1
• Versicherungen; siehe ggfs. *Sozialwesen, Leistungsträger*	2.3.6
• Werbung, Markt- und Meinungsforschung	2.2.18 bis 2.2.20, 2.3.4, 2.3.5, 3.2.2, 3.3.2, 3.3.3, 4.2.3, 9.4,
• Sonstiges, Allgemeines	2.1.4, 2.1.5, 2.2.4
Infrastruktureller Sektor	
• Energie-, Wasser- und Versorgungswirtschaft	2.2.10, 2.2.11, 4.1.4
• Verkehrs- und Beförderungswesen	6.1.3
• Wohnungswirtschaft, Immobilienverwaltung	2.2.14, 2.2.16, 2.2.17, 2.2.26, 3.1.1, 4.2.2
• Rechenzentren	vgl. 4.6
• Sonstiges, Allgemeines	
Internet, Medien, Kommunikation	
• E-Mail, Telekommunikationsvorgänge, Post	2.2.18 bis 2.2.20, 3.3.2, 3.3.3, 4.1.4, vgl. 4.6
• E-Commerce	2.2.20, 2.3.4, 3.3.3, 4.1.3
• Social Media, Telemedien	2.2.21, 3.3.2, 4.1.5, 4.5.2, 6.1.2
• Sonstiges, Allgemeines	1.8, vgl. auch 1.9, 2.2.22, 4.1.1, 4.6, 5, vgl. 6.1.1, 7.7, 9.2 bis 9.4
Kammern, berufsständische Körperschaften d. ö. R.*	vgl. auch 3.1.2

Datenschutz-Grundverordnung (EU) 2016/679	**Fundstelle**
Kommunale Selbstverwaltung*, siehe ggfs. *Fachverwaltung*, siehe ggfs. *Registerbehörden,* siehe ggfs. *Finanzverwaltung*	1.2, 2.2.3, 2.2.9, 2.2.10, 2.2.12, 2.2.14, 2.3.1, 4.3.1
Medien, siehe *Internet, Medien, Kommunikation*	
Meldung von Datenschutzverletzungen, Artikel 33	4.6**;** vgl. 1.2
Ordnungswidrigkeiten – Sächsischer Datenschutzbeauf.	6.4**;** vgl. 4.4
Registerbehörden* (unter anderem Melderecht, Personenstandswesen)	2.2.12
Religionsgemeinschaften	
Sächsischer Datenschutzbeauftragter	6**;** 1.3, 1.7, 4.4
Sächsischer Landtag als Verwaltung*	1.5
Sächsischer Rechnungshof*	
Schule, siehe *Bildung und Wissenschaft*	
Sensible Daten, Artikel 9	2.4**;** 2.2.1, 2.2.3, 2.2.5 bis 2.2.7, 2.2.9, 2.3.3, 4.5.1, 4.5.2, 9.7
Sicherheit der Verarbeitung, siehe ggfs. auch *Technische und organisatorische Maßnahmen*	4.5**;** 9.5
Sozialwesen	
• Sozialbehörden*	2.1.6, 3.3.1, 9.7
• Kindertagesstätten	2.2.9
• Leistungsträger	2.1.3, 4.1.6
• Sonstiges, Allgemeines	
Statistikwesen*	vgl. 2.2.17
Technische und organisatorische Maßnahmen, s. ggfs. *Sicherheit der Verarbeitung,* siehe. ggfs. *Verzeichnis von Verarbeitungstätigkeiten*	4**;** 9.5
Vereine (auch Parteien), Verbände, Stiftungen	vgl. auch 1.5, 4.2.1
Verkehrswesen	vgl. auch 4.7, 6.1.3
Verzeichnis von Verarbeitungstätigkeiten, Kooperationspflicht	4.4; vgl. 1.2
Videografie und Bildverarbeitung	
• Behördliche Überwachung/Verarbeitung*	vgl. 1.2, 2.2.11, 4.2.1
• Beschäftigte, vgl. ansonsten *Beschäftigtendatenverarbeitung*	2.2.27 bis 2.2.29
• Dashcam, Drohnen	2.2.30
• Handel, Gewerbe	2.2.28, 2.2.29, 3.3.5
• Wohnbereiche	2.2.11, 2.2.23 bis 2.2.26
• Sonstiges, Allgemeines	1.2, 1.4, 2.2.27, 2.3.1, 3.1.1, 4.2.1
Wahlrecht*	
Zertifizierung, Akkreditierungen, Prüfsiegel	4.8

Richtlinie (EU) 2016/680	**Fundstelle**
Polizei*	8.1, 8.2; vgl. auch 1.9, 2.2.5, 4.2.1, 6.4.1
Ordnungswidrigkeitenbehörden*	8.3; vgl. 6.4.3, 9.5
Strafverfolgung*	8.1; 1.9, 9.2
Strafvollzug*	
Sonstige Bereiche (außerhalb Verordnung 2016/679 und Richtlinie EU 2016/680)	
Sächsischer Landtag als Parlament	1.5, vgl. 1.7, 1.8
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 Partizip Präsens wird auf Ersatzformen wie Nutzende oder Anwendende verzichtet.

1 Datenschutz im Freistaat Sachsen

1.1 Datenschutz in Zeiten der Coronavirus-Pandemie

Im Berichtszeitraum hat die Corona-Pandemie ab März 2020 auch in Sachsen zu einer Vielzahl datenschutzrechtlicher Fragen geführt. Neben meinem sonstigen laufenden Geschäft war ich deshalb wie auch andere sächsische öffentliche Stellen zusätzlich mit wichtigen und häufig auch dringlichen Corona-bezogenen Vorgängen befasst.

Im Wesentlichen handelte es sich dabei um drei Bereiche: Zum einen wurde ich durch die Staatsregierung, insbesondere das Sächsische Staatsministerium für Soziales und Gesellschaftlichen Zusammenhalt, konsultiert. Hauptsächlich ging es dabei um die jeweiligen Sächsischen Corona-Schutzverordnungen. Gemäß Art. 36 Abs. 4 Datenschutz-Grundverordnung (DSGVO) bin ich bei der Ausarbeitung von Rechtsvorschriften zu konsultieren. Ich habe diese Einbindung genutzt, um Einfluss auf die konkreten Formulierungen der Rechtsvorschriften zu nehmen und sie möglichst datenschutzkonform gestalten zu lassen. Ich hoffe, dass ich auch zukünftig beteiligt werde, so wie es Art. 36 Abs. 4 DSGVO verlangt (vgl. auch 1.7). Zum anderen habe ich eine Vielzahl aktuell diskutierter Fragen aufgegriffen und mich gegenüber Beteiligten oder gar öffentlich dazu geäußert. Das betraf beispielsweise die Kontaktnachverfolgung durch Gesundheitsämter, die Datenverarbeitung im Zusammenhang mit der sächsischen Lernplattform LernSax, die Gesundheitsbestätigungen für den Schulbesuch, die Datenerhebung durch Erfassungsbögen beim Betreten von Gerichtsgebäuden oder Rathäusern, die Kontaktnachverfolgung mit Hilfe von beim Friseur hinterlegten Daten, die Rechtmäßigkeit des Verlangens einer Apotheke nach Ausweiskopien und gegebenenfalls noch weiterer Erklärungen für die Ausgabe von kostenlosen FFP2-Masken oder die Weitergabe von Listen mit positiv Getesteten und in Quarantäne befindlichen Personen an die Polizei. Schließlich gab es – schätzungsweise mehrere Hundert – einzelne Bürgeranfragen, Petitionen oder bloße Hinweise auf datenschutzrechtlich relevante Sachverhalte der Corona-Bekämpfung. Als Beispiel mögen die arbeitsrechtlichen Fragen nach den Befugnissen von Arbeitgebern und Dienstherrn bei der Erhebung von Daten über Corona-Testergebnisse dienen. All dies hat – wie erwähnt – zu einem erheblichen Arbeitsaufwand in meiner Behörde geführt, der mit den vorhandenen personellen Ressourcen nicht zu bewältigen war (vgl. 6.3).

Bei alledem habe ich stets darauf geachtet, dass wesentliche Aussagen unverzüglich auch auf meiner Webseite veröffentlicht wurden. So habe ich mich dort unter anderem zu den zulässigen Maßnahmen von Arbeitgebern beziehungsweise Dienstherren im Interesse des Infektionsschutzes, zum Datenschutz bei der (Tele-)Heimarbeit beziehungsweise im Homeoffice, zum Grundkonzept der Corona-Warn-App oder zu den erforderlichen Inhalten von Masken-Befreiungsattesten geäußert.

Einen wichtigen Aspekt meiner Tätigkeit habe ich auch darin gesehen, durch eine transparente datenschutzrechtliche Bewertung der Maßnahmen zur Bekämpfung der Corona-Pandemie Mythen und Verschwörungstheorien entgegenzuwirken.

In den Beiträgen 2.2.1 bis 2.2.7, 2.3.2, 2.3.3 und 8.1 stelle ich meine Tätigkeit und konkrete Problemlagen im Zusammenhang mit der Pandemie detailliert dar.

1.2 Befragung zum Datenschutz bei Kommunen

Die Datenschutz-Grundverordnung (DSGVO) gilt seit dem 25.05.2018 unmittelbar. Sie ist die Grundlage für ein einheitliches Datenschutzrecht in der Europäischen Union. Infolgedessen haben wir Anfang 2020 eine Umfrage zum Stand der Umsetzung der DSGVO bei ausgewählten Kommunen durchgeführt. Wir wollten Aufschluss darüber erhalten, inwieweit die Kommunen in Sachsen diese bereits umgesetzt und die jeweiligen Datenverarbeitungsprozesse an die Regelungen der DSGVO angepasst wurden. Eine ähnliche Umfrage erfolgte bereits in anderen Bundesländern. Somit konnten wir auf dem Fragebogen der Landesbeauftragten für den Datenschutz Niedersachsen für unsere Abfrage aufbauen.

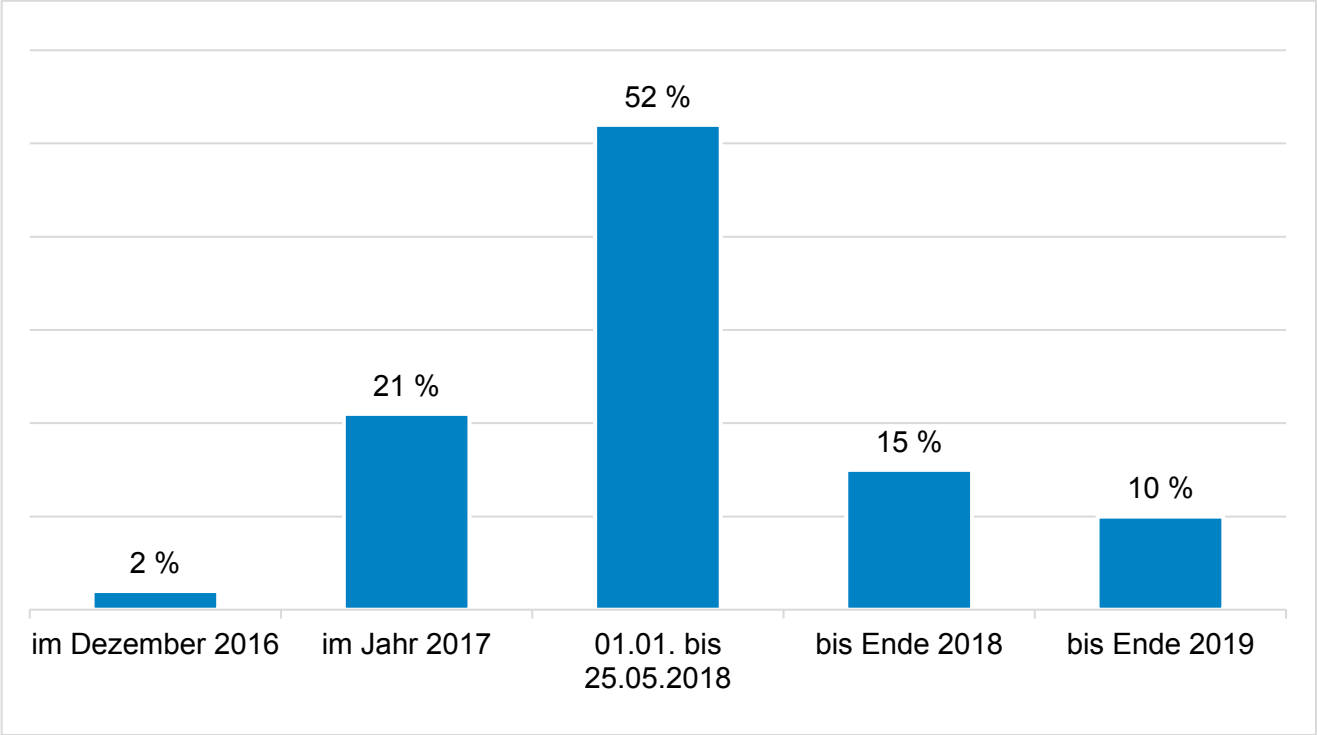
Um ein möglichst aussagekräftiges Umfrageergebnis zu erzielen, wurden neben allen kreisfreien Städten und Landkreisen verschiedene Kommunen unterschiedlicher Größe für die Abfrage von uns stichprobenartig ausgewählt. Der Fragebogen mit insgesamt vier Themenkomplexen wurde an 118 Stellen versendet. Davon gingen von 61 Stellen Rückmeldungen bei uns im Jahr 2020 ein. Nur wenige der Stellen antworteten innerhalb der gesetzten Frist von sechs Wochen. Mit Beginn der Corona Pandemie konnten wir jedoch keine weiteren Posteingänge verzeichnen. Erfreulicherweise haben wir zusätzlich 27 ausgefüllte Formulare von einzelnen Fachämtern von Behörden erhalten.

An der Umfrage nahmen letztendlich alle zehn Landkreise, die drei kreisfreien Städte (Dresden, Leipzig, Chemnitz) und weitere 48 Städte und Gemeinden teil. Herzlichen Dank an alle, die bei der Abfrage mitgemacht haben!

Die 39 Fragen beinhalteten Themen aus der DSGVO zur Datenschutzorganisation, wie die Bestellung eines behördlichen Datenschutzbeauftragten (Art. 37) und Fragen zum Verzeichnis der Verarbeitungstätigkeiten (Art. 30). Im Weiteren waren Fragen zur konkreten datenschutzkonformen Verarbeitung gestellt, beispielsweise zur Basis einer Einwilligung (Art. 7), zur Auftragsverarbeitung (Art. 28 und 29), zur Datenschutz-Folgenabschätzung (Art. 35 und 36) sowie zu den Informationspflichten (Art. 12, 13 und 14) und Auskunftsersuchen einer betroffenen Person (Art. 15). Abschließend wurde zum Thema der Meldung von Datenpannen (Art. 33) gefragt.

Zusammenfassung der wichtigsten Ergebnisse

Die DSGVO ist bereits im Jahr 2016 in Kraft getreten und gilt seit dem 25. Mai 2018 in allen Mitgliedstaaten der Europäischen Union unmittelbar. Die Auswertung hat ergeben, dass leider nur 23 Prozent der angeschriebenen Kommunen bis zum Ende des Jahres 2017 mit den Umsetzungsarbeiten begonnen hatten und demzufolge die zweijährige Übergangszeit bis zum Wirksamwerden der DSGVO genutzt haben. Der überwiegende Teil (77 Prozent) der angeschriebenen Kommunen hat mit der Umsetzung erst im Jahr 2018 oder – noch später – erst 2019 begonnen. Demzufolge plante die Hälfte der befragten Kommunen die durch die DSGVO notwendigen Anpassungen von Rechtsvorschriften, Formularen, Verträgen und so weiter erst bis zum Jahresende 2020 abzuschließen. Weitere zwölf Kommunen (circa 20 Prozent) werden erst im Laufe des Jahres 2021 oder noch später die Datenschutzbestimmungen europarechtskonform umgesetzt haben.



Positiv hervorzuheben ist, dass nahezu alle Kommunen als Verantwortliche einzelne Beschäftigte oder Projektteams für die strategischen und operativen Umsetzungsaufgaben für den Datenschutz in ihrem Hause benannt haben. In fast allen Kommunen (95 Prozent) wurden auch die an den Verarbeitungsvorgängen beteiligten Beschäftigten über das neue Datenschutzrecht informiert. 54 Kommunen (89 Prozent) gaben an, dass für die Beschäftigten zum Zeitpunkt der Abfrage bereits Schulungsmaßnahmen angeboten wurden.

Eine Behörde oder öffentliche Stelle hat gemäß Art. 37 Abs. 1 Buchst. a) DSGVO einen Datenschutzbeauftragten (DSB) zu benennen. Fast alle Kommunen in Sachsen erfüllen diese Anforderung. Jeweils 36 Kommunen (59 Prozent) haben einen eigenen Beschäftigten zum Datenschutzbeauftragten bestellt. 20 (33 Prozent) – meistens kleinere Kommunen – beauftragten einen externen Dienstleister mit dieser Aufgabe. Nach Art. 37 Abs. 3 kann für mehrere solcher Behörden oder Stellen unter Berücksichtigung ihrer Organisationsstruktur und ihrer Größe ein gemeinsamer Datenschutzbeauftragter benannt werden. Von dieser Möglichkeit machten vier kleinere Gemeinden (7 Prozent) Gebrauch. In den meisten Kommunen (89 Prozent) verfügt der DSB bereits über die erforderliche Fachkunde oder es sind bereits Fortbildungsmaßnahmen geplant.

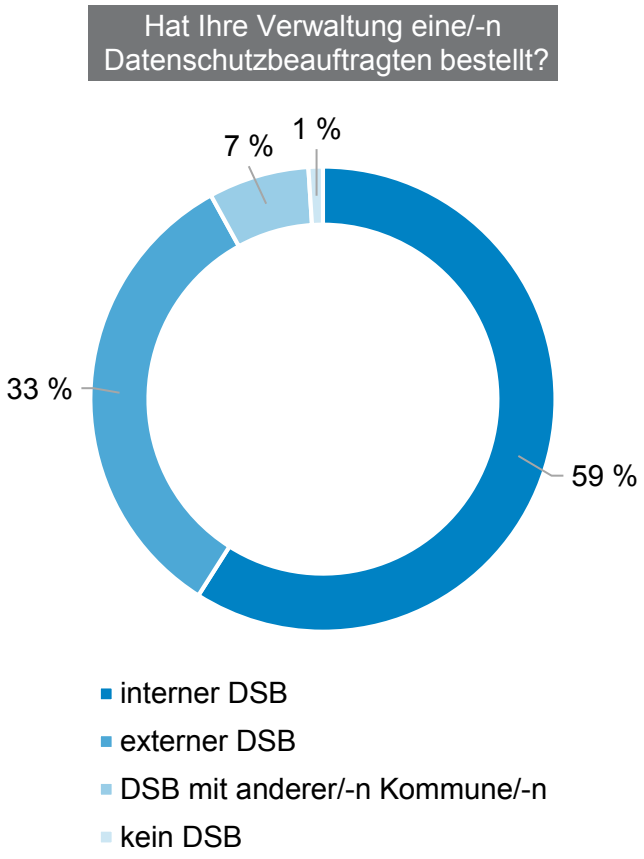


Abbildung 2: DSB-Bestellung in Kommunen

Nach Art. 30 DSGVO sind die Verantwortlichen verpflichtet, ein Verzeichnis aller Verarbeitungstätigkeiten (VVT) zu erstellen. 43 Kommunen (70 Prozent) gaben an, dass sie ein VVT erstellt haben. Ein vollständiges VVT wurde nur von zwei Kommunen (3 Prozent) erstellt und 16 Kommunen (26 Prozent) haben dies zumindest in einem Umfang von 75 bis 99 vom Hundert erstellt. Bedenklich ist, dass 21 befragte Kommunen (34 Prozent) zum Befragungszeitpunkt noch am Anfang der erforderlichen Arbeiten stehen standen. Entweder hatten sie mit der Erstellung des VVT noch nicht begonnen oder weniger als die Hälfte vom Hundert erledigt. Nur jeder zweite Verantwortliche nutzte elektronische Verfahren zur Bearbeitung

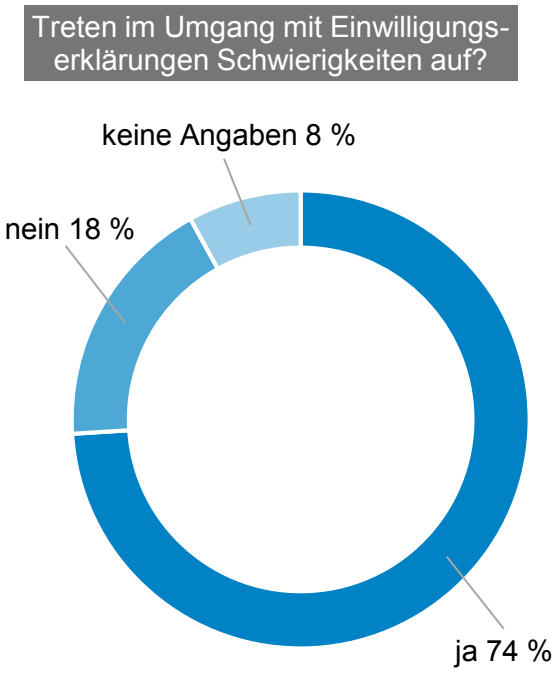


Abbildung 3: Schwierigkeiten im Umgang mit Einwilligungserklärungen

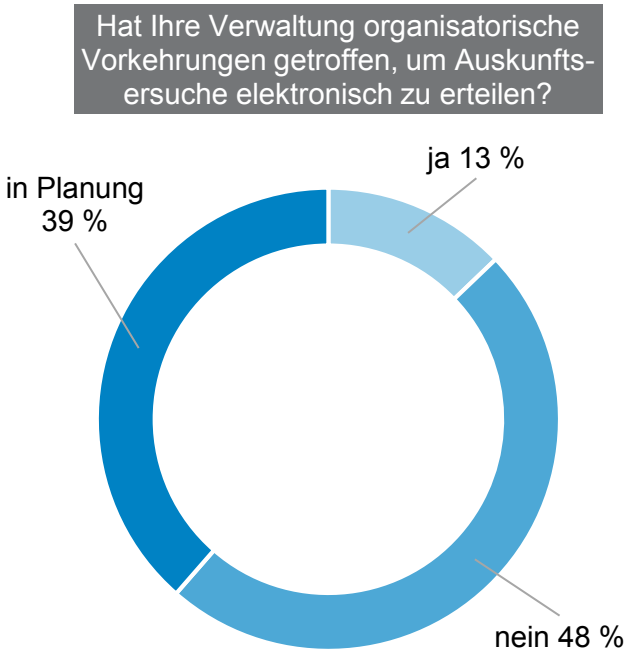


Abbildung 4: Vorkehrungen für Erteilung elektronischer Auskunftsersuche

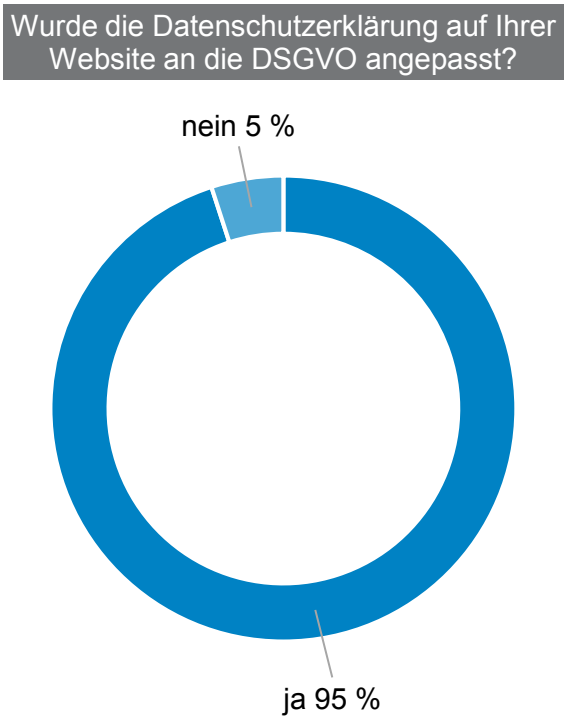


Abbildung 5: Anpassung der Datenschutzerklärung auf der Website

des VVT. 25 Kommunen (41 Prozent) gaben an, dass sie bei der Erstellung des VVT noch Schwierigkeiten haben und dass der mit der Umsetzung der DSGVO verbundene Aufwand in den Kommunen unterschätzt wurde. Neben Zeit- und Ressourcenproblemen wurden beispielsweise auch Schwierigkeiten bei der Zuordnung von Rechtsgrundlagen oder der Festlegung von angemessenen und dem Zweck entsprechenden Aufbewahrungs- und Löschungsfristen genannt. Einige Kommunen teilten in der Abfrage mit, dass Schwierigkeiten bei landes- oder bundesweiten Verfahren auftreten. Für die Erstellung der VVT und die datenschutzrechtliche Überprüfung dieser zentralen Verfahren, die in allen Verwaltungen zum Einsatz kommen, wäre die Erarbeitung von Vorgaben oder von Mustern empfehlenswert. Dies könnte zu einer Reduzierung des Aufwands in den Kommunen führen und die Umsetzung der DSGVO möglicherweise verbessern.

Fast alle der befragten Kommunen (89 Prozent) haben die an den Verarbeitungsvorgängen beteiligten Beschäftigten über die Meldepflicht von Datenpannen gemäß Art. 33 DSGVO informiert. Zum Zeitpunkt der Abfrage hatten erst ungefähr die Hälfte der befragten Verwaltungen organisatorische Vorkehrungen für die Information von Betroffenen nach Art. 34 DSGVO vorgesehen. Weitere 25 Kommunen (41 Prozent) haben dies zumindest bis Ende des Jahres 2020 terminiert.

23 Kommunen (38 Prozent) gaben an, in ihrer Verwaltung Videoüberwachung einzusetzen. Vier der 23 Kommunen, die Videoüberwachung nutzen, haben noch keine o-

der keine ausreichende Beschilderung aller Videokameras angebracht. Ferner fragten wir danach, ob die Informationen zur Videoüberwachung an die DSGVO angepasst wurden. Die Informationspflichten des Verantwortlichen bei der Videoüberwachung richten sich nach Art. 13 Abs. 1 DSGVO. Bei sechs verantwortlichen Stellen wurden diese Informationen des Verantwortlichen zur Videoüberwachung nach DSGVO noch nicht angepasst.

Insgesamt vermitteln die Umfrageergebnisse einen guten Eindruck, wie die Bestimmungen der DSGVO bis Anfang 2020 in den sächsischen Kommunen umgesetzt waren. Die Auswertung offenbarte aber nicht nur, welche Herausforderungen gemeistert wurden. Gleichsam traten die Defizite zu Tage, die eineinhalb Jahre nach Wirksamwerden der DSGVO noch bestanden. Diese Erkenntnisse sind bereits in meine Beratungsarbeit in 2020 eingeflossen, um das Datenschutzniveau in den Gemeinden weiter zu verbessern.

1.3 Vorsitz der Datenschutzkonferenz

Nach 2003 übernahm Sachsen 2020 zum zweiten Mal seit Bestehen der Behörde den Vorsitz der Datenschutzkonferenz (DSK). Das Gremium der 18 unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder hat die Aufgabe, die Datenschutzgrundrechte zu wahren und zu schützen, eine einheitliche Anwendung des europäischen und nationalen Datenschutzrechts zu erreichen und gemeinsam für seine Fortentwicklung einzutreten. Dies geschieht namentlich durch Entschließungen, Beschlüsse, Orientierungshilfen, Standardisierungen, Stellungnahmen, Pressemitteilungen und Festlegungen.

Die DSK tagt jährlich unter wechselndem Vorsitz im Turnus von jeweils zwei Haupt- und Vorkonferenzen sowie drei Zwischenkonferenzen. Hinzu kommt eine Sitzung mit den so-genannten spezifischen Aufsichtsbehörden, zu denen unter anderem die Kirchendaten-schutzbeauftragten oder die Rundfunkdatenschutzbeauftragten für den öffentlich-rechtlichen Rundfunk gehören.

Üblicherweise bringt der DSK-Vorsitz ein hohes Arbeitspensum mit sich. Zahlreiche Ab-stimmungen und Umlaufverfahren sind zu organisieren. Zudem vertritt der Vorsitzende das Gremium nach außen. Vor diesem Hintergrund stellte die Coronavirus-Pandemie eine zusätzliche Herausforderung mit neuen Gestaltungsmöglichkeiten dar. So fanden mit Ausnahme der ersten Zwischenkonferenz alle Zusammenkünfte erstmalig per Videokonferenz statt. In dieser Hinsicht war Sachsen also Vorreiter. Zugegeben: Zum Jubiläum der 100. Datenschutzkonferenz am 25. und 26. November hätten wir die Teilnehmer auch gern persönlich in Dresden begrüßt. Aber das Pandemiegeschehen ermöglichte nur eine Zusammenkunft per Videoschaltung. Die Ergebnisse konnten sich dennoch – auch im übertragenen Sinne – sehen lassen. Eine Übersicht über alle 2020 veröffentlichten Dokumente der DSK finden Sie in Kapitel 7.

Anfang 2021 wechselte planmäßig der DSK-Vorsitz zur Landesbeauftragten für Datenschutz und Informationsfreiheit des Saarlandes. Allerdings fiel die Planung und Durchführung des Europäischen Datenschutztages am 28. Januar 2021 noch in meine Zuständigkeit (vgl. 7.7).

1.4 Aufsichtsschwerpunkt Videoüberwachung

Fast täglich erreichen mich Eingaben und Hinweise zu vermeintlich unzulässigen Videokameras. Die Videografie stellt damit – insbesondere im nicht-öffentlichen Bereich – unverändert einen Arbeitsschwerpunkt meiner Behörde dar. Der enorme Preisverfall der Videoüberwachungstechnik sowie die breite Verfügbarkeit über zahlreiche Internetanbieter sowie vor Ort im Fachhandel, in Baumärkten und gar Discountern im Rahmen von Sonderaktionen führen zu einer stets steigenden Verbreitung der Technik und neuartigen Überwachungsgeschehen. Die Kameras verfügen oftmals über eine WLAN-Funktion und lassen sich damit auch für den technischen Laien unkompliziert ins heimische Netzwerk einbinden. Über entsprechende Anwendungssoftware lassen sich Live-Bilder ortsunabhängig über mobile Endgeräte wie zum Beispiel Smartphones und Tablets betrachten.

Im Regelfall ist der für Sicherheitszwecke erfolgende Einsatz von Videoüberwachungstechnik nicht nur mit einzelnen konkreten Geschäftsmodellen beziehungsweise -zwecken verbunden, sondern über alle Branchen verbreitet und somit sowohl für öffentliche als auch nicht-öffentliche Stellen in gleichem Maße und zunehmend auch für Privatpersonen interessant. In verstärktem Maße führen die Kamerabetreiber das subjektiv gestiegene Sicherheitsbedürfnis als Motivation für den Einsatz der Videoüberwachungstechnik an, was in meinen Augen eine wesentliche Ursache für die immer größere Durchdringung aller Bereiche des wirtschaftlichen und gesellschaftlichen Lebens mit Videoüberwachungstechnik ist.

Die in meinem Tätigkeitsbericht beispielhaft vorgestellten Sachverhalte stehen sinnbildlich für die vielfältigen Einsatzbereiche der Videoüberwachung (vgl. 2.2.3 bis 2.2.30, 3.1.1, 3.3.5, 4.2.1).

Häufig zeigt sich, dass Kamerabetreiber aus einer allgegenwärtig scheinenden Videoüberwachung für sich ebenso das Recht zum Betrieb einer Videoüberwachungsanlage ableiten. Sie übersehen dabei nur zu oft die (fehlende) Sinnhaftigkeit einer diesbezüglichen Investition. Wenn ich Kamerabetreiber dann mit alternativen, gleichfalls oder in ihrer Wirkung sogar effektiveren Maßnahmen konfrontiere, stelle ich regelmäßig fest, dass diese immer mehr in den Hintergrund rücken und Verantwortliche solche Maßnahmen zunehmend weniger in ihre Sicherheitsüberlegungen einbeziehen. Als Beispiele seien eine ausreichende Ausleuchtung gefährdeter Bereiche oder auch Alarmanlagen mit optischen oder akustischen Signalen, die im Bedarfsfall einen Alarm bei der Polizei auslösen, zu nennen.

An meinen Zulässigkeitsausführungen in früheren Tätigkeitsberichten hat sich auch unter der seit dem 25. Mai 2018 anwendbaren Datenschutz-Grundverordnung (DSGVO) im Wesentlichen nichts geändert. Die bei der Beobachtung öffentlich zugänglicher Räume anzuwendende Vorschrift des § 6b Bundesdatenschutzgesetz alter Fassung ist ersetzt worden. Die vom Bundesgesetzgeber mit § 4 Abs. 1 Bundesdatenschutzgesetz als Nachfolgeregelung erlassenen Vorgaben zur Videoüberwachung wurden vom Bundesverwaltungsgericht allerdings mit Urteil vom 27. März 2019 (6 C 2-18) als europarechtswidrig eingestuft (siehe Tätigkeitsbericht 2019, 9.1, Seite 161 ff.). Somit findet die eigentlich vorgesehene Vorschrift bei der Videoüberwachung im nicht-öffentlichen Bereich keine Anwendung. Bei privaten Stellen kommt einzig eine Beurteilung anhand der Maßstäbe des Art. 6 Abs. 1 Buchst. f DSGVO im Wege einer umfassenden Interessenabwägung in Betracht, soweit sich eine Videoüberwachung auf Bereiche jenseits der privaten Sphäre, das heißt der eigenen Wohnung beziehungsweise des eigenen Grundstücks erstreckt.

Eine Videoüberwachung, die sich auf den öffentlichen Raum erstreckt, kann nicht als eine ausschließlich persönliche oder familiäre Tätigkeit angesehen werden, auf die die datenschutzrechtlichen Vorschriften keine Anwendung fänden (vgl. Art. 2 Abs. 2 Buchst. c DSGVO). Die diesbezügliche Entscheidung des Europäischen Gerichtshofes vom 11. Dezember 2014 (Rechtssache C-212/13) besitzt nach wie vor Gültigkeit (vgl. dazu auch 7. Tätigkeitsbericht für den nicht-öffentlichen Bereich (04/2013 bis 03/2015), Seite 33 ff.

Die bereits erwähnte Vorschrift des Art. 6 Abs. 1 Buchst. f DSGVO schreibt ein berechtigtes Interesse auf Seiten des Kamerabetreibers beziehungsweise eines Dritten vor, das mit den entgegenstehenden schutzwürdigen Interessen betroffener Personen in Abwägung zu bringen ist. Eine Ausdehnung der Videoüberwachung auf öffentliche Verkehrsflächen (Geh- oder Radwege, Straßen, Plätze) wird im Allgemeinen nur dann überhaupt in Betracht kommen, wenn diese Verkehrsbereiche unmittelbar an das zu schützende Gebäude angrenzen. Es muss sich auch um einen absoluten Ausnahmefall handeln, das heißt schwerwiegenden Beeinträchtigungen der Rechte des Kamerabetreibers, etwa Angriffen auf seine Person und Familie oder seine unmittelbare Wohnsphäre lassen sich nicht in anderer Weise zumutbar begegnen. In jedem Fall bedarf es hierzu einer umfassenden Prüfung im Einzelfall.

Der Bundesgerichtshof hat bereits in seinem Urteil vom 25. April 1995 (VI ZR 272/94) klargestellt, dass Privatleute von notwehrähnlichen Situationen abgesehen, nicht das Recht haben, durch Videoaufzeichnungen Passanten auf öffentlichen Wegen zu erfassen. Privatpersonen rechnen nicht damit, von anderen Privatpersonen während ihres Verweilens im öffentlichen Raum gefilmt zu werden. Das vom Bundesverfassungsgericht anerkannte Recht auf informationelle Selbstbestimmung verbürgt das Recht des Einzelnen, sich insbesondere in der Öffentlichkeit frei und ungezwungen bewegen zu dürfen, ohne befürchten zu müssen, ungewollt zum Gegenstand einer Videoüberwachung gemacht zu werden. Die sich hieraus ergebenden schutzwürdigen Interessen der Betroffenen überwiegen regelmäßig das Betreiberinteresse an

einer präventiven Überwachung des Eigentums sowie der Beweissicherung bei strafrechtlich relevanten Vorfällen Diebstahl, Einbruch oder Sachbeschädigung.

Kein datenschutzrechtlich relevanter Fall liegt vor, wenn mit der Videoüberwachung überhaupt keine Verarbeitung personenbezogener Daten verbunden ist, vgl. Art. 2 Abs. 1 DSGVO. So fallen oft zu findende Kameraattrappen oder auch als solche nur dienende, aber eigentlich funktionstüchtige Kameras nicht unter das Datenschutzrecht. In diesen Fällen kann ich betroffene Personen nur auf das allgemeine Zivilrecht verweisen. Durch Attrappen werden überhaupt keine Daten erhoben, ja es werden noch nicht einmal Signale zu Beobachtungszwecken weitergeleitet. Fehlt es insoweit mangels Anwendbarkeit der datenschutzrechtlichen Vorschriften an der Kontrollzuständigkeit meiner Behörde, kann lediglich darauf hingewiesen werden, dass Kameraattrappen von der Rechtsprechung bei der Anwendung allgemeinen Zivilrechtes regelmäßig wie funktionstüchtige Kameras bewertet werden und daher zumindest eine analoge Anwendung der DSGVO in Erwägung gezogen sollte. Denn für die Betroffenen, die einen „scheinbar“ überwachten Bereich passieren, stellt sich das äußere Bild beim bloßen Vorhandensein einer Attrappe nicht anders dar als beim Betrieb einer funktionstüchtigen Videokamera. Dies gilt umso mehr, als der Zweck einer Kameraattrappe einzig in deren abschreckender Wirkung liegt. Allein in dem bei den vermeintlich betroffenen Personen hervorgerufenen Eindruck der Live-Beobachtung sowie des Anfertigens einer Videoaufnahme und dem sich daraus ergebenden und gerade bei Attrappen zielgerichtet und bewusst bezweckten Überwachungsdruck sieht die Rechtsprechung bereits einen erheblichen Eingriff in das allgemeine Persönlichkeitsrecht. Sie spricht den Betroffenen Unterlassungs-, Beseitigungs- oder gar Schadensersatzansprüche zu. Vor diesem Hintergrund empfehle ich bei Attrappen regelmäßig deren Demontage oder zumindest eine Änderung der Ausrichtung dergestalt, dass für Außenstehende überhaupt nicht mehr der Eindruck einer Überwachung entstehen kann.

Zusätzliche Klarheit sowohl für Verantwortliche als auch Betroffene wurde mit der unter den Datenschutzaufsichtsbehörden bundesweit abgestimmten „Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen“ vom 17. Juli 2020 geschaffen (vgl. 7.3). Darin finden sich Informationen zu zahlreichen Fallgestaltungen, in denen Videokameras zum Einsatz kommen. Auch das bereits seit Längerem von den Aufsichtsbehörden empfohlene Vorgehen zur praxisgerechten Ausgestaltung der Informationspflichten des Art. 13 DSGVO wird darin nochmals erläutert (vgl. Tätigkeitsbericht 2019, 3.1.1, Seite 71 ff.).

Als ein Eingabeschwerpunkt kristallisieren sich immer mehr Streitigkeiten unter Nachbarn heraus (vgl. 2.2.23 bis 2.2.25). Als Gründe hierfür sehe ich sowohl die Unkenntnis der rechtlichen Voraussetzungen als auch eine mangelnde Sensibilisierung für datenschutzrechtliche Belange. Darüber hinaus scheint sich ein gewisser Gewöhnungseffekt einzustellen, ist es heute doch nahezu unmöglich, sich nach Verlassen des eigenen Wohnbereichs in Anbetracht der Beobachtungsdichte bei öffentlichen Verkehrsmitteln, Haltestellen, Bahnhöfen, Tankstellen unbeobachtet im öffentlichen Raum zu bewegen.

Dies hat mich bewogen, vor der Befassung meiner Behörde mit mir zur Kenntnis gebrachten Fällen den beteiligten Parteien mithilfe eines kurzen, zweiseitigen Hinweisblatts die für eine Videoüberwachung wesentlichen Informationen an die Hand zu geben. Die mir zur Verfügung stehenden personellen Ressourcen erlauben es bereits nicht, jedem aus dem nachbarschaftlichen Bereich stammenden Hinweis oder Beschwerde adäquat nachzugehen. Das Hinweisblatt kommt dann zur Anwendung, wenn sich aus dem mir vorgetragenen Sachverhalt noch keine belastbaren Anhaltspunkte ergeben, dass – neben der Überwachung nachbarlicher Grundstücke tatsächlich auch darüber hinausgehend öffentliche Verkehrsbereiche von der mutmaßlichen Videoüberwachung tangiert sind. Mit einem Schreiben an die beteiligten Parteien, denen ich jeweils das erwähnte Hinweisblatt beilege, verbinde ich die Hoffnung, dass dies zu einem Rückgang diesbezüglicher Beschwerden beiträgt, zumal mir in rein privaten nachbarschaftlichen Auseinandersetzungen nur eingeschränkte Untersuchungsbefugnisse zustehen und ich deshalb auf die Richtigkeit gemachter Angaben beziehungsweise auf freiwillige Offenbarungen vertrauen muss. Gerade bei zerrütteten Nachbarschaftsverhältnissen trägt dies in der Mehrzahl der Fälle nicht zu einer Befriedung bei. So verfüge ich insbesondere nicht über ein Betretungsrecht privater Grundstücke und Wohnungen. Die Vorschriften in Art. 58 Abs. 1 Buchst. f DSGVO sowie § 40 Abs. 5 Bundesdatenschutzgesetz eröffnen mir eine entsprechende Befugnis nur bei Geschäftsräumen.

1.5 Anwendung der Datenschutz-Grundverordnung auf die parlamentarische Tätigkeit

Die Geschäftsordnung des Sächsischen Landtags der 7. Wahlperiode enthält mit einer Verweisung in § 11 als Anlage 3 die Datenschutzordnung des Sächsischen Landtags. Sie soll die Verarbeitung personenbezogener Daten bei der Wahrnehmung parlamentarischer Aufgaben regeln.

Die Normsetzung entsprach bislang meiner bisherigen rechtlichen Einschätzung und der Auffassung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder. Danach sollte die Datenschutz-Grundverordnung (DSGVO) keine Anwendung auf Parlamente und deren Organe sowie die Tätigkeit der Abgeordneten in Bezug auf die parlamentarischen Kerntätigkeiten finden. Datenschutzrechtliche Vorgaben und eine Aufsicht der Aufsichtsbehörde sollte sich nur unter der Voraussetzung normenklarer gesetzlicher Bestimmungen ergeben (siehe den Beschluss im Wortlaut im Tätigkeitsbericht 2017/2018 Teil 2, 7.2.6). Insoweit wäre auch die eigenständige Regelung des Sächsischen Landtags erforderlich gewesen. Empfohlen hatte die Konferenz insoweit auch ausdrücklich eine an der DSGVO orientierte eigene „Datenschutzordnung“. Kongruent damit ist die Vorschrift des Sächsischen Datenschutzdurchführungsgesetzes, die bestimmt, dass soweit der Landtag, seine Gremien, seine Mitglieder, die Fraktionen und deren Beschäftigte sowie die Landtagsverwaltung in Wahrnehmung parlamentarischer Aufgaben personenbezogene Daten verarbeiten, im Wege

einer Datenschutzordnung des Parlaments Regelungen geschaffen werden sollen (siehe § 2 Abs. 1 Satz 4 Sächsisches Datenschutzdurchführungsgesetz und auch Satz 3 der Vorschrift).

Mit der Entscheidung des Europäischen Gerichtshofs vom 9. Juli 2020 in der Rechtssache C-272/19 war im Rahmen eines Vorabentscheidungsverfahrens über den Anwendungsbereich der DSGVO allerdings Gegenläufiges entschieden worden. Dem Rechtsstreit lag ein vom Verwaltungsgericht Wiesbaden zu beurteilender Auskunftsantrag eines Petenten zu Grunde, der nach Einreichen einer Petition Aufschluss über die Verarbeitung seiner personenbezogenen Daten begehrte. Diese wurde seitens des Hessischen Landtags abgewiesen, da der Geltungsbereich der DSGVO, die ein entsprechendes Auskunftsrecht gemäß Art. 15 vorsieht, verneint wurde.

Der Europäische Gerichtshof entschied hingegen, dass die DSGVO auch auf den Petitionsausschuss des Landesparlaments Anwendung findet. Könnte man dem Petitionsausschuss noch den Wirkungskreis einer exekutiven Tätigkeit zuordnen, urteilte das Gericht über den konkreten Schwerpunkt des Streits hinausgehend, dass Verantwortliche im Sinne der DSGVO nicht nur Behörden, sondern alle Stellen seien, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Datenverarbeitung entscheiden. Festgelegte spezifische Tätigkeiten der Staaten oder Stellen seien zwar vom Anwendungsbereich der DSGVO ausgenommen, dies gelte aber eben gerade nicht für parlamentarische Tätigkeiten.

Der zurückliegende Beschluss der Datenschutzkonferenz vom 5. September 2018 zur Anwendung der DSGVO im Bereich der Parlamente, Fraktionen, Abgeordneten und politischen Parteien ist daraufhin von den Datenschutzaufsichtsbehörden ausgesetzt worden (siehe Überblick zu den Beschlussmaterialien der Datenschutzkonferenz unter 7.3).

In Bezug auf die politischen Parteien, die zudem als nicht-öffentliche Stellen einzuordnen sind, ergeben sich gegenüber dem zurückliegenden Konferenzbeschluss von 2018 keine Änderungen. Sie sind zum einen weiterhin Normadressaten der DSGVO, zum anderen unterliegen sie unstreitig der Aufsicht der Datenschutzaufsichtsbehörden.

Den Sächsischen Landtag werde ich in der Angelegenheit – nach Abstimmung mit den anderen Datenschutzaufsichtsbehörden – weitergehend beraten.

1.6 Das Sächsische Datenschutzdurchführungsgesetz im Verhältnis zur Datenschutz-Grundverordnung und zum Bundesdatenschutzgesetz – Einwilligung im Beschäftigungsverhältnis

Im Berichtszeitraum war ich auch mit Fragen zur Form der wirksamen Einwilligung nach der Datenschutz-Grundverordnung (DSGVO) konfrontiert.

Das Sächsische Datenschutzdurchführungsgesetz enthält keine weiteren Bestimmungen zur Einwilligung. Nach Vorstellung des sächsischen Gesetzgebers sollten die Vorschriften der DSGVO genügen. Wie im 18. Tätigkeitsbericht (04/2015 bis 03/2017) unter 1.6, Seite 26 ff. bereits dargestellt, lässt die DSGVO für den nationalen und den Landesgesetzgeber nur bereichsspezifische Konkretisierungen und Ergänzungen bezüglich der Einwilligungen zu.

§ 11 Sächsisches Datenschutzdurchführungsgesetz regelt die Verarbeitung von Beschäftigtendaten öffentlicher sächsischer Stellen. Eine Einwilligungsregelung wie in der Vorgängervorschrift des § 37 Sächsisches Datenschutzgesetz enthält § 11aber nicht. Gleichwohl sollte das nicht zu Missverständnissen führen. Eine Einwilligung im Beschäftigungsverhältnis ist auch im Anwendungsbereich des § 11 Sächsisches Datenschutzdurchführungsgesetz zulässig. Dabei wird die Einwilligung im Beschäftigungsverhältnis, auch wegen der im Dienst- und Arbeitsverhältnis eher gleichmäßigen Datenverarbeitung eher die Ausnahme bleiben. Die Freiwilligkeit ist zudem trotz des Abhängigkeitsverhältnisses zu gewährleisten.

Demgegenüber legt das Bundesdatenschutzgesetz (BDSG) in § 26 Abs. 2 Satz 1 und 2 Auslegungsregeln zur Freiwilligkeit fest. Über die Bestimmungen der DSGVO zur Einwilligung hinausgehend legt § 26 Abs. 2 Satz 3 BDSG die Schriftform beziehungsweise elektronische Form der Einwilligung fest, soweit nicht wegen besonderer Umstände eine andere Form angemessen sei. In Satz 4 ist zudem die Pflicht zur Aufklärung in Textform über den Zweck der Datenverarbeitung und des Widerrufsrechts nach Art. 7 Abs. 3 DSGVO geregelt. Ergänzend wird in Abs. 3 auch bei der Einwilligung in die Verarbeitung besonderer Kategorien personenbezogener Daten auf Abs. 2 verwiesen (vgl. § 26 Abs. 3 Satz 2 BDSG).

Vereinzelt werden in der Literatur Überlegungen zur ergänzenden Anwendbarkeit der bundesdatenschutzgesetzlichen Vorschriften auch bei Verantwortlichen und Stellen nach Landesrecht vertreten. Der Wortlaut spricht dagegen: Das BDSG kommt nur insoweit für öffentliche Stellen der Länder zur Anwendung, soweit der Datenschutz nicht durch ein Landesgesetz geregelt ist und – kumulativ – soweit Bundesrecht ausgeführt wird, was bei der Verarbeitung von Beschäftigtendaten nicht zu bejahen ist.

Der Landesgesetzgeber hat entsprechende Regelungen schlicht nicht vorgesehen. Ergänzend kann nach meiner Überzeugung das BDSG keine Anwendung finden.

Im Ergebnis wird man, was die Auslegungsvermutungen und was insbesondere die Schriftform der Einwilligung angeht, die nach dem Sächsischen Datenschutzdurchführungsgesetz nicht verlangt ist, in der Praxis häufig zu gleichen oder vergleichbaren Ergebnissen kommen, gilt doch auch eine Nachweispflicht, was eine erfolgte Einwilligung anbelangt (vgl. Art. 7 Abs. 1 DSGVO sowie Erwägungsgrund 42 Satz 1 DSGVO). Für die Verarbeitung besonderer Kategorien personenbezogener Daten gilt dies im Besonderen, da für diesen Fall eine „ausdrückliche“ Einwilligung erforderlich wird. In meinem zurückliegenden Tätigkeitsbericht hatte ich bereits auf die Zweckmäßigkeit einer schriftlichen Erklärung des Einwilligenden für den Verantwortlichen hingewiesen (siehe 18. Tätigkeitsbericht für den öffentlichen Bereich (04/2015 bis 03/2017), 1.6, Seite 26 ff.). Die Schriftlichkeit beziehungsweise elektronische Form der Einwilligung ist sächsischen öffentlichen Stellen unabhängig von einer entsprechenden Formvorgabe zu empfehlen.

1.7 Konsultation bei staatlichen Rechtsetzungsvorhaben

Im Berichtszeitraum wurde ich bei verschiedenen Rechtsetzungsvorhaben verfahrensbegleitend beteiligt. Dabei handelte es sich beispielsweise um Stellungnahmen zur Sächsischen E-Government-Gesetz-Durchführungsverordnung, zum Sächsischen Schulgesetz und den Sächsischen Corona-Schutz-Verordnungen sowie dem Sächsischen Ausführungsgesetz zum Glückspielstaatsvertrag. Stellung bezog ich auch mit den anderen Mitgliedern der Datenschutzkonferenz hinsichtlich der Bundesgesetzgebung, etwa bei der Evaluierung des Bundesdatenschutzgesetzes oder zum Entwurf des Registermodernisierungsgesetzes.

Art. 36 Abs. 4 Datenschutz-Grundverordnung (DSGVO) bestimmt, dass die staatlichen rechtsetzenden Körperschaften sowohl bei formeller Gesetzgebung als auch bei Verordnungen, die die personenbezogene Datenverarbeitung betreffen, die Aufsichtsbehörde zu konsultieren haben. Sie gilt – selbstverständlich – auch für die Ebene der eigenstaatlichen Länder.

Erwägungsgrund 96 der europarechtlichen Verordnung besagt, dass die Konsultation der Aufsichtsbehörde während der Ausarbeitung von Gesetzes- oder Regelungsvorschriften erfolgen soll, um die Vereinbarkeit der geplanten Verarbeitung mit der DSGVO sicherzustellen. Insoweit ist zu betonen, dass regelmäßig eine zeitlich adäquate Beteiligung meiner Dienststelle anzustreben ist.

Die Konsultationspflicht gegenüber meiner Behörde gilt für Vorhaben materiell-rechtlicher Gesetze jeder Art. Das schließt auch bloße Änderungen, die einzelne Rechtsvorschriften zu personenbezogener Datenverarbeitung zum Gegenstand haben, ein. Nach meiner Überzeugung gehören ebenso für Staatsverträge, die der Freistaat Sachsen mitzeichnet, dazu. Sie bindet

die Staatsregierung, wohl aber auch den Sächsischen Landtag und dessen Organe, wenn Gesetzesvorhaben initiativ durch den Landtag eingeleitet werden sollen (siehe 1.5).

Die Geschäftsordnung der Sächsischen Staatsregierung enthält eine Bestimmung zur Beteiligung des Sächsischen Datenschutzbeauftragten (siehe § 12 Abs. 3 Satz 2). Der materiellrechtlichen Vorschrift des Art. 36 Abs. 4 DSGVO und den dargestellten Erwägungsgründen könnte die in der Geschäftsordnung der Sächsischen Staatsregierung enthaltene Festlegung in § 12 Abs. 3 Satz 1 nur bedingt entsprechen, bezieht man sie auch auf den Satz 2 und soweit der Sächsische Datenschutzbeauftragte regelmäßig nach Fertigstellung eines Referentenentwurfs beteiligt werden soll. Dem Wortlaut nach sollen „Gesetzentwürfe, Entwürfe von Rechtsverordnungen der Staatsregierung, Entwürfe zu Vorlagen und Schreiben der Staatsregierung [...] erst nach Beschlussfassung der Staatsregierung über die Freigabe zur Anhörung an den Landtag, andere Körperschaften, Verbände oder sonstige Organisationen weitergeleitet“ werden. Im Blick sollte behalten werden, dass nach den Vorstellungen des europäischen Verordnungsgebers die Beteiligung der Aufsichtsbehörde (Konsultation) „während der Ausarbeitung“ und zur Sicherstellung einer datenschutzrechtlichen Gesetzeskonformität erfolgen soll. Bei komplexeren Rechtstexten mit Datenverarbeitungsbezug empfiehlt sich insoweit auch für den federführenden Geschäftsbereich der Regierung eine vorgezogene Beteiligung meiner Behörde. Legt man den Text der Geschäftsordnung, der nicht unbedingt in Verbindung mit dem vorstehenden Satz gelesen werden muss und vom Wortlaut her schlicht besagt, dass soweit das Recht auf informationelle Selbstbestimmung betroffen ist, der Sächsische Datenschutzbeauftragte zu beteiligen ist, so aus, dass auch eine zeitlich vorgelagerte Konsultation meiner Behörde nicht ausgeschlossen ist, könnte und sollte man einer bestmöglichen Beratung durch Beteiligung meiner Behörde Rechnung tragen.

Über den Appell einer frühzeitigen Konsultation hinaus bleibt mir, die Befolgung des Art. 36 Abs. 4 DSGVO grundsätzlich anzumahnen. Die Nichteinhaltung ist natürlich ein Verstoß gegen die DSGVO.

Abschließend weise ich noch auf § 20 Sächsisches Datenschutzdurchführungsgesetz hin. Demnach haben öffentliche Stellen meine Behörde über den beabsichtigten Erlass von Verwaltungsvorschriften – soweit sie das Recht auf informationelle Selbstbestimmung betreffen – zu informieren. Dabei handelt es sich um eine ergänzende Vorschrift für untergesetzliche Rechtsetzung, die ich im vorstehenden Zusammenhang nicht weiter zu betrachten hatte.

1.8 Gesetz zum 23. Rundfunkänderungsstaatsvertrag

Der Ausschuss für Wissenschaft, Hochschule, Medien, Kultur und Tourismus des Sächsischen Landtags hat sich im Frühjahr 2020 mit dem Gesetzentwurf der Staatsregierung zum Gesetz zum Dreiundzwanzigsten Rundfunkänderungsstaatsvertrag (Drucksache 7/679) befasst. Ich habe dies zum Anlass genommen, dem Ausschuss meine datenschutzrechtliche Position mitzuteilen. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat sich bereits im Frühjahr 2019 mit den geplanten Änderungen des Rundfunkänderungsstaatsvertrages befasst. Die datenschutzrechtlichen Bedenken wurden durch den damaligen Konferenzvorsitzenden Prof. Dr. Dieter Kugelmann, Landesbeauftragter für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz, in der Sitzung der Rundfunkkommission der Länder vorgetragen. Im April 2019 hat die Datenschutzkonferenz diese Position als Beschluss „Geplante Einführung eines regelmäßigen vollständigen Meldedatenabgleichs zum Zweck des Einzugs des Rundfunkbeitrags stoppen“ verabschiedet – veröffentlich als PDF-Datei auf datenschutzkonferenz-online.de.

Ungeachtet dessen haben die Regierungschefs der Länder am 6. Juni 2019 den Entwurf des 23. Rundfunkänderungsstaatsvertrags beschlossen. Der Sächsische Landtag wurde vom Ministerpräsidenten des Freistaates Sachsen am 21. Juni 2019 darüber (Drucksache 6/18143) informiert.

Der vorliegende Entwurf war hinsichtlich des Meldedatenabgleichs selbst unverändert. Er war aber „zur Wahrung der Verhältnismäßigkeit zwischen Beitragsgerechtigkeit und dem Schutz persönlicher Daten“ um eine Regelung ergänzt worden, nach der ein Abgleich unterbleiben soll, soweit die Kommission zur Ermittlung des Finanzbedarfs bei Rundfunkanstalten (KEF) feststellt, dass der Datenbestand hinreichend aktuell ist. Die Beurteilung solle die Kommission unter Berücksichtigung der Entwicklung des Beitragsaufkommens „und sonstiger Faktoren“ vornehmen. Darüber hinaus sah der Entwurf Einschränkungen für die Rechte der betroffenen Personen auf Information gemäß Art. 13 Datenschutz-Grundverordnung (DSGVO) und Auskunft (Art. 15 DSGVO) vor.

Die Datenschutzkonferenz hat bereits den im Jahr 2013 durchgeführten erstmaligen Datenabgleich als datenschutzrechtlich hochbedenklich eingestuft. Den damals vorgetragenen Bedenken wurde mit Verweis auf die notwendige Erhebung im Rahmen der Umstellung des Gebührenmodells auf das Wohnungsprinzip und die Einmaligkeit der Erhebung begegnet.

Die nun vorgesehene regelmäßige Wiederholung des vollständigen Meldedatenabgleichs in einem vierjährigen Turnus stellt einen unverhältnismäßigen Eingriff in die informationelle Selbstbestimmung dar und steht im Konflikt mit den in der DSGVO vorgegebenen Grundsätzen der Datenminimierung und der Erforderlichkeit (Art. 5 Abs. 1 Buchst. a und c, Art. 6 Abs. 1 DSGVO). Bei einem vollständigen Meldedatenabgleich werden in großem Umfang Daten von

Personen verarbeitet, die entweder gar nicht beitragspflichtig sind (weitere Bewohnerinnen oder Bewohner neben dem Beitragszahlenden in einer Wohnung oder generell Gebührenbefreite) oder bereits ordnungsgemäß als Beitragszahlende erfasst sind. Darüber hinaus umfasst der Meldedatenabgleich mehr Daten, zum Beispiel Doktorgrad und Familienstand, als für eine Beitragserhebung erforderlich sind.

Die Rundfunkanstalten gehen im Übrigen selbst davon aus, dass ein vollständiger Meldeabgleich letztlich in weniger als einem Prozent der Fälle zu einer zusätzlichen, dauerhaften Anmeldung von Beitragspflichtigen führt (siehe Evaluierungsbericht der Länder gemäß § 14 Abs. 9a Rundfunkbeitragsstaatsvertrag vom 20. März 2019). Das Bedürfnis der Rundfunkanstalten nach einer berechtigten Sicherung ihrer Einnahmen wäre mit gezielten Maßnahmen ebenso realisierbar, für die spezielle Übermittlungsbefugnisse geschaffen werden könnten. Stattdessen soll eine Übermittlung des kompletten Datenbestandes der Einwohnermeldeämter in Bezug auf sämtliche volljährige Bürgerinnen und Bürger verstetigt werden.

Die Regelungen berücksichtigen die Maßstäbe der DSGVO nicht in ausreichendem Maße. Aufgrund des Anwendungsvorrangs europäischer Verordnungen müssen nationale Datenschutzvorschriften auf eine Öffnungsklausel der DSGVO gestützt werden können. Bei Regelungen, die auf die Öffnungsklausel nach Art. 6 Abs. 2 und Abs. 3 in Verbindung mit Art. 6 Abs. 1 Buchst. e DSGVO gestützt werden, sind die Grundsätze der Datenminimierung und Erforderlichkeit zu beachten. Danach dürfen mitgliedstaatliche Regelungen für die Erfüllung von Aufgaben eingeführt werden, die im öffentlichen Interesse liegen, wenn sie die DSGVO zwar präzisieren, nicht aber deren Grenzen überschreiten. Regelungen, die sich auf diese Öffnungsklausel beziehen, müssen sich folglich in dem Rahmen halten, den die DSGVO vorgibt. Bei der neuen Regelung bestehen in dieser Hinsicht erhebliche Bedenken im Hinblick auf die Grundsätze der Datenminimierung und der Erforderlichkeit.

Die aufgrund der Äußerungen der Datenschutzkonferenz vorgesehene Regelung zum Verzicht auf den Meldedatenabgleich ist ebenfalls problematisch. Das Gesetz belässt Vorgaben zur Ermittlung der Aktualität des Meldedatenbestands an die KEF bei der vagen Formulierung „unter Berücksichtigung der Entwicklung des Beitragsaufkommens und sonstiger Faktoren". Damit wird den datenschutzrechtlichen Bedenken jedoch nicht ausreichend Rechnung getragen. Die Ergänzung schafft vielmehr ein zusätzliches verfassungsrechtliches Problem, indem die Entscheidung über die Durchführung eines vollständigen Meldedatenabgleichs an die KEF delegiert wird, ohne dieser klare Kriterien für diese Entscheidung an die Hand zu geben. Solche wesentlichen Entscheidungen in Bezug auf die Verarbeitung personenbezogener Daten aller volljährigen Einwohnerinnen und Einwohner Deutschlands muss jedoch der Gesetzgeber selbst treffen (Gesetzesvorbehalt).

Das Gesetz sieht weiterhin Einschränkungen der Rechte betroffener Personen vor. So können Auskunftsrechte der betroffenen Personen nach Art. 15 DSGVO beschränkt werden. Das datenschutzrechtlich vorgesehene Prinzip, dass eine Auskunft vollständig oder mit gesetzlich

festgelegten Ausnahmen zu erfolgen hat, wird im Gesetz grob missachtet, indem eine Auskunftserteilung auf eine abschließende Liste von Daten beschränkt wird. Diese geplante Beschränkung des Auskunftsrechts ist mit den Bestimmungen der DSGVO nicht vereinbar: Art. 23 Abs. 1 DSGVO enthält eine abschließende Aufzählung der Gründe, aus denen der nationale Gesetzgeber Betroffenenrechte über das in der DSGVO selbst vorgesehene Maß hinaus einschränken kann. Der Gesetzgeber stützt sich dabei auf den „Schutz sonstiger wichtiger Ziele im allgemeinen öffentlichen Interesse“. In der Begründung wird ausgeführt, dass die Regelung sicherstellen soll, dass „die Auskunftspflichten der Landesrundfunkanstalten das Ziel der Datenverarbeitung beziehungsweise die Erfüllung des damit verfolgten öffentlichen Interesses nicht gefährden“. Diese Begründung ist in Anbetracht der zu erwartenden Auskunftsersuchen absurd und missachtet die in der DSGVO verankerten Grundrechte betroffener Personen.

Die zusätzliche Einschränkung der Auskunftsrechte für Daten „die nur deshalb gespeichert sind, weil sie aufgrund gesetzlicher oder satzungsmäßiger Aufbewahrungsvorschriften nicht gelöscht werden dürfen oder ausschließlich Zwecken der Datensicherung oder der Datenschutzkontrolle dienen" ist datenschutzrechtlich ebenfalls nicht zulässig. Der Landesgesetzgeber hat das Unterbleiben der Auskunft nach Artikel 15 DSGVO im Sächsischen Datenschutzdurchführungsgesetz (SächsDSDG) abschließend geregelt. Durch die jetzige Regelung werden damit die Auskunftsrechte der betroffenen Personen über das sonst für öffentliche Stellen des Freistaates geltende Maß hinaus weiter beschränkt, ohne dass dafür eine Notwendigkeit ersichtlich ist.

Der Sächsische Landtag hat das Gesetz zum Dreiundzwanzigsten Rundfunkänderungsstaatsvertrag am 29. April 2020 beschlossen.

1.9 „Eigeninitiierte“ Öffentlichkeitsarbeit von Behörden

Gelegentlich erhalte ich Beschwerden von Personen, die auf polizeiliche Veröffentlichungen hin angesprochen werden, weil die Angaben in den Meldungen die Identifizierbarkeit ihrer Person ermöglichten. Bei den angesprochenen Personen handelt es sich zumeist um Geschädigte von Straftaten. So erreichte mich im vergangenen Jahr die Petition eines Arztes, dessen Praxis Ziel eines Einbruchs geworden war. In der dazu ergangenen Medieninformation, veröffentlicht auf der Website der zuständigen Polizeidirektion, war von einem Einbruch in eine Arztpraxis auf der konkret benannten Straße die Rede. Die Meldung enthielt auch Angaben zur Höhe des Stehl- und Sachschadens sowie die Information, dass ein Tresor mit einer exakt bezeichneten Summe Bargeld, Blankorezepten, diversen Arzneimitteln und Datenträgern entwendet worden sei. Aufgrund der örtlichen Angaben konnte ohne Weiteres auf die konkrete Praxis geschlossen werden. Noch am Tag der polizeilichen Veröffentlichung der Meldung sei der Arzt von einer Boulevardzeitung und Bekannten kontaktiert und zum Einbruch befragt worden, unter anderem dazu, ob Patientendaten gestohlen worden seien.

Der Fall verdeutlicht die Risiken, die in der Veröffentlichung von zu präzisen Angaben über konkrete Vorkommnisse liegen. Ist anhand der Angaben in den polizeilichen Informationen ein Personenbezug herstellbar, liegt ein Eingriff in das Grundrecht der betroffenen Person auf informationelle Selbstbestimmung vor. Eine hierfür erforderliche gesetzliche Grundlage allerdings fehlt. In der – konstruktiven – Erörterung des Vorfalls mit der Polizeidirektion stellte sich heraus, dass bislang keine Richtlinien oder vergleichbaren Regelungen existierten, die den Bewertungsprozess zur Veröffentlichung von polizeilich relevanten Sachverhalten beschreiben. Ich habe daher gegenüber dem Sächsischen Staatsministerium des Innern (SMI) dringend angeregt, die Polizeidienststellen im Freistaat bei der datenschutzgerechten Formulierung und Veröffentlichung von Polizeimeldungen beziehungsweise Medieninformationen zu unterstützen, indem Hinweise zur Vermeidung eines Personenbezugs in entsprechenden Meldungen gegeben werden.

Im September 2020 trat die Kommunikationsrichtlinie der Polizei Sachsen, die einen verbindlichen Rahmen für die Kommunikation der Polizei Sachsen hinsichtlich der Ziele, Struktur, Aufgaben, Inhalte und Prozesse beschreibt, in Kraft.

Zudem wurde aufgrund meiner Anregung mit der Überarbeitung der Gemeinsamen Verwaltungsvorschrift des Sächsischen Staatsministeriums der Justiz und des Sächsischen Staatsministeriums des Innern über die Unterrichtung der Öffentlichkeit in Strafverfolgungssachen vom 29. Januar 1992 unter der Federführung des Sächsischen Staatsministeriums der Justiz und für Demokratie, Europa und Gleichstellung (SMJusDEG) begonnen. Im Rahmen der hierfür erforderlichen Abstimmung des SMI mit dem SMJusDEG wurde ich seitens des SMI um Stellungnahme dahingehend gebeten, inwieweit § 4 Sächsisches Gesetz über die Presse (SächsPresseG) als Rechtsgrundlage für eine „eigeninitiierte“ Öffentlichkeitsarbeit staatlicher Behörden – in deren Rahmen gegebenenfalls personenbezogene beziehungsweise -beziehbare Daten offengelegt werden können – herangezogen werden kann.

Ich vertrete seit jeher die Auffassung, dass Behördeninformationen, die eigeninitiiert, also ohne zugrundeliegende Presseanfrage, auf der Website der Behörde oder in einem anderen Medium veröffentlicht werden und die sich mithin nicht (nur) an die Presse richten, sondern unmittelbar für eine breite Öffentlichkeit bestimmt sind, mangels tauglicher Ermächtigungsgrundlage unzulässig in Grundrechte eingreifen, sofern sie personenbezogene oder personenbeziehbare Daten enthalten. Nach § 4 Abs. 1 Satz 1 SächsPresseG sind alle Behörden verpflichtet, den Vertretern der Presse und des Rundfunks, die sich als solche ausweisen, die der Erfüllung ihrer öffentlichen Aufgabe dienenden Auskünfte zu erteilen, sofern nicht spezielle Regelungen des Sächsischen Gesetzes über die Presse selbst oder allgemeine Rechtsvorschriften dem entgegenstehen. Dem gesetzgeberischen Willen nach ist somit gerade nicht jeder beziehungsweise „die Öffentlichkeit“ anspruchsberechtigt. Auf welche Weise die Behörde („Wie“) die konkrete Anfrage eines oder mehrerer Pressevertreter beantwortet (allgemeine Medieninformation durch Pressemitteilung oder singuläre Auskunftserteilung), liegt grundsätzlich in deren Ermessen. Allerdings muss die Behörde im Rahmen ihrer umfassenden Abwägung

zwischen dem Interesse der Presse an der Offenlegung der Information und den gegenläufigen Interessen Betroffener am Unterbleiben der Auskunft auch diesen Punkt berücksichtigen (§ 4 Abs. 2 SächsPresseG). Danach darf die Behörde die Auskunft gegenüber den Pressevertretern unter anderem verweigern, wenn und soweit durch sie ein überwiegendes schutzwürdiges privates Interesse verletzt würde oder ihr Umfang das zumutbare Maß überschreiten würde. So wäre es kaum erforderlich und verhältnismäßig, auf eine Anfrage eines einzelnen Pressevertreters mittels einer allgemeinen, jedermann zugänglichen Pressemitteilung zu antworten. Voraussetzung für die Erteilung von Auskünften ist in jedem Fall die Anfrage zumindest eines auskunftsberechtigten Vertreters der Presse.

Der Auffassung, dass § 4 SächsPresseG keine taugliche Rechtsgrundlage für „eigeninitiierte“ behördliche Öffentlichkeitsarbeit unter Offenlegung personenbezogener und -beziehbarer Daten ist, steht auch nicht entgegen, dass eine Auskunftserteilung an Pressevertreter rein faktisch – bei späterer Veröffentlichung der Informationen durch die Presse – in ihren Auswirkungen auf das geschützte Recht auf informationelle Selbstbestimmung des Betroffenen der direkten Information der Öffentlichkeit häufig gleich käme. Bei der Veröffentlichung dieser personenbezogenen oder personenbeziehbaren Daten durch die Presse handelt es sich gerade nicht um staatliche Eingriffe in den grundrechtlich geschützten Rechtskreis der Bürger, sondern, jedenfalls bei der Tätigkeit von Pressevertretern, um eine ebenfalls grundrechtlich geschützte Tätigkeit. Eine Behörde wird aber nicht journalistisch tätig. Auch wenn sie Öffentlichkeitsarbeit betreibt, kann sie sich nicht auf die Pressefreiheit berufen.

Diese Grundsätze und insbesondere die Feststellung, dass der landesrechtlich bestimmte Auskunftsanspruch der Presse keine Rechtsgrundlage für eine eigeninitiierte Information der Öffentlichkeit unter Offenlegung personenbezogener Daten durch Behörden darstellt, wurden jüngst durch eine Entscheidung des OVG Münster zu einer (unzulässigen) Internetveröffentlichung eines Amtsgerichts über die Anklage gegen einen Prominenten bestätigt (OVG Münster, Beschluss vom 4. Februar 2021 – 4 B 1380/20).

Die prinzipiellen Überlegungen zum sächsischen Presserecht und zur Befugnis, der Öffentlichkeit beziehungsweise Medien Informationen zu offenbaren, gelten nicht allein für Polizei und Strafverfolger; sie sind auf andere Bereiche der Verwaltung übertragbar.

2 Grundsätze der Datenverarbeitung

2.1 Datenverarbeitungsgrundsätze, Begriffsbestimmungen

2.1.1 Betriebsarzt als eigener Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO

Vereinzelt hatte ich mich mit der Frage auseinanderzusetzen, ob Betriebsärzte als eigene Verantwortliche im Sinne der Datenschutz-Grundverordnung anzusehen sind. Interne Betriebsärzte sind nach meiner Überzeugung als funktionale Stellen innerhalb des Verantwortlichen anzusehen. Sie sind aber dem Verantwortlichen zugehörig und keine eigenen Verantwortlichen. Dies gilt auch, wenn die Betriebsärzte als Berufsgeheimnisträger agieren. Zwar unterliegen sie einer besonderen Geheimhaltungspflicht, die dazu führt, dass sie innerhalb der datenverarbeitenden Stelle informationell abgeschottet agieren und sie unterliegen auch innerhalb ihres geheimhaltungspflichtigen Wirkungsbereichs fachlich-inhaltlich keiner Weisungspflicht, doch bleiben sie weiterhin Teil der Entität. Betroffenenrechte, wie zum Beispiel bei nicht selten auftretenden Auskünften, sind von internen Betriebsärzten eigenständig ohne Verletzung von Geheimhaltungspflichten zu erfüllen. Der Verantwortliche hat aber die technisch-organisatorischen Möglichkeiten und Voraussetzungen zur prozessualen Umsetzung zu schaffen (vgl. auch Tätigkeitsbericht 2019, 9.3, Seite 165 ff. und Tätigkeitsbericht 2017/2018, 2.11.1, Seite 103 f.).

Anders zu betrachten ist die Tätigkeit externer Betriebsärzte. Bei diesen handelt es sich um eigene Verantwortliche, die zwar im Auftrag der personalverwaltenden Stelle datenverarbeitend tätig sind, aber eben selbst über Zweck und Mittel der Verarbeitung der personenbezogenen Daten entscheiden.

2.1.2 Datenschutzbeauftragter als eigener Verantwortlicher

Im letzten Berichtszeitraum war ich mit einer Beschwerde konfrontiert, bei der betroffene Personen sich an mich wandten, da sie Auskunft von einem externen Datenschutzbeauftragten begehrten. Zuvor hatten sich die betroffenen Personen bereits an den Verantwortlichen, der eigentlichen datenverarbeitenden Stelle, mit einem Auskunftsersuchen gewandt, woraufhin sich der externe Datenschutzbeauftragte eingeschaltet hatte.

Den internen Datenschutzbeauftragten behandelt meine Behörde als einen dem Verantwortlichen zuzuordnenden Funktionsträger, auch wenn dieser weisungsfrei agiert – Art. 38 Abs. 3 Satz 1 Datenschutz-Grundverordnung (DSGVO) – und einem Berufsgeheimnisträger gleichgestellt wird (vgl. 3.1.2 am Ende sowie den Wortlaut von Art. 38 Abs. 5 DSGVO, vgl. zudem Tätigkeitsbericht 2019, 9.3, Seite 165 ff. und Tätigkeitsbericht 2017/2018, 2.11.1, Seite 103 f.).

Anders zu beurteilen ist es wiederum bei einem gewerblich tätigen – externen – Datenschutzbeauftragten. Dieser betreibt selbst die personenbezogenen Datenverarbeitungsprozesse und bestimmt über den Zweck und die Mittel der Verarbeitung.

Auch sind die Inhalte der verarbeiteten Daten nicht inkorporiert. Das heißt, die Datenverarbeitung ist ausgegliedert und mit der Verarbeitung des Verantwortlichen, der den externen Datenschutzbeauftragten benannt hat, nur teilidentisch. So werden auch bei externen Datenschutzbeauftragten in der Praxis Beschwerden und abweichende Inhalte zum Beschwerdeverfahren verarbeitet werden, zu denen der benennende Verantwortliche selbst keinen Zugang hat oder die ihm nicht lediglich aus Geheimhaltungsgründen sondern auch prozessual vorenthalten werden (vgl. 2.1.1).

Insoweit besteht auch für betroffene Personen grundsätzlich ein Auskunftsrecht gemäß Art. 15 DSGVO gegenüber externen Datenschutzbeauftragten. Auskunftsersuchen gegenüber internen Datenschutzbeauftragten sind hingegen als Auskünfte gegenüber dem Verantwortlichen zu werten. Im Falle von in Rede stehenden Geheimhaltungspflichten wird der interne Datenschutzbeauftragte aber gegebenenfalls selbst auskunftserfüllend tätig.

2.1.3 MDK-Reformgesetz – Medizinischer Dienst als eigener Verantwortlicher

Mit dem zum 1. Januar 2020 in Kraft getretenen MDK-Reformgesetz (BT-DS 19/13397) stellen die Medizinischen Dienste der Krankenversicherung (MDK) keine Arbeitsgemeinschaften der Krankenkassen mehr dar, sondern werden als eigenständige Körperschaft des öffentlichen Rechts einheitlich unter der Bezeichnung „Medizinischer Dienst“ (MD) geführt.

Im Zuge dessen ist in Paragraf 276 Abs. 2 Fünftes Buch Sozialgesetzbuch (SGB V) – er ist für den MD eine zentrale Rechtsgrundlage zur Datenverarbeitung – die Vorschrift des § 35 SGB I ausdrücklich aufgenommen worden. Dies stellt sicher, dass der MD auch in seiner neuen Rechtsform als eigenständige Körperschaft des öffentlichen Rechts als Stelle nach § 35 des Ersten Buches (SGB I) dem Sozialdatenschutz unterliegen. Bisher war dies der Fall, da die MDK als Arbeitsgemeinschaften der Krankenkassen von § 35 Abs. 1 Satz 4 SGB I umfasst waren. Um ein Absenken des Schutzniveaus für die durch den MD verarbeiteten Daten zu verhindern, ist es sachgerecht, den MD auch weiterhin an die strengen bereichsspezifischen Regelungen des Sozialdatenschutzes nach dem SGB zu binden.

2.1.4 Verdeckte Erhebung von Fahrzeugkennzeichen – Transparenz

Eine Kundin eines Unternehmens, das hochwertige Geräte an Laufkundschaft vermietet, hatte sich darüber beschwert, dass ein Beschäftigter der Firma das amtliche Kennzeichen ihres im

Hof auf einem Kundenparkplatz abgestellten Kraftfahrzeugs auf einem Blatt Papier notiert hätte.

Auf Nachfrage räumte das Unternehmen ein, Fahrzeugkennzeichendaten in Einzelfällen auf nichtautomatisiertem Weg (Papiernotiz) zu erheben, soweit keine andere geeignete Möglichkeit zu Identifikation (in der Regel durch Vorlage des Personaldokuments) möglich sei. Festgelegt sei dann jedoch eine unmittelbare Information der betroffenen Kunden über dieses Vorhaben. Nach beanstandungsfreier Rückgabe des gemieteten Gerätes würden die Daten sofort wieder gelöscht.

Den Widerspruch zwischen dem insoweit nicht bestrittenen Sachverhalt sowie der Compliance-Regel habe ich nicht weiterverfolgt. Auch war fraglich, ob der sachliche Anwendungsbereich der Datenschutz-Grundverordnung (DSGVO) eröffnet gewesen war (Art. 2 Abs. 1 DSGVO). Dem Unternehmen habe ich jedoch deutlich gemacht, dass kommunikative Transparenz in Bezug auf die Wahrung legitimer Interessen Beschwerden zu vermeiden hilft (vgl. Art. 5 Buchst. a DSGVO). Diese Feststellung gilt allübergreifend.

2.1.5 Geschwärzte Ausweiskopien nach Geldwäschegesetz – Datenminimierung

Nach den §§ 8, 10, 12 Geldwäschegesetz (GwG) müssen geldwäscherechtlich Verantwortliche die Identität des wirtschaftlich Berechtigten eines (anzubahnenden) Geschäfts prüfen und dies dokumentieren. Dazu ist grundsätzlich die Kopie des vorgelegten Ausweisdokuments zulässig, da einer entsprechenden gesetzlichen Pflicht gehorcht wird (vgl. Art. 6 Abs. 1 Buchst. c DSGVO).

Der genaue Umfang dieser verpflichtenden Kopie des Ausweisdokuments ist jedoch umstritten. Da die zugrundeliegende Vorschrift des § 8 Abs. 2 S. 2 GwG in den letzten Jahren mehreren Gesetzesänderungen, zuletzt zum Beginn des Berichtszeitraums, unterlag, kursieren hier widersprüchliche Informationen.

Zu diesem Thema erreichen mich regelmäßig Beschwerden und Beratungsanfragen. Daneben war die Frage der Möglichkeit einer Teilschwärzung entsprechender Kopien beziehungsweise Beschränkung von elektronischen Kopien etwa durch Kopiermasken auch Gegenstand im Arbeitskreis Kreditwirtschaft der Datenschutzkonferenz (DSK).

Nach meiner gefestigten Auffassung hat aus einer Reihe von Gründen der betroffene Ausweispflichtige das Recht, für die Zwecke des GwG nicht erforderliche Angaben in der Kopie des Ausweisdokuments unkenntlich zu machen beziehungsweise bei der optoelektronischen Erfassung teilweise abzudecken, insbesondere Körpergröße, Augenfarbe, Lichtbild und Zugangsnummern; siehe im Einzelnen unten.

Die zugrundeliegende geldwäscherechtliche Erfassung von Verantwortlichen und Geschäften wird regelmäßig ausgeweitet, so dass zunehmend auch kleinere Unternehmer wie Makler und Güterhändler betroffen sind. Aus der Vervielfachung betroffener Transaktionen und entsprechender Systeme zur Datenverarbeitung folgt eine ganz erhebliche Steigerung der datenschutzrechtlichen Risiken. Damit sind nicht mehr nur wenige, zentrale und mit umfangreichen Compliance-Systemen ausgestattete Verantwortliche zu Dokumentationen nach GwG verpflichtet. Vielmehr sind entsprechende Kopien über eine siebenstellige Anzahl teilweise wenig abgesicherter IT- und Aktensysteme verteilt. Daneben gebietet auch die zunehmende digitalisierte Erfassung von Ausweiskopien, die damit massiv angestiegene Missbrauchsgefahr wirksam zu begrenzen. Denn derartige hochauflösende elektronische Kopien (Scans) weisen typischerweise eine gegenüber Fotokopien substantiell gesteigerte Qualität und Weiterverwendbarkeit auf. Sie können zudem viel leichter verloren gehen, und etwa zu Identitätsdiebstahl und Dokumentenfälschung missbraucht werden.

Die zum Recht des Betroffenen auf Schwärzung beziehungsweise Teilabdeckung spiegelbildliche Pflicht für Dokumentationspflichtige folgt aus dem Gebot der Datenminimierung (Art. 5 Abs. 1 Buchst. c DSGVO). Dies gilt insbesondere auch für elektronische Kopien oder Scans, deren datenschutzrechtliches Risiko gegenüber Kopien auf Papier erheblich gesteigert ist. Denn auch bei der Erhebung und Verarbeitung von Ausweiskopien ist dem aktualisierten Wortlaut des § 8 Abs. 2 Satz 2 GWG und höherrangigem Recht Rechnung zu tragen. Lediglich für die Videoidentifizierung kann gelten, dass die vollständige Aufnahme auch des Ausweisdokumentes zulässig ist, soweit dies von der Einwilligung umfasst und für den Zweck der Identifikation erforderlich ist. Diese für Missbrauch zunehmend anfälligen Daten (vgl. etwa "deepfakes") sind jedoch entsprechend der von ihnen ausgehenden Risiken nochmals gesteigerten Schutzpflichten unterworfen.

In allen Fällen, in denen im Freistaat Sachsen ansässige Verantwortliche Kopien anfertigen wollten oder anfertigten, konnte ich durch entsprechende Hinweise eine Schwärzung oder Teilabdeckung beim Kopiervorgang erwirken. In Fällen, in denen (auch) von anderen Behörden beaufsichtigte Verantwortliche Kopien anfertigen, kann ich lediglich im Rahmen meines Beratungsmandats auf meine Rechtsauffassung und gegebenenfalls das rechtliche Klärungsbedürfnis hinweisen sowie das Verfahren an die zuständige Behörde verweisen.

Um der Uneinheitlichkeit der Rechtsauslegung entgegenzuwirken und Verantwortlichen wie betroffenen Personen eine eigene Entscheidung im Rahmen ihrer Verantwortung beziehungsweise Rechte zu ermöglichen, werden nachfolgend die wesentlichen Argumente dargestellt:

Für eine Vollständigkeit der anzufertigenden Kopie und damit einen Ausschluss von Schwärzungen wird angeführt, dass begrifflich jede Kopie vollständig zu sein habe. Auch sei das Bundesfinanzministerium dieser Auffassung – freilich ohne dass erkennbar die für die konkrete Geldwäscheverfolgung und -ermittlung zuständigen Behörden beteiligt worden wären. Ein kon-

kreter inhaltlicher Grund für diese Auffassung ist trotz eingehender Diskussionen weder vorgetragen noch ersichtlich. Allerdings wäre nach dieser Auffassung die frühere Qualifikation der anzufertigenden Kopie im Gesetz zur Umsetzung der Vierten Geldwäscherichtlinie, zur Ausführung der EU-Geldtransferverordnung und zur Neuorganisation der Zentralstelle für Finanztransaktionsuntersuchungen als „vollständig“ zumindest überflüssig gewesen.

Zwar ist aus den Gesetzgebungsmaterialien des Gesetzes zur Umsetzung der Änderungsrichtlinie zur Vierten EU-Geldwäscherichtlinie nicht direkt ersichtlich, aus welchen Gründen der Gesetzgeber die Qualifizierung „vollständig“ aus der Vorschrift des § 8 Abs. 2 GwG entfernt hat. Anhaltspunkte für ein Gesetzgebungsversehen sind jedoch nicht erkennbar: Die 2020 in § 8 Abs. 2 GWG erfolgte Änderung trägt vielmehr den ausdrücklichen Vorgaben der umzusetzenden Fünften Geldwäsche-Richtlinie Rechnung (Richtlinie (EU) 2018/843 des Europäischen Parlaments und des Rates vom 30. Mai 2018 zur Änderung der Richtlinie (EU) 2015/849 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung und zur Änderung der Richtlinien 2009/138/EG und 2013/36/EU). Art. 1 Nr. 25 betont die Beschränkung der Kopie auf das Erforderliche explizit. Danach ist "eine Kopie der erhaltenen Dokumente und Informationen, die für die Erfüllung der Sorgfaltspflichten gegenüber Kunden gemäß Kapitel II erforderlich sind" anzufertigen.

Auch ist kein Grund ersichtlich, aus dem der datenschutzrechtliche Grundsatz der Datenminimierung aus Art. 5 Abs. 1 Buchst. c DSGVO hier unanwendbar sein könnte. Schon die Vereinbarkeit der früheren Fassung des § 8 Abs. 2 GwG (2017: „vollständige Kopien dieser Dokumente oder Unterlagen anzufertigen oder sie vollständig optisch digitalisiert zu erfassen“) mit höherrangigem Recht erschien recht zweifelhaft. Denn das Gebot der Datenminimierung beziehungsweise Datensparsamkeit entspringt nicht einfachem Recht, sondern ist überzeugender Auffassung nach ein direktes Resultat des grundgesetzlichen Rechts auf informationelle Selbstbestimmung (vgl. BVerfG, Urteil vom 15. Dezember 1983 – 1 BvR 209/83).

So ist die entsprechende Begründung im Gesetzgebungsverfahren des GWG 2017 bestenfalls irreführend und vermag die 2017 eingeführte „Vollständigkeit“ von Kopien kaum zu rechtfertigen:
„§ 8 dient der Umsetzung von Artikel 40 der Vierten Geldwäscherichtlinie. Die Vorschrift entspricht im Wesentlichen § 8 des bisherigen Geldwäschegesetzes. Weil Art. 40 Abs. 1 Buchst. a der Vierten Geldwäscherichtlinie stärker als die Dritte Geldwäscherichtlinie auf Kopien abstellt, sieht Abs. 2 Satz 2 die Fertigung von vollständigen Kopien der Dokumenten und Unterlagen vor, die der Überprüfung der Identität der natürlichen oder juristischen Person dienen.“ BT-Drucksache 18/11555, Seite 114 f. = BR-Drucksache 182/17, Seite 130 f.

Die Vierte Geldwäscherichtlinie (Richtlinie (EU) 2015/849 des Europäischen Parlaments und des Rates vom 20. Mai 2015 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung, zur Änderung der Verordnung (EU) Nr. 648/2012 des Europäischen Parlaments und des Rates und zur Aufhebung der Richtlinie

2005/60/EG des Europäischen Parlaments und des Rates und der Richtlinie 2006/70/EG der Kommission) selbst sieht allerdings an keiner Stelle eine Vollständigkeit der Kopie vor, sondern gebietet vielmehr Datenminimierung: "Personenbezogene Daten sollten von den Verpflichteten nur in dem Umfang erhoben und weiterverarbeitet werden, wie dies zur Erfüllung der Anforderungen dieser Richtlinie notwendig ist" (Erwägungsgrund 43, Seite 3).

Wie die Speicherung von (in Ausweisdokumenten gespeicherten) Körpergrößen, Augenfarben, Lichtbildern oder Zugangsnummern der Bekämpfung von Geldwäsche oder der Umsetzung der Richtlinie dienen könnten, ist nicht ersichtlich. Während die Gesetzesbegründung des GWG 2017 also vorgibt, mit § 8 GWG 2017 im Wesentlichen die Vierte Geldwäsche-Richtlinie umzusetzen, verstieß das Gesetz eklatant gegen deren ausdrückliche Vorgaben und höherrangiges Recht. Die mit dem GWG 2020 umgesetzte Fünfte Geldwäsche-Richtlinie betont nochmals verstärkt die Bedeutung des datenschutzrechtlichen Verhältnismäßigkeitsprinzips (vgl. Erwägungsgrund 5, Seite 2) und generell des Datenschutzes (vgl. Erwägungsgrund 21, 38, 51). Insoweit erscheint überaus naheliegend, dass der deutsche Gesetzgeber mit der Neufassung des § 8 Abs. 2 GwG unions-, verfassungs- und datenschutzkonforme Zustände herstellen wollte.

Nach meiner Überzeugung folgt grundlegend auch aus dem Recht auf informationelle Selbstbestimmung sowie den entsprechenden unions- und menschenrechtlichen Vorgaben, dass die Erhebung und Verarbeitung von für den Gesetzeszweck nicht erforderlichen Daten zu unterbleiben hat. Dies gilt wohl unabhängig davon, dass die Vierte und Fünfte Geldwäsche-Richtlinien insoweit ausreichend konkrete Individualrechte verleihen dürften, und somit die Datenminimierung auch aus richtlinienkonformer Auslegung des Geldwäschegesetzes verpflichtend scheint.

Eine verbindliche Klärung dieser Frage durch die Gerichte erscheint wünschenswert und aktuell die einzige Möglichkeit, europa- beziehungsweise deutschlandweit einheitliche Auslegungen herbeizuführen.

2.1.6 Datenminimierung im Sozialbereich: Umfang der bei der Verwendungsnachweisprüfung der Eingliederungshilfe zu prüfenden Unterlagen

Ein Petent hatte mich gebeten zu prüfen, welche Unterlagen das Sozialamt des Landkreises aus datenschutzrechtlicher Sicht zur Prüfung des Verwendungsnachweises der Eingliederungshilfe anfordern darf.

Der Petent schilderte den Sachverhalt folgendermaßen: Er bezieht Eingliederungshilfe durch das Sozialamt und erhält dabei Leistungen in Form eines persönlichen Budgets das zur Verwendung von Unterstützungsleistungen dienen soll. In einem Vertrag zwischen dem Sozialamt

und dem Petenten wurde unter anderem auch geregelt, wie der Verwendungsnachweis zu erfolgen hat.

Bezugnehmend auf den im Vertrag festgelegten Verwendungsnachweis wandte sich der Petent an mich. Zum einen rügte er die Anforderung von personenbezogenen Daten zur Überprüfung der Verwendung der gezahlten Leistungen, zum Beispiel das Vorlegen der Kontoauszüge des Budgetkontos. Zum anderen wandte er sich gegen die Führung eines detaillierten Pflegetagebuchs. Seiner Ansicht nach sei eine Einnahme-Ausgaben-Rechnung ausreichend.

Nach meiner Einschätzung ist es erforderlich eine Gegenüberstellung von Einnahmen und Ausgaben mit den Kontoauszügen des Budgetkontos und den dazugehörigen aussagefähigen Nachweisen/Belegen für den Abrechnungszeitraum zu führen und vorzulegen. Die Vorlage der Belege ist erforderlich, um nachzuweisen, welche Einnahmen beziehungsweise Ausgaben tatsächlich angefallen sind.

Da es sich um öffentliche Mittel handelt, die in Anspruch genommen werden, sehe ich den vom Landratsamt geforderten Umfang der Verwendungsnachweise insgesamt als erforderlich an. Die darin getroffenen Festlegungen zu den Nachweisen waren aus datenschutzrechtlicher Sicht daher nicht zu beanstanden.

2.2 Rechtmäßigkeitsvoraussetzungen der Datenverarbeitung

Im vergangenen Jahr erreichte mich eine Vielzahl von Anfragen und Beschwerden zur Kontaktdatenerhebung in der Coronavirus-Pandemie. Eine Auswahl der Fälle finden Sie in den Beiträgen 2.2.1 bis 2.2.7. Daneben gab es erwähnenswerte Vorgänge zur Rechtmäßigkeit der Datenverarbeitung aus dem öffentliche Bereich (2.2.8 bis 2.2.14) und im nicht-öffentlichen Bereich (2.2.15 bis 2.2.22). Die Eingaben zur Videografie ebbten auch 2020 nicht ab. Einige Beispiele sind in 2.2.23 bis 2.2.30 aufgeführt (siehe auch 1.4, 3.1.1, 3.2.3, 4.2.1).

2.2.1 Was geschieht mit meinen personenbezogenen Daten bei einem Coronatest?

Ein Betroffener, dessen Test auf eine Erkrankung an COVID-19 positiv ausgefallen war, hat sich Ende März 2020 an mich gewandt und um Mitteilung gebeten, was mit seinen personenbezogenen Daten beziehungsweise Gesundheitsdaten, die beim Test erhoben werden, passiert. Er bat um Information, an wen diese weitergegeben werden.

Um sich auf COVID-19 testen zu lassen, ist es in der Regel erforderlich, zuerst zum Hausarzt zu gehen, da die Corona-Ambulanzen eine Überweisung des Hausarztes fordern. Mit seinem Arzt schließt der Betroffene einen Behandlungsvertrag ab. § 630 f Bürgerliches Gesetzbuch

(BGB) regelt, dass Patientenunterlagen zehn Jahre aufzubewahren sind. Dazu zählen zum Beispiel Befunde.

Bei der vom Patienten beim Coronatest entnommenen Probe handelt es sich nicht um personenbezogene Daten im Sinne des Art. 4 Abs. 1 Datenschutz-Grundverordnung (DSGVO). Erst wenn diese analysiert wird und Informationen, die den Patienten betreffen, verarbeitet werden – das Labor stellt fest, der Patient ist an COVID-19 erkrankt beziehungsweise der Verdacht hat sich nicht bestätigt – ist dieses der Fall.

Bei COVID-19 handelt es sich um eine meldepflichtige Krankheit im Sinne des § 6 Infektionsschutzgesetz (IfSG). Sollte der Arzt feststellen, dass der Patient daran erkrankt ist, hat er dies nach § 8 Abs. 1 Nr. 1 IfSG zu melden. Auch ein beauftragtes Labor hat diese Feststellung nach § 8 Abs. 1 Nr. 2 IfSG an das zuständige Gesundheitsamt zu melden.

Nach § 9 IfSG handelt es sich um eine namentliche Meldung. § 9 Abs. 1 beziehungsweise Abs. 2 IfSG führt die weiteren Punkte auf, die die Meldung umfasst, zum Beispiel Adresse und Kontaktdaten. Die Meldung hat unverzüglich an das zuständige Gesundheitsamt des Landkreises beziehungsweise der Kreisfreien Stadt zu erfolgen.

Die verarbeiteten Daten zu meldepflichtigen Daten werden gemäß § 11 IfSG von dem Gesundheitsamt, in dessen Bezirk der Patient seinen Hauptwohnsitz hat, über die zuständige Landesbehörde – in Sachsen die Landesuntersuchungsanstalt – an das Robert Koch-Institut (RKI) gemeldet. Diese Meldung erfolgt pseudonymisiert. Das heißt, das RKI kann keinen Bezug zur Person des Patienten herstellen.

Weiter teilte ich dem Betroffenen mit, dass das RKI auf seiner Internetseite rki.de unter dem Punkt „COVID-19“ Antworten auf häufig gestellte Fragen zum Coronavirus SARS-CoV-2/ Krankheit COVID-19 eingestellt hat. Auf die Antworten zu den Fragen, was alles meldepflichtig ist, wie der Meldeweg funktioniert und welche Informationen ans RKI übermittelt werden, habe ich hingewiesen.

Da das IfSG regelt, wer welche Daten zu melden hat und an wen die Meldung erfolgt, ist die Übermittlung der personenbezogenen Daten im Sinn des Art. 4 Nr. 1 DSGVO durch den Arzt beziehungsweise das Labor an das Gesundheitsamt und dann an das RKI nach Art. 6 Abs. 1 Buchst. c und e sowie Abs. 3 DSGVO rechtmäßig, da die Verarbeitung für die Erfüllung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt. Soweit es sich um die Übermittlung der Gesundheitsdaten des Patienten im Sinne des Art. 9 Abs. 1 DSGVO handelt, ist dies nach Art. 9 Abs. 2 Buchst. g und i sowie Abs. 3 DSGVO zulässig.

2.2.2 Führung von Besucherlisten an sächsischen Gerichten

Im Frühjahr 2020 erreichte mich eine Reihe von Anfragen, die die Führung von Besucherlisten bei sächsischen Gerichten zum Inhalt hatten. Im Zuge der Bemühungen um eine Eingrenzung des Infektionsgeschehens in der sich abzeichnenden Pandemie legten die Gerichte im Eingangsbereich Listen aus. Darin sollten sich Besucher des Gerichts eintragen, um eine künftig möglicherweise notwenige Kontaktnachverfolgung zu ermöglichen. Einheitliche Vorgaben seitens des Staatsministeriums der Justiz, für Demokratie, Europa und Gelichstellung (SMJusDEG) für das Vorgehen der Gerichtsverwaltungen gab es nicht.

Nachdem ich mich wegen der Betroffenheit verschiedener Gerichtsbarkeiten und Standorte an das SMJusDEG gewandt hatte, bestand zwischen unseren Häusern zügig Einigkeit darüber, dass wegen der seinerzeit fehlenden gesetzlichen Grundlage für die Erfassung und Speicherung von Besucherdaten für Zwecke des Infektionsschutzes eine Verarbeitung ausschließlich mit Einwilligung der Betroffenen erfolgen durfte (Art. 6 Abs. 1 Buchst. a DSGVO).

Eine Rechtsgrundlage für die Erfassung der Kontaktdaten von Besuchern der Gerichte fand sich weder im Infektionsschutzgesetz (IfSG) noch in der damals gültigen Sächsischen Corona-Schutz-Verordnung (SächsCoronaSchVO). Auf das gewohnheitsrechtlich verankerte Hausrecht konnten die Präsidenten und Direktoren der Gerichte die Erhebung und Speicherung der Daten ebenfalls nicht stützen, da ein solcher Eingriff in das Grundrecht auf informationelle Selbstbestimmung – jedenfalls für „hausrechtfremde“ Zwecke wie dem Infektionsschutz – einer normenklaren gesetzlichen Grundlage bedarf und nicht in Ausübung lediglich gewohnheitsrechtlicher Befugnisse erfolgen kann (Art. 6 Abs. 3 DSGVO; Bundesverfassungsgerichtsentscheidung 65, 1, Rdnr. 151; Art. 33 Verfassung des Freistaates Sachsen).

In der Folge unseres Austauschs stimmte das Staatsministerium mit den Präsidenten der sächsischen Obergerichte sowie dem Generalstaatsanwalt des Freistaates Sachsen „Handlungsempfehlungen für die Gerichte und Staatsanwaltschaften des Freistaates Sachsen für die Dauer der Pandemie des Coronavirus (SARS-CoV-2)“ ab. Danach sollten Besucherinnen und Besucher von Gerichten und Staatsanwaltschaften im Rahmen der Zugangskontrolle beim Betreten des Gebäudes gebeten werden, die Besucherkarten auszufüllen. Die Besucherkarten sollten tagesweise – jedenfalls aber unter Verschluss – gesammelt und nach drei Wochen vernichtet werden. Den Besucher sollten bei der Zugangskontrolle zugleich in geeigneter Weise die Hinweise erteilt werden, dass die Erfassung ihrer Daten dazu dient, bei bekanntwerdenden Infektionen mögliche Kontaktpersonen informieren zu können, diese Daten ausschließlich im Fall einer auftretenden Infektion verwendet und nach drei Wochen vernichtet werden sowie, dass ihre Angaben freiwillig seien.

Ende des Jahres erfolgte eine Änderung der Rechtslage. Mit Inkrafttreten der am 11. Dezember 2020 beschlossenen Sächsischen Corona-Schutz-Verordnung unterlagen ausdrücklich

auch Behörden und Gerichte der Rechtspflicht (Art. 6 Abs. 1 Buchst. c DSGVO), Name, Telefonnummer oder E-Mail-Adresse und Postleitzahl der Besucher sowie Zeitraum und Ort des Besuchs zu erfassen und zeitlich befristet ausschließlich für Zwecke der Kontaktnachverfolgung, das heißt eine etwaige Anforderung durch das Gesundheitsamt aufzubewahren. Mit der damit geschaffenen gesetzlichen Grundlage – § 5 Abs. 6 SächsCoronaSchVO vom 11. Dezember 2020 in Verbindung mit § 32 Satz 1 in Verbindung mit § 28 Abs. 1 Satz 1 und 2 sowie mit § 28a Abs. 1, Abs. 2 Satz 1 und Abs. 3 IfSG – war eine Erhebung von Besucherdaten durch Gerichte auch ohne der Einwilligung der Betroffenen zulässig, genauer: verpflichtend. Für potenzielle Besucher, die eine Erfassung ihrer Daten zum Zweck der Kontaktnachverfolgung vermeiden wollten, blieb die Option, auf ihren Besuch des Gerichts zu verzichten.

Vergleiche auch Beitrag 2.2.3 zu Besucherlisten im Rathaus.

2.2.3 Corona-Erfassungsbogen im Rathaus

Ein Stadtrat wandte sich an mich wegen eines Erfassungsbogens für Besuche im Rathaus. In diesem sollte eidesstattlich erklärt werden, dass man sich in den zurückliegenden 14 Tagen in keinem vom Robert Koch-Institut benannten Corona-Risikogebiet aufgehalten habe, zu keinem nachweislich mit dem Virus infizierten Kontakt hatte und sich insgesamt gesund fühle.

Ich forderte die Stadtverwaltung zur kurzfristigen Stellungnahme auf. Dabei wies ich darauf hin, dass ich nicht das Erfordernis einer Versicherung an Eides statt nach § 294 Zivilprozessordnung sehe. Weiterhin konnte ich dem verwendeten Formular keine Informationen nach Art. 13 Datenschutz-Grundverordnung (DSGVO), wie beispielsweise der Aufbewahrungsdauer, entnehmen. Zudem wurde auch nicht darauf hingewiesen, ob die Angaben verpflichtend (auf welcher Rechtsgrundlage?) oder freiwillig sind. Sollte letzteres der Fall sein, wovon ich zunächst ausgehe, hätte die Einwilligung nicht den Anforderungen von Art. 7 DSGVO genügt.

Der benannte städtische Datenschutzbeauftragte teilte mir daraufhin mit, dass meine Bedenken geteilt würden. Gegen den überarbeiteten und übersandten Erfassungsbogen bestanden keine datenschutzrechtlichen Bedenken.

Vergleiche auch 2.2.2 zu Besucherlisten im Gericht.

2.2.4 Kontaktdatenerhebung bei Friseurbesuchen in der Coronavirus-Pandemie

Bereits Ende April 2020 erhielt ich die Anfrage einer Kundin, die wissen wollte, ob es rechtmäßig sei, dass bei einem Friseurbesuch die Kontaktdaten des jeweiligen Kunden erhoben und gegebenenfalls auch an Behörden weitergeleitet werden würde.

Mit der Allgemeinverfügung zum Vollzug des Infektionsschutzgesetzes des Sächsischen Staatsministeriums für Soziales und Gesellschaftlichen Zusammenhalt vom 22. März 2020 wurden anlässlich der Coronavirus-Pandemie erstmals Ausgangsbeschränkungen in Sachsen verhängt (erster Lockdown). Damit gingen drastische Einschränkungen von Grundrechten und die weitgehende Stilllegung des öffentlichen Lebens, insbesondere auch die Schließung von Friseurgeschäften und Restaurants, einher.

Am 31. März 2020 trat dann die erste Sächsische Corona-Schutz-Verordnung (SächsCoronaSchVO) in Kraft, die diese Beschränkungen auf Verordnungsbasis regelte. Die SächsCoronaSchVO vom 30. April 2020 sah zunächst die Öffnung bestimmter gewerblicher Einrichtungen unter der Voraussetzung der Kontaktdatenerhebung von Kunden und Besuchern vor.

Der Kundin teilte ich mit, dass nach § 9 Abs. 2 SächsCoronaSchVO, Stand 30. April 2020, die Friseure ab 4. Mai 2020 Friseurdienstleistungen unter den Voraussetzungen der Einhaltung der SARS-CoV-2-Arbeitsschutzstandards des Bundesministeriums für Arbeit und Soziales und vorliegender branchenspezifischer Umsetzung sowie der vom Ministerium für Soziales und Gesellschaftlichen Zusammenhalt durch Allgemeinverfügung festgelegten Hygienevorschriften erbringen dürfen. Entsprechend Punkt II Ziff. 12 (Zutritt betriebsfremder Personen zu Arbeitsstätten und Betriebsgelände) des SARS-CoV-2-Arbeitsschutzstandards des Bundesministeriums für Arbeit und Soziales sind die Kundenkontaktdaten möglichst zu dokumentieren. Auch die Berufsgenossenschaft für das Friseurhandwerk hat in seinen SARS-CoV-2-Arbeitsschutzstandards, Stand 30. April 2020, festgelegt, dass diese Maßnahme der Dokumentation der Kundenkontaktdaten in das betriebliche Maßnahmenkonzept des Arbeitsschutzes aufzunehmen ist. Hintergrund dieser Kontaktdatenerhebung ist, dass das Friseurhandwerk zu den Berufsgruppen gehört, bei denen aufgrund des direkten Kundenkontaktes ein erhöhtes Infektionsrisiko besteht, da insbesondere der Mindestabstand von 1,5 Metern nicht sicher eingehalten werden kann. Ziel soll die Rückverfolgung von Infektionsketten, zum Beispiel bei einer Infektion eines Mitarbeiters im Friseursalon, sein. Mit dieser Maßnahme sollen dann die Infektionsketten unterbrochen und damit auch weitere Infektionen vermieden werden. Ziel dieser Kontaktdatenerhebung ist der Gesundheitsschutz der Bevölkerung sowie der Beschäftigten. Diese Datenverarbeitung ist durch § 32 Satz 1 in Verbindung mit § 28 Abs. 1 Satz 1 und 2 Infektionsschutzgesetz, § 10 Abs. 2 SächsCoronaSchVO in Verbindung mit Art. 6 Abs. 1 Buchst. c und f Datenschutz-Grundverordnung gerechtfertigt.

Auch in anderen Bereichen, wie zum Beispiel im Gaststätten- und Hotelgewerbe, wurde die Kontaktdatenerhebung für Kunden und Besucher durch die jeweils geltende Sächsische Corona-Schutz-Verordnung eingeführt. Aufgrund der Vielzahl von Anfragen und Beschwerden zur Rechtmäßigkeit der Kontaktdatenerhebung, insbesondere welche Daten für welchen Zweck erhoben und verwendet werden dürfen, wie diese Daten erfasst werden dürfen, wie lange sie gespeichert werden dürfen und vieles mehr, habe ich auf meiner Website eine „Handreichung – Datenschutzrechtliche Aspekte der Erhebung von Kontaktdaten von Kunden und

Besuchern während der Corona-Pandemie“ sowie entsprechende Musterformulare veröffentlicht. Diese werden der jeweils geltenden Verordnung angepasst beziehungsweise laufend aktualisiert.

2.2.5 Weitergabe von personenbezogenen Daten beziehungsweise Gesundheitsdaten durch die Gesundheitsämter an die Polizei

Im Zusammenhang mit der Coronavirus-Pandemie erreichten mich verschiedene Anfragen, unter welchen Bedingungen eine Übermittlung von personenbezogenen Daten zulässig ist. In einigen Fällen ging es um die Weitergabe der Daten positiv Getesteter von den Gesundheitsämtern an die Polizei.

Eine Erhebung von Gesundheitsdaten durch den Polizeivollzugsdienst beziehungsweise durch die Rettungsleitstelle bei den zuständigen Gesundheitsämtern und die Übermittlung der erforderlichen Daten an den Polizeivollzugsdienst/die Rettungsleitstelle sehe ich im Einzelfall als zulässig an, soweit Anhaltspunkte für eine konkrete Gefahr vorliegen.

Dies begründe ich wie folgt:

Nach § 7 Abs. 1 Satz 3 Gesetz über den öffentlichen Gesundheitsdienst im Freistaat Sachsen (SächsGDG) in Verbindung mit § 6 Abs. 2 Satz 2 SächsGDG kommt eine Übermittlung von Gesundheitsdaten durch die Gesundheitsämter der Landkreise und Kreisfreien Städte an andere Stellen, wie zum Beispiel den Polizeivollzugsdienst, nur in Betracht, wenn das zur Abwehr einer Gefahr für Leben oder Gesundheit Dritter erforderlich ist. Der Betroffene soll hierauf hingewiesen werden. Eine Übermittlung von Infektionsdaten durch die Gesundheitsämter an den Polizeivollzugsdienst ist insoweit zulässig. Voraussetzung ist das Vorliegen einer (konkreten) Gefahr für Leben oder Gesundheit Dritter sowie die Geeignetheit und Erforderlichkeit der Datenübermittlung zur Gefahrenabwehr.

Dem SächsGDG ist jedoch keine Rechtsgrundlage für eine vorsorgliche (präventive), anlassunabhängige Übermittlung sensibler Gesundheitsdaten an die Rettungsleitstelle beziehungsweise den Polizeivollzugsdienst zu entnehmen. Ebenso verhält es sich bei den Regelungen des Infektionsschutzgesetzes (IfSG). Die Übermittlung der sensiblen Gesundheitsdaten ist in diesen Fällen damit auch datenschutzrechtlich unzulässig. Ein genereller Zugriff der Rettungsleitstelle oder des Polizeivollzugsdienstes auf Daten des Gesundheitsamts zu an Corona erkrankten Personen, die zum Beispiel in einer Datenbank abgespeichert sind, ist damit ebenfalls nicht zulässig.

Gegebenenfalls kann im Einzelfall vor dem konkreten Einsatz eine Nachfrage beim Gesundheitsamt durch die Rettungsleitstelle oder die Polizei zur Eigensicherung der Rettungskräfte beziehungsweise der Polizei zulässig sein.

Eine pauschale Übermittlung von Daten insbesondere von sensiblen Gesundheitsdaten durch die Gesundheitsämter an die Rettungsleitstelle oder den Polizeivollzugsdienst ist hingegen nicht zulässig.

2.2.6 Atteste zur Befreiung von der Pflicht zum Tragen einer Mund-Nasenbedeckung in Schulen

Mich erreichten zahlreiche Anfragen von Eltern, denen zum Teil von Schulleitern sogar angedroht wurde, ihren Kindern den Zutritt zum Schulgebäude zu verwehren. Hintergrund waren die Atteste zur Befreiung von der Pflicht zum Tragen einer Mund-Nasenbedeckung. Zum einen wurde gefordert, dass diese eine Begründung enthalten müssen, zum anderen wollte man die Atteste jedenfalls in Kopie in der Schule aufbewahren.

Keine Fassung der Sächsischen Corona-Schutz-Verordnung enthielt Anforderungen an den Inhalt eines ärztlichen Attests. Dementsprechend führte das Sächsische Staatsministerium für Soziales und Gesellschaftlichen Zusammenhalt (SMS) von Anfang an im Internet aus: „Zur Glaubhaftmachung genügt die Vorlage eines ärztlichen Attests. Eine gesonderte Begründung der Ärztin beziehungsweise des Arztes ist dabei nicht erforderlich."

Dessen ungeachtet hat die Sächsische Landesärztekammer, die gemäß § 37 Abs. 1 des Sächsischen Heilberufekammergesetzes der Aufsicht des SMS unterliegt, in einer Pressemitteilung vom 9. November 2020 …

„aktuell die inhaltlichen Vorgaben an ein wirksames ärztliches Attest zusammengefasst. Um zum Beispiel eine sachgerechte Entscheidung über die Befreiung von der sog. Maskenpflicht aus medizinischen Gründen zu ermöglichen, muss das ärztliche Attest gewissen Mindestanforderungen genügen (Oberverwaltungsgericht Nordrhein-Westfalen, Beschluss vom 24. September 2020 - 13 B 1368/20). […] Neben dem vollständigen Namen und des Geburtsdatums muss sich aus dem Attest deshalb nachvollziehbar ergeben, welche konkret zu benennenden gesundheitlichen Beeinträchtigungen auf Grund einer Mund-Nasen-Bedeckung zu erwarten sind und woraus diese im Einzelnen resultieren. Soweit relevante Vorerkrankungen vorliegen, sind diese konkret zu bezeichnen. Darüber hin-aus muss im Regelfall erkennbar werden, auf welcher Grundlage der attestierende Arzt zu seiner Einschätzung gelangt ist."

Das SMS nahm dies vermutlich zum Anlass, in der Begründung zur Fassung der Sächsischen Corona-Schutz-Verordnung vom 11. Dezember 2020 schließlich (völlig zutreffend) auszuführen:

„[…] stellt darüber hinaus klar, dass zum Nachweis der Befreiung von der Tragepflicht die Vorlage eines ärztlichen Attests, das von einer approbierten Ärztin beziehungsweise einem

approbierten Arzt ausgestellt worden ist, genügt. Eine gesonderte Begründung der Ärztin beziehungsweise des Arztes ist dabei aus datenschutzrechtlichen Gründen nicht erforderlich. Dem Betroffenen kann nicht zugemutet werden, fremden Personen die Diagnose zu offenbaren, zumal es sich bei diesen Personen nicht um medizinisch geschultes Personal handelt."

Mir ist nicht bekannt, dass das SMS vorliegend von seinen Aufsichtsrechten gegenüber der Sächsischen Landesärztekammer Gebrauch gemacht hat. Die Presseerklärung war zum Ende des Berichtszeitraums weiterhin und unkommentiert auf slaek.de abrufbar.

Hinsichtlich der Zulässigkeit einer Kopie des Attests enthielt die Sächsische Corona-Schutz-Verordnung vom 29. September 2020 in § 2 Abs. 7 folgende Formulierung: „Zur Glaubhaftmachung einer Befreiung von der Pflicht nach Satz 1 genügt die Vorlage eines Schwerbehindertenausweises oder ärztlichen Attests."

Dies schien für etliche Schulleiter nicht verständlich genug zu sein. Ich wandte mich daher an das Sächsische Staatsministerium für Kultus (SMK) mit der Bitte tätig zu werden.

Zwischenzeitlich machte es die Fassung der Sächsischen Corona-Schutz-Verordnung vom 21. Oktober 2020 noch klarer: „Zur Glaubhaftmachung einer Befreiung von der Pflicht nach Satz 1 genügt die Gewährung der Einsichtnahme in einen Schwerbehindertenausweis oder in ein ärztliches Attest."

So teilte dann auch das SMK in einem Schulleiterbrief vom 30. Oktober 2020 mit:

„Das Kopieren von Attesten, mit denen Schülerinnen oder Schüler vom Tragen einer Mund-Nasenbedeckung befreit werden, ist nicht zulässig. Ebenso ist es nicht zulässig, diese Atteste zur Schülerakte zu nehmen. Darauf hat der Sächsische Daten-schutzbeauftrage hingewiesen. Für die jeweilige Schülerin beziehungsweise für den jeweiligen Schüler sollte jedoch vermerkt werden, dass ein entsprechendes Attest vorgelegt wurde."

Eine völlige Kehrtwende nahm das SMS schließlich mit der Fassung der Sächsischen Corona-Schutz-Verordnung vom 27. November 2020 vor. Dort war nunmehr in § 3 Abs. 3 geregelt: „Schulen und Einrichtungen der Kindertagesbetreuung sind befugt, das ärztliche Attest, mit dem eine Befreiung von der Pflicht nach Absatz 1 glaubhaft gemacht wird, in analoger oder digitaler Kopie oder mit Zustimmung des Vorlegenden im Original aufzubewahren."

Dies war datenschutzrechtlich nach meiner Auffassung auch noch zulässig, da ergänzend geregelt wurde, dass die Kopie oder das Attest vor unbefugtem Zugriff zu sichern ist und nach Ablauf des Zeitraumes, für welchen das Attest gilt, unverzüglich zu löschen oder zu vernichten ist, spätestens jedoch mit Ablauf des Jahres 2021.

Nicht geregelt war jedoch das Verhältnis zwischen der weiterhin bestehenden generellen Beschränkung auf Gewährung der Einsichtnahme und der Befugnis für Schulen, Kopien zu erstellen. Die Begründung der Fassung der Sächsischen Corona-Schutz-Verordnung vom 11. Dezember 2020 führt dazu (bei allerdings insofern unverändertem Wortlaut des nunmehrigen § 3 Abs. 4) aus: „Klarstellend ist nunmehr auch geregelt, dass die Schule oder Einrichtung der Kindertagesbetreuung eine Kopie des Attests fertigen darf; der Vorlegende hat dies also zu ermöglichen und zu dulden."

2.2.7 Gesundheitsbestätigungen für Schulbesuch

Im Frühjahr 2020 wendeten sich zahlreiche Eltern an mich. Es ging um die durch sie auszufüllenden Gesundheitsbestätigungen. Diese waren täglich vorzuzeigen und gehörten zum Öffnungskonzept von Kitas und Grundschulen mit festen, voneinander getrennten Gruppen. Kinder duften nur dann am Unterricht teilnehmen, wenn weder sie selbst noch Mitglieder des Hausstandes Symptome der Krankheit Covid-19 aufwiesen. Dies mussten Eltern täglich per Unterschrift bescheinigen. Das Sächsische Staatsministerium für Kultus (SMK) stellte dazu in der Presse klar, dass damit keinerlei Haftung verbunden ist. Hiergegen habe ich keine datenschutzrechtlichen Bedenken gehabt; dies sah die Rechtsprechung letztinstanzlich ebenso.

Unzulässig war aber die von einigen Schulen praktizierte Aufbewahrung dieser Monatsbögen, wie mir auch das SMK auf Anfrage bestätigte. Zum Teil wurden diese von den Schulen zu Unterrichtsbeginn eingesammelt und nach Unterrichtsende wieder verteilt, zum Teil nach Ablauf des jeweiligen Monats auch dauerhaft eingesammelt. Sämtliche Schulleiter haben jedoch nach meinen Anschreiben die Datenschutzverstöße abgestellt und bereits eingesammelte Gesundheitsbestätigungen wieder herausgegeben.

2.2.8 Überprüfung eines bevollmächtigten Bezirksschornsteinfegers

Ein bevollmächtigter Bezirksschornsteinfeger beschwerte sich bei mir über das für ihn zuständige Landratsamt. Dieses habe Eigentümern, in deren Anwesen eine Feuerstättenschau durch den Beschwerdeführer erfolgte, im Nachgang schriftlich um die Beantwortung einer Reihe von Fragen zur Zufriedenheit mit seiner Tätigkeit gebeten. Dies umfasste unter anderem die Frage, ob die Feuerstättenschau persönlich durchgeführt wurde.

Das von mir um Stellungnahme gebetene Landratsamt teilte mir zunächst mit, dass der bevollmächtigte Bezirksschornsteinfeger selbst in einem Schreiben gefordert hat: „Wenn mir nicht geglaubt wird, schreiben Sie doch zu meiner Entlastung einige der Liegenschaften an wo ich war."

Unabhängig davon erfolgte die Versendung der in Rede stehenden Fragebögen in Wahrnehmung der Aufsichtspflichten nach § 21 Abs. 1 Schornsteinfeger-Handwerksgesetz

(SchfHwG). Demnach kann die zuständige Behörde die bevollmächtigten Bezirksschornsteinfeger hinsichtlich der Wahrnehmung der ihnen übertragenen Aufgaben und Befugnisse und der Einhaltung ihrer Pflichten jederzeit überprüfen. Zu diesen sogenannten Berufspflichten gehört unter anderem auch die persönliche Durchführung der Feuerstättenschau durch den bevollmächtigten Bezirksschornsteinfeger (§ 14 SchfHwG). Einen Datenschutzverstoß konnte ich daher nicht erkennen.

2.2.9 Nachweis ausreichender Impfschutz gegen Masern

Das Inkrafttreten des Masernschutzgesetzes zum 1. März 2020 hatte zahlreiche Beschwerden und Anfragen bei meiner Dienststelle zur Folge. Diese betrafen zum einen die Verfahrensweise mit den Nachweisen eines ausreichenden Impfschutzes gegen Masern und zum anderen die Frage, wann eine Benachrichtigung des Gesundheitsamts zu erfolgen hat.

Mehrere Eltern rügten in ihren Beschwerden, dass durch die Leitung der Kindertagesstätte beziehungsweise des Kindergartens die Nachweise des ausreichenden Impfschutzes gegen Masern ihres Kindes kopiert wurden, um einen Beleg zu den Akten zu nehmen.

Das Masernschutzgesetz änderte unter anderem das Infektionsschutzgesetz (IfSG). Dieses legt in § 20 Abs. 8 Nr. 1 fest, dass Personen, die in Gemeinschaftseinrichtungen nach § 33 Abs. 1 Nr. 1 bis 3 betreut werden oder tätig sind, einen ausreichenden Impfschutz gegen Masern aufweisen müssen. Dazu gehören nach Nummer 1 Kindertageseinrichtungen und Kinderhorte sowie nach Nummer 3 Schulen und sonstige Ausbildungseinrichtungen.

Der Nachweis erfolgt nach § 20 Abs. 9 Satz 1 IfSG gegenüber der Leitung der Einrichtung durch Vorlage einer Impfdokumentation oder eines ärztlichen Zeugnisses über die Immunität gegen Masern oder ein ärztliches Attest über das Vorliegen einer medizinischen Kontraindikation oder der Bestätigung einer staatlichen Stelle, dass der Nachweis bereits vorgelegen hat.

Es genügt zum Beispiel, wenn die Eltern des zu betreuenden Kindes das ärztliche Attest vorlegen. Nach meiner Auffassung dürfen der Impfausweis und auch ein ärztliches Attest aus datenschutzrechtlichen Gründen nicht kopiert und zu den Akten genommen werden, da diese andere als die gesetzlich geforderten Daten enthalten – Grundsatz der Datenminimierung. Die Leitung der Einrichtung kann zum Beispiel durch einen Vermerk dokumentieren, dass der Nachweis vorgelegt wurde. Die Dokumentation sollte sich auf die notwendigen Angaben beschränken.

Den Träger der Einrichtung, hier die Gemeindeverwaltung, habe ich um Stellungnahme zu der Beschwerde gebeten. Dabei habe ich diesen über die Rechtslage informiert und gebeten, die Leitung der Einrichtung entsprechend zu informieren. Sollte es zutreffen, dass Kopien der

Nachweise gefertigt wurden, sind diese durch einen Vermerk zu ersetzen und anschließend zu vernichten. In diesem Falle war mir die Vernichtung der Nachweise zu bestätigen.

Etliche Anfragen der Eltern richteten sich auch darauf, wann durch die Leitung der Einrichtung Informationen an das zuständige Gesundheitsamt des Landratsamtes beziehungsweise der Kreisfreien Stadt weiterzuleiten sind, die personenbezogene Daten enthalten.

Ist dem ärztlichen Zeugnis zu entnehmen, dass es sich um eine dauerhafte medizinische Kontraindikation handelt, wird der Nachweis durch dessen Vorlage nach § 20 Abs. 9 Satz 1 IfSG erbracht.

Eine unverzügliche Benachrichtigung des Gesundheitsamtes und Übermittlung personenbezogener Daten ist nach § 20 Abs. 9 Satz 4 IfSG in zwei Fällen vorgesehen: Wenn der Nachweis nach Satz 1 nicht vorgelegt wird oder wenn sich ergibt, dass ein Impfschutz gegen Masern erst zu einem späteren Zeitpunkt möglich ist oder vervollständigt werden kann. Nach § 20 Abs. 9 Satz 4 IfSG ist das Gesundheitsamt, in dessen Bezirk sich die Einrichtung befindet, unverzüglich zu benachrichtigen und dem Gesundheitsamt personenbezogene Angaben zu übermitteln.

2.2.10 Einsatz elektronischer Wasserzähler

In meinem Tätigkeitsbericht vom 1. April 2017 bis zum 31. Dezember 2018 hatte ich mich unter 2.2.6 (Seite 175) bereits zur Zulässigkeit der Datenverarbeitung mittels elektronischer Wasserzähler geäußert. Damals musste ich leider berichten, dass das Sächsische Staatsministerium des Innern nicht tätig werden wollte, da sich nur schwer einschätzen ließe, „welche konkrete Bedeutung der geschilderte Sachverhalt vor Ort hat“.

Das hat sich erfreulicherweise geändert. Nach einer Abstimmung mit meiner Behörde wurde ein detailliertes Rundschreiben über die Landesdirektion Sachsen an alle kommunalen Aufgabenträger der Wasserversorgung (Gemeinden und Zweckverbände) versandt.

In dem Dokument wird ausgeführt, dass es gegebenenfalls notwendig ist, dass ein kommunaler Aufgabenträger im Rahmen seiner Zuständigkeit für die Aufgabe der Trinkwasserversorgung in seiner kommunalen (Wasserversorgungs-)Satzung festlegt, dass er elektronische Wasserzähler einsetzt beziehungsweise diese mit einem Funkmodul ausstattet. Es wird zutreffend darauf hingewiesen, dass für den Einsatz von elektronischen Wasserzählern im Rahmen der öffentlichen Trinkwasserversorgung weder die Verordnung über Allgemeine Bedingungen für die Versorgung mit Wasser (AVBWasserV) noch fachlich in Betracht kommende Landesgesetze, wie etwa das Sächsische Wassergesetz, bereichsspezifische Regelungen vorsehen, die den Anforderungen von Art. 6 Abs. 2 und 3 Datenschutz-Grundverordnung (DSGVO) entsprechen würden.

In einer solchen Satzung sollte insbesondere Näheres zu den Betroffenenrechten gemäß Art. 12 bis 17 DSGVO geregelt werden, beispielsweise Informationspflichten, Auskunftsrechte, Recht auf Berichtigung und Löschung der Daten, Widerspruchsrecht. Im Falle des Einsatzes von Funkmodulen ist das in Art. 5 Abs. 1 Buchst. c DSGVO normierte Prinzip der Datensparsamkeit (oder Gebot der Datenminimierung) zu beachten. Je nach eingesetzter Technik können etwa Regelungen zu den zeitlichen Intervallen geboten sein, in denen ein Funkmodul Daten an den Wasserversorger übertragen soll.

2.2.11 Luftaufnahmen von Grundstücken durch die öffentliche Hand beziehungsweise deren Beauftragte

Verschiedentlich haben mich im Berichtszeitraum Beschwerden und Anfragen erreicht, die die Anfertigung und Nutzung von Luftbildern zum Gegenstand hatten. Zweck derartiger Aufnahmen war in diesen Fällen die Bestimmung versiegelter Flächen zur Bestimmung der Abwassergebührenpflicht und die Bestimmung von Grünflächen zur Prüfung einer Teilbefreiung von Abfallgebühren (Biotonnenpflicht).

Fotografische Aufzeichnungen wie Luftaufnahmen stellen zwar regelmäßig personenbezogene Daten dar, wenn Personen oder persönliche Identifikatoren wie Kfz-Kennzeichen erkennbar sind; eine derartige feine Auflösung konnte jedoch in den konkreten Fällen ausgeschlossen werden. Entscheidend ist insoweit die Granularität („Pixelauflösung“) der angefertigten Aufnahmen.

Die Identifizierbarkeit einzelner Grundstücke oder Häuser machen die Aufnahmen in Bezug auf Eigentümer und Pächter beziehungsweise Mieter personenbezogen, soweit der Verantwortliche die rechtliche Möglichkeit besitzt, die betroffenen Flurgrundstücke einem Eigentümer beziehungsweise Mieter oder Pächter zuzuordnen.

Bereits zurückliegend hatte ich mich mit den datenschutzrechtliche Voraussetzungen und Rahmenbedingungen für derartige Überfliegungen auseinanderzusetzen (vgl. 18. Tätigkeitsbericht für den öffentlichen Bereich (04/2015 bis 03/2017), 5.5.5., Seite 57 ff.). Materiellrechtliche Voraussetzungen haben sich im Wesentlichen nicht geändert. Derartige Aufnahmen können nach Art. 6 Abs. 1 Buchst. c Datenschutz-Grundverordnung in Verbindung bestehendem (Satzungs-)Recht zur Erfüllung rechtlicher Verpflichtungen gerechtfertigt sein. Konkret bildeten in den Verfahren des Berichtszeitraums insbesondere die hoheitliche Pflicht zur Gebührengerechtigkeit, die abfallrechtlichen beziehungsweise (ab-)wasserrechtlichen Betretungsrechte und die dezentral geregelten Befugnisse für die Überprüfung der Angaben den Hintergrund. Dabei ist unschädlich, wenn der konkret Verantwortliche als Beliehener oder Verwaltungshelfer handelt, bestehende Datenbanken nutzt oder einen Auftragsverarbeiter einschaltet, solange die entsprechenden Voraussetzungen erfüllt sind. Die Datenerfassung mittels Luftaufnahmen diente der möglichst kostengünstigen Datenerfassung

beziehungsweise Überprüfung von Angaben. Diese erfolgte im Interesse einer möglichst sachgerechten Umlegung der für die Abfall- beziehungsweise Abwasserentsorgung anfallenden Gesamtkosten. Demgegenüber sind Grundstückseigentümer und andere – bei entsprechender Granularität der Aufnahmen – nur punktuell in ihrer Sozialsphäre berührt.

Den konkreten Verfahren im Berichtszeitraum lagen teils die Nutzung der Geodatenportale des entsprechenden Landkreises beziehungsweise des Freistaats, teils die Nutzung eigens angefertigter Luftaufnahmen zugrunde. In allen diesen Fällen waren die Voraussetzungen rechtmäßiger Datenverarbeitung erfüllt. Insoweit ist erfreulich, dass – soweit ersichtlich – die durch meine Behörde 2017 erarbeiteten Rahmenbedingungen auch in der Fläche eingehalten werden.

2.2.12 Nutzung von Melderegisterdaten durch Ortsvorsteher

Ein Ortsvorsteher bat mich für folgende Pläne um eine datenschutzrechtliche Prüfung: Er beabsichtigte, alle in den Jahren 2019 und 2020 neu zugezogenen Einwohner einzuladen. Dazu sollten auch diejenigen gehören, welche Grundstücke gekauft haben, um ein Wohnhaus zu errichten. Ziel war es, mit den Einwohnern ins Gespräch zu kommen sowie Hilfe und Unterstützung anzubieten. Auch seien die Freiwillige Feuerwehr, Vereine und Gruppen bemüht, neue Mitglieder zu gewinnen.

Hierfür wandte sich der Ortsvorsteher an die Gemeindeverwaltung, die einen entsprechenden Abgleich mit den Einwohnermeldedaten vornehmen sollte. Er bat außerdem, die betreffenden Einwohner anzuschreiben und einzuladen. Dies wurde jedoch zutreffenderweise abgelehnt.

Auch wenn das Anliegen – neue Einwohner auf diese Art und Weise in die Dorfgemeinschaft zu integrieren – nachvollziehbar ist, müssen die gesetzlichen Rahmenbedingungen eingehalten werden.

Gemäß § 37 Abs. 1 Bundesmeldegesetz (BMG) dürfen innerhalb der Verwaltungseinheit, der die Meldebehörde angehört, unter den in § 34 Abs. 1 BMG genannten Voraussetzungen Meldedaten weitergegeben werden. Zu diesen Voraussetzungen von § 34 Abs. 1 BMG gehört, dass dies zur Erfüllung der in ihrer Zuständigkeit oder in der Zuständigkeit des Empfängers liegenden öffentlichen Aufgaben erforderlich ist.

Dies konnte ich bei der vorgesehenen Information von neuen Einwohnern nicht erkennen. Darüber hinaus dürfen gemäß § 50 Abs. 2 BMG Mandatsträgern die dort genannten Jubiläumsdaten zur Verfügung gestellt werden. Von weiteren Regelungen hat der Gesetzgeber abgesehen.

Ich habe daher empfohlen, die entsprechende Information künftig bei der Anmeldung zur Verfügung zu stellen. Auch das Verteilen entsprechender Informationen an alle Einwohner ohne Nutzung des Melderegisters wäre natürlich denkbar.

2.2.13 Nachbarbeteiligung bei Bauvorhaben

Eine Petentin fragte an, ob sämtliche Bauunterlagen, also insbesondere auch die Grundrisse und die Größenangaben der einzelnen Räume des geplanten Hauses, ihren Nachbarn zur Einsichtnahme vorgelegt werden müssten.

Zunächst ist hierbei § 70 Sächsische Bauordnung zu beachten. Ergänzend dazu gilt die Verwaltungsvorschrift des Sächsischen Staatsministeriums des Innern zur Sächsischen Bauordnung. Dort ist unter Ziffer 70 im Einzelnen die Beteiligung der Nachbarn geregelt.

Nach Ziffer 70.2.2 ist dabei festgelegt, dass die Nachbarbeteiligung durch die Bauaufsichtsbehörde erfolgt, soweit sie nicht bereits durch den Bauherrn erfolgt ist. Den Nachbarn sind aus Gründen des Datenschutzes nur die Bauvorlagen zur Kenntnis zu geben, die für die Beurteilung ihrer Betroffenheit erforderlich sind.

Der Umfang der vorzulegenden Unterlagen kann daher nur anhand des jeweiligen Einzelfalls festgelegt werden.

2.2.14 Offenlegung von Pfändungs- und Einziehungsverfügungen gegenüber Dritten

Wegen des Versands von Pfändungs- und Einziehungsverfügungen seitens einer Kommune an die Mieter seines Wohnhauses und der damit verbundenen Offenlegung seiner Daten wandte sich ein Petent an mich. Ich nahm zu diesem Vorgang wie folgt Stellung:

Die Pfändungs- und Einziehungsverfügung ist in Deutschland eine Maßnahme der Zwangsvollstreckung. Die Pfändungs- und Einziehungsverfügung wird von der zuständigen Vollstreckungsbehörde selbst erlassen. Dies war hier die Kämmerei (Stadtkasse). Einkünfte aus Vermietung sind, sofern sie nicht dem Pfändungsschutz unterliegen, grundsätzlich uneingeschränkt durch Gläubiger im Wege einer Forderungsvollstreckung pfändbar. Der Mieter ist hierbei sogenannter Drittschuldner. Die Pfändungs- und Einziehungsverfügung wird mit der Zustellung an den Drittschuldner wirksam (siehe § 309 Abs. 2 Abgabenordnung). Ab diesem Moment muss er die Pfändung beachten. Aus diesem Grund ist dem Drittschuldner, hier also den Mietern des Wohn- und Geschäftshauses, die betreffende Verfügung auch zur Kenntnis zu geben.

Ob die Pfändungs- und Einziehungsverfügung rechtmäßig ergangen ist, also die geltend gemachten Forderungen der Kommune gegen den Petenten tatsächlich bestanden, ist in der Sache keine datenschutzrechtliche Frage, so dass dies meiner Überprüfung entzogen war.

2.2.15 Adressangabe des Lebensmittelherstellers

Ein Imker wandte sich mich wegen der Offenlegung seiner Kontaktdaten auf Honiggläsern an mich.

Nach der VERORDNUNG (EU) Nr. 1169/2011 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 25. Oktober 2011 betreffend die Information der Verbraucher über Lebensmittel und zur Änderung der Verordnungen (EG) Nr. 1924/2006 und (EG) Nr. 1925/2006 des Europäischen Parlaments und des Rates und zur Aufhebung der Richtlinie 87/250/EWG der Kommission, der Richtlinie 90/496/EWG des Rates, der Richtlinie 1999/10/EG der Kommission, der Richtlinie 2000/13/EG des Europäischen Parlaments und des Rates, der Richtlinien 2002/67/EG und 2008/5/EG der Kommission und der Verordnung (EG) Nr. 608/2004 der Kommission sind in Artikel 8 die Verantwortlichkeiten dementsprechend geregelt, dass Verantwortlich für die Information über ein Lebensmittel der Lebensmittelunternehmer ist, unter dessen Namen oder Firma das Lebensmittel vermarktet wird oder, wenn dieser Unternehmer nicht in der Union niedergelassen ist, der Importeur, der das Lebensmittel in die Union einführt.

Der für die Information über das Lebensmittel verantwortliche Lebensmittelunternehmer gewährleistet gemäß dem anwendbaren Lebensmittelinformationsrecht und den Anforderungen der einschlägigen einzelstaatlichen Rechtsvorschriften das Vorhandensein und die Richtigkeit der Informationen über das Lebensmittel. Art. 9 enthält im Verzeichnis der verpflichtenden Angaben unter Buchst. h) den Namen oder die Firma und die Anschrift des Lebensmittelunternehmers nach Art. 8 Abs. 1.

Die Verordnung gilt verbindlich in allen Mitgliedstaaten der EU. Ein Abweichen von der Adressangabe ist daher nicht möglich.

2.2.16 Weitergabe von Mieterkontaktdaten an Makler und Nachmieter

Im Bereich der Wohnungswirtschaft führt die Weitergabe personenbezogener Kontaktdaten (Telefonnummer, E-Mail-Adresse) im Rahmen der Beendigung des Mietverhältnisses zunehmend zu Beschwerden.

Petenten monieren dabei regelmäßig eine unautorisierte Weitergabe ihrer Daten an Makler, Mietinteressenten oder Nachmieter. Dies verdeutlicht die bei den Mietern weit verbreitete Sorge, ihnen werde die Kontrolle darüber genommen, wem sie diese Daten offenbaren. Tatsächlich ist die Gefahr eines Datenmissbrauchs nicht von der Hand zu weisen, zumal die

E-Mail-Adresse oftmals zur Identifizierung bei diversen Internetdiensten verwendet wird. In Bezug auf die Weitergabe der Telefonnummer beklagten sich betroffene Personen über Anrufe zur Unzeit, etwa in den frühen Morgen- oder späten Abendstunden.

Telefonnummer und E-Mail-Adresse sind personenbezogene Daten im Sinne des Art. 4 Nr. 1 Datenschutz-Grundverordnung (DSGVO). Ihre Weitergabe fällt unter den Verarbeitungsbegriff (Art. 4 Nr. 2 DSGVO). Für deren Rechtmäßigkeit bedarf es einer Rechtsgrundlage nach Art. 6 Abs. 1 DSGVO.

Zunächst ist klarzustellen, dass die Erhebung, Speicherung und Verwendung der Telefonnummer sowie der E-Mail-Adresse als Kontaktdaten der Mieter regelmäßig von der Zweckbestimmung des Mietverhältnisses Art. 6 Abs. 1 Buchst. b DSGVO gedeckt ist. Dies gilt jedoch nur unter der Einschränkung, dass diese Daten ausschließlich für eigene Zwecke des Vermieters oder der Hausverwaltung im Rahmen der Durchführung des Mietvertrags genutzt werden.

Vermieter und auch Hausverwalter unterliegen oft der irrigen Ansicht, dass mit einer vom Mieter gegengezeichneten Datenschutzerklärung eine rechtliche Grundlage für eine Datenweitergabe geschaffen werden kann. Tatsächlich kommen sie damit jedoch lediglich der ihnen von Gesetzes wegen auferlegten Informationspflicht nach Art. 13 DSGVO nach. Eine Datenschutzerklärung kann eine Datenverarbeitung nach Art. 6 Abs. 1 DSGVO nicht rechtfertigen, sondern stellt lediglich eine diese flankierende Maßnahme dar. Daran ändert auch eine Gegenzeichnung auf Mieterseite nichts. Schon gar nicht ist eine solche als Einwilligung im Sinne des Art. 6 Abs. 1 Buchst. a DSGVO zu qualifizieren. Eine Einwilligung muss freiwillig, für einen konkreten Fall, nach ausreichender Information und in unmissverständlicher Weise abgegeben werden. Daneben muss sie an einen oder mehrere ausdrücklich genannte Zwecke gebunden sein und darüber hinaus einen ausdrücklichen Hinweis auf die jederzeit bestehende Widerrufsmöglichkeit enthalten.

Kann die Verwendung der Kontaktdaten während des Mietverhältnisses, etwa für Handwerker und Beauftragte des Vermieters oder der Hausverwaltung im Einzelfall gegebenenfalls noch mit mietvertraglichen Notwendigkeiten begründet werden, ist die Weitergabe von Telefonnummer und E-Mail-Adresse an Nachmieter oder Makler auch nicht zur weiteren Erfüllung des Mietvertrags erforderlich, mithin greift auch regelmäßig nicht der Zulässigkeitstatbestand des Art. 6 Abs. 1 Buchst. b DSGVO. Was dabei zur Erfüllung des Mietvertrags erforderlich ist, ist an diesbezüglichen Vorschriften des Bürgerlichen Gesetzbuches (§§ 535 ff. BGB) zu messen. Auch die umfassende Interessenabwägung nach Art. 6 Abs. 1 Buchst. f DSGVO greift nicht. Danach ist die Verarbeitung personenbezogener Daten 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. Mieter müssen es aber nicht hinnehmen, dass personenbezogene Daten, über die der Vermieter oder Verwalter verfügt, ungefragt an Dritte, mit denen sie selbst keinerlei Beziehung eingehen wollen, weitergegeben

werden. Auch eine dies-bezügliche Unterrichtung im Zuge eines entsprechenden Hinweisschreibens führt nicht zur Zulässigkeit einer insoweit beabsichtigten Datenweitergabe; eine rechtswirksame Einwilligung setzt eine eindeutige Handlung der betroffenen Person voraus.

Im Folgenden sollen exemplarisch einige Beispielsfälle dargestellt werden:

Nach der Kündigung ihrer Mietwohnung erhielt eine Mieterin auf ihrem privaten Handy einen Anruf einer Immobilienvermittlung zwecks Vereinbarung eines Besichtigungstermins. Außerdem wurde sie darüber unterrichtet, dass die (noch) von ihr bewohnte Wohnung auf mehreren Internetportalen zur Weitervermietung eingestellt worden sei.

Wie mir die Hausverwaltung belegte, hatte die Mieterin ihre Telefonnummer vor dem Zustandekommen des bisherigen Mietverhältnisses zwar in einer Mieterselbstauskunft dem Makler gegenüber offengelegt. Außerdem gab es eine schriftliche Vorabinformation darüber, dass sich der Makler mit ihr bezüglich eines Besichtigungstermins in Verbindung setzen wird. Jedoch eignet sich eine zur Eingehung des bestehenden Mietverhältnisses erteilte Selbstauskunft schon deshalb nicht als Rechtfertigung für eine darauf gestützte Datenweitergabe, weil nach dem Grundsatz der Speicherbegrenzung der Makler nach dem Mietvertragsschluss nicht mehr über die personenbezogenen Daten der Mieterin hätte verfügen dürfen (Art. 5 Abs. 1 Buchst. e DSGVO). Der Zweck der Datenerhebung war erreicht, somit hätten die beim Makler vorhandenen Mieterdaten unverzüglich gelöscht beziehungsweise an den Vermieter übergeben werden müssen.

Im Übrigen müssen (Noch-)Mieter – abgesehen von einer ausdrücklichen Einwilligung (Art. 6 Abs. 1 Buchst. a DSGVO) – eine Weitergabe ihrer Kontaktdaten zu Zwecken der Vorbereitung sich anschließender neuer Mietverhältnisse natürlich nicht hinnehmen. Eine Datenübermittelung an Maklerunternehmen zur Abstimmung von Besichtigungs-terminen ist weder von der Zweckbestimmung des Mietvertrags (Art. 6 Abs. 1 Buchst. b Datenschutz-Grundverordnung) umfasst, noch aus einer Interessenabwägung (Art. 6 Abs. 1 Buchst. f Datenschutz-Grundverordnung) herleitbar. Unabhängig vom Fehlen eines berechtigten Interesses hätte die Hausverwaltung die Terminabstimmung auch unkompliziert selbst vornehmen können. Damit wäre ein Eingriff in die Persönlichkeitsrechte der Mieterin effektiv zu vermeiden gewesen.

Die Hausverwaltung wies mir schließlich nach, dass sie bei dem beauftragten Makler eine weitere Verwendung der Daten unterbunden hat. Dieser wies ihr gegenüber auch die Löschung der entsprechenden Daten nach.

In einem weiteren Fall meldete sich ein Mieter einer Wohnungseigentümergemeinschaft bei mir und klagte über tägliche Anrufe während der Arbeitszeit. Nach einer von seinem Vermieter ausgehenden Weitergabe seiner Telefonnummer an drei Unternehmen, die ihrerseits wiederum Makler beauftragt hatten, wurde er permanent zwecks Terminvereinbarungen telefonisch

kontaktiert. Vor Einreichung einer Petition bei meiner Behörde hatte er sich mit dem Vermieter diesbezüglich in Verbindung gesetzt. Dieser hatte ihn jedoch lediglich lapidar auf die Kündigungsbestätigung, die einen schriftlichen Hinweis auf die Datenweitergabe (Name, Telefonnummer und E-Mail-Adresse) an drei Firmen enthielt, verwiesen. Der Verwalter machte mir gegenüber zu seiner Rechtfertigung zusätzlich auf die im Rahmen des Mietverhältnisses gemäß Art. 13 DSGVO erfolgte Aufklärung über die Datenverarbeitung aufmerksam.

Zwar stelle ich nicht das legitime Interesse des Vermieters an einer lückenlosen Weitervermietung in Frage. Eine Notwendigkeit, hierzu die Daten an mit der Mietersuche beauftragte Unternehmen und von diesen beauftragte Makler weiterzugeben, sehe ich indes nicht. Der Verweis auf die Datenschutzerklärung ging auch fehl, da mit dieser keine Legalisierung für eine eigentlich unzulässige Verarbeitung personenbezogener Daten erreicht werden kann (siehe oben). Im Übrigen enthielt diese Datenschutzerklärung keine über allgemeine Formulierungen hinausgehenden Hinweise. Sie benannte weder Makler oder mit der Weitervermietung beauftragte Unternehmen als (mögliche) Empfänger noch enthielt sie Ausführungen zum Umfang der Datennutzung.

Die unzulässige Nutzung der Mieterdaten wurde schließlich dadurch beendet, dass der Vermieter die von ihm beauftragten Unternehmen zur Löschung und dem Verzicht auf eine weitere Nutzung aufforderte.

Beim dritten Beispiel stellte sich im Nachgang eines Besichtigungstermins zwecks Nachvermietung den Mietinteressenten noch die Frage, ob denn ihre bisherige Küche auch in die neue Wohnung passe. Deshalb kontaktierten sie die Hausverwaltung, um sich direkt an die bisherigen Mieter wenden zu können. Mit der von der Verwaltung genannten Telefonnummer ausgestattet, wandten sie sich telefonisch an die Mieter, was diese zum Anlass nahmen, sich hierüber bei meiner Behörde zu beschweren.

Auf Befragen der Beschwerdeführerin war sich der Hausverwaltung keiner Schuld bewusst. Sie zeigte sich uneinsichtig und führte an, dass andere Mieter das schließlich auch nicht so schlimm sehen würden.

Auch in diesem Fall gab es für die Datenherausgabe keine Berechtigung. Die Mieter mussten nicht damit rechnen, dass die potenziellen Nachmieter direkt mit ihnen in Verbindung treten würden, zumal die Besichtigung auf Veranlassung der Hausverwaltung zustande gekommen war. Die Verwaltung hätte also entweder selbst die Mieterin kontaktieren müssen und um Mitteilung der Küchenmaße beziehungsweise selbständige Kontaktaufnahme bitten können oder im Bedarfsfalls einen (weiteren) Besichtigungstermin koordinieren müssen.

Die Hausverwaltung veranlasste auch hier die Löschung des Namens sowie der Telefonnummer gegenüber den potenziellen Nachmietern.

Hausverwaltungen und betroffenen Mietern rate ich, was die Verwendung der Mieterdaten angeht, ausdrückliche und eindeutige Vereinbarungen zu treffen. Weitergaben von E-Mail- und Telefonkontaktdaten sind die betroffenen Mieter aber berechtigt, auch im Nachgang einzuschränken. Hausverwaltungen und Vermieter sollten im Übrigen in Zweifels- und Einzelfällen, was die Weitergabe an Dritte anbelangt Rücksprache führen beziehungsweise ggfs. gesonderte Einwilligungen einholen.

2.2.17 Zur Frage der Übertragung der Datenbereitstellung nach dem Zensusgesetz auf die Hausverwaltung

Ursprünglich war für das Jahr 2021 eine alle zehn Jahre stattfindende Bevölkerungszählung in den Mitgliedsstaaten der Europäischen Union geplant, an der Deutschland auf der Basis des Zensusgesetzes 2021 (ZensG 2021) teilnehmen sollte. Eigentlicher Stichtag war der 16. Mai 2021, § 1 Abs. 1 ZensG 2021. Der Zweck dieser statistischen Erhebung besteht in der Ermittlung von grundlegenden wirtschafts- und soziostrukturellen Erkenntnissen bezogen auf die Bevölkerung und deren Wohnsituation in Deutschland. Die ermittelten Bevölkerungszahlen finden unter anderem Verwendung bei der Einteilung der Wahlkreise oder der Stimmenverteilung der Länder im Bundesrat. Aber auch der Länderfinanzausgleich, die Berechnung für EU-Fördermittel sowie die Verteilung von Steuermitteln beruhen auf den gewonnenen Zensusdaten. Infolge der Coronavirus-Pandemie wurde dieser Zensus aber von 2021 in das Jahr 2022 verschoben; die gesetzliche Grundlage wurde vom Zensusgesetz 2021 in das Zensusgesetz 2022 (ZensG 2022) geändert. Neuer Stichtag ist nunmehr der 15. Mai 2022, § 1 Abs. 1 ZensG 2022.

Ein Zentraler Bestandteil des Zensus ist die Gebäude- und Wohnungszählung, § 9 Abs. 1 ZensG 2022. Auskunftspflichtig sind die Eigentümer und die Verwalter gemäß § 24 Abs. 1 ZensG 2022. Verwaltungen, die (wohnungsbezogene) Angaben nach § 10 ZensG 2022 nicht machen können, sind verpflichtet stattdessen Angaben zu den Eigentümern zu erteilen, § 24 Abs. 2 ZensG 2022.

Der eigentlich für das Jahr 2021 geplante Zensus war Anlass der Beschwerde eines Eigentümers einer größeren Wohnungseigentümergemeinschaft. Diese Beschwerde richtete sich gegen die Umsetzung des Zensus 2021 und einen diesbezüglichen Beschluss in der Eigentümerversammlung. Mit der Beschlussfassung habe die Hausverwaltung gegen Bestimmungen des Datenschutzes verstoßen, so der Beschwerdeführer. Der Beschluss sah vor, dass der Verwalter für den Mehraufwand zur Erfüllung der sich aus dem Zensus ergebenden Mitteilungspflichten eine pauschale Sondervergütung erhält und die Kostenverteilung nach der Anzahl der Wohnungen erfolgen sollte. Bei Einsicht in das Versammlungsprotokoll ergab sich in der Tat zunächst der Eindruck, als wolle sich die Hausverwaltung mit einem Mehrheitsbeschluss der Eigentümer nicht nur die Übermittlung der gebäudebezogenen Merkmale – § 10 Abs. 1 Nr. 1 ZensG 2021 – übertragen lassen, sondern auch die Übermittlung der Wohnungs- und Personenmerkmale (vgl. § 10 Abs. 1 Nr. 2, Abs. 2 ZensG 2021). Diese beinhalten indes

auch personenbezogene Daten im Sinne des Art. 4 Nr. 1 Datenschutz-Grundverordnung (DSGVO), so zum Beispiel Nettokaltmiete und Namen der Wohnungsnutzer.

Bei einer per Mehrheitsbeschluss allen Eigentümern auferlegten Verpflichtung zur Bereitstellung dieser personenbezogenen Daten an die Hausverwaltung würden die einzelnen Eigentümer insoweit aber die Herrschaft über die sie betreffenden personenbezogenen Daten auch dann verlieren, wenn sie diesem Beschluss nicht zugestimmt haben. Ein Mehrheitsbeschluss stellt keine Einwilligung im Sinne von Art. 6 Abs. 1 Buchst. a DSGVO dar. In einem solchen Fall würden von den auf der Eigentümerversammlung anwesenden beziehungsweise dem Beschluss zustimmenden Eigentümern praktisch über die Köpfe der dagegen votierenden oder abwesenden Eigentümer hinweg Entscheidungen in ausschließlich den jeweiligen einzelnen Eigentümer beziehungsweise dessen personenbezogene Daten betreffenden Angelegenheiten getroffen. Dem steht allerdings das verfassungsmäßige Recht auf informationelle Selbstbestimmung entgegen. Dieses regelt die Herrschaft des Einzelnen über die Preisgabe und Verwendung seiner personenbezogenen Daten und ist somit ein individuelles und höchstpersönliches Grundrecht. Ein solcher Mehrheitsbeschluss konnte daher keine Bindungswirkung für die einzelnen Eigentümer entfalten.

Wie sich schließlich herausstellte, waren sowohl der Beschlusstext als auch die dazugehörige Erläuterung lediglich missverständlich formuliert, was für die Irritation beim Beschwerdeführer gesorgt hatte. Tatsächlich war die diesbezügliche Dienstleistung der Hausverwaltung lediglich als freiwilliges, gleichwohl aber natürlich nicht kostenfreies Angebot gegenüber den Eigentümern gedacht, für diese die Informationsübermittlung insgesamt zu übernehmen. In der ersten Phase sollte durch die Hausverwaltung die Übermittlung der Daten im Rahmen der Gebäudezählung erfolgen unter gleichzeitiger Herausgabe der Eigentümerlisten, in der zweiten Phase dann gegebenenfalls die Übermittlung der Wohnungs- und Personenmerkmale. Ob der Prozess in seiner zweiten Stufe als Auftragsverarbeitung ausgestaltet oder aber auf eine Einwilligung gestützt würde, stand zum Abschluss des Aufsichtsverfahrens noch nicht fest. Da diese Angelegenheit seitens der Hausverwaltung auch von deren externen Datenschutzbeauftragten begleitet worden ist, konnte ich von einer weiteren Befassung meiner Behörde absehen. Insoweit habe ich lediglich noch dafür gesorgt, dass die Hausverwaltung zur Vermeidung weiterer Eingaben oder Nachfragen eine schriftliche Klarstellung gegenüber allen Eigentümern der Gemeinschaft vornimmt.

2.2.18 Die Nutzung von E-Mail- und Telefonkontaktdaten bei bestehender Geschäftsbeziehung

Ein Beschwerdeführer hatte sich an mich gewandt, weil er der Auffassung war, dass der seitens des Verantwortlichen mit der Absicht einer Vertragsverlängerung mit ihm geführte Anruf unzulässig gewesen wäre. Der Beschwerdeführer hätte seinerseits keine ausdrückliche Einwilligung dafür erteilt.

Wie mir das Unternehmen in seiner Stellungnahme plausibel dargelegt hat, erfolgte der Anruf im kausalen Zusammenhang mit dem Besuch des Kunden im Laden des Verantwortlichen und hat sich auch inhaltlich im Rahmen der von ihm selbst initiierten Vertragsanbahnungsverhandlungen bewegt. Um einen Werbeanruf im Sinne von § 7 Gesetz gegen den unlauteren Wettbewerb (UWG) handelt es sich daher insoweit nicht. Unter dieser Voraussetzung bedarf es gemäß Art. 6 Abs. 1 Satz 1 Buchst. b Datenschutz-Grundverordnung zur diesbezüglichen Datenverarbeitung auch keiner (zusätzlichen) Einwilligung des Betroffenen.

Ein Kundenwille, von bestimmten Kommunikationswegen abzusehen, ist selbstverständlich zu vermerken und (außer in Notfällen) zu respektieren.

2.2.19 Zulässigkeit von Business-to-Business-Marketing

Bei sogenannter „Business-to-Business“-Werbung ist ein etwaiger Personenbezug zu beachten. Auch ist eine entsprechende Dokumentation der Werbemailing-Prozesse umzusetzen, die Auskunftsverlangen betroffener Personen ermöglicht.

Das Verbot der Kaltakquise nach dem Gesetz gegen den unlauteren Wettbewerb gilt in Absolutheit zwar nur für den sogenannten „Business-to-Consumer“-Bereich. Verkannt worden ist in einem mir vorgelegten Fall aber offenbar der Umstand, dass auch Firmen-E-Mail-Adressen einen Personenbezug enthalten, soweit darin Namensbestandteile vorkommen oder – wenngleich weniger beschwerend – auf Personengesellschaften verweisen. Ich habe den Verantwortlichen auf die Rechtslage hingewiesen. Damit verbunden war die Belehrung, dass Daten (vorläufig) nicht gelöscht werden dürfen, soweit Auskunftsverlangen anhängig sind.

2.2.20 Abgrenzung nicht werblicher Kundeninformationen von Werbeansprachen und Erinnerungsmails – „Nudgemails“

In einem Beschwerdeverfahren hat ein Portalbetreiber zusätzlich zum (insoweit unauffälligen) Newsletter nicht abwählbare Erinnerungs-E-Mails („Nudgemails“) kreiert, die – laut digitalem Paperwork, das dem Betroffenem auch zu Vertragsschluss bekannt gemacht worden war – „automatisiert“ waren und „nicht ausgeschaltet“ werden konnten, ohne zugleich das Nutzerkonto zu löschen. Ein Werbewiderspruch nach Art. 21 Abs. 2 Datenschutz-Grundverordnung (DSGVO) durch den Betroffenen war mit eben dieser Argumentation zurückgewiesen worden, so dass dieser sich vor die Entscheidung gestellt sah, entweder die Sendungen hinzunehmen oder das Konto zu kündigen und sich an meine Behörde wandte.

Für die Beurteilung solcher Erinnerungs-E-Mails drängt sich zunächst die Frage auf, ob nicht doch Werbung im rechtlichen Sinn verbreitet werden soll. Werbung könnte zu bejahen sein, wenn ein Absatzziel in Richtung eines kostenpflichtigen Alternativ- oder Zusatzprodukts bestanden hätte. Dafür bot der Vorgang allerdings keine Anhaltspunkte.

Die Voraussetzungen nach dem Gesetz gegen unlauteren Wettbewerb für elektronische Werbung habe ich daher als objektiv nicht erfüllt angesehen. Dennoch verblieb die Frage, ob eine Rechtsgrundlage nach Art. 6 DSGVO vorgelegen hatte. Mit der Erinnerungs-E-Mail wurde dem Kunden mitgeteilt, dass länger inaktive Profile deaktiviert würden. Mit Stellungnahme des Verantwortlichen hatte dieser dies mit dem Ablauf von neun Monaten präzisiert. Dies führe zur Einstellung jeglicher E-Mail-Kontaktierung und zwar auch dann, wenn das Vertragsverhältnis durch den Nutzer nicht gekündigt worden sei.

Als Instrument zur Identifikation und Löschung von „File-Leichen“ erachte ich die Erinnerungs-E-Mail vertraglich und gemessen an den Erwartungen des Vertragspartners als üblich und vertretbar. Folgende Voraussetzungen müssen jedoch nach meiner Überzeugung eingehalten werden: Die Sendungen haben einen kundenbezogenen, vertraglich relevanten Informationsgehalt aufzuweisen, insbesondere im Hinblick auf eine Warnung vor Konsequenzen bei weiterer Inaktivität. Auch darf technisch keine Endlosroutine eingerichtet sein und der zeitliche Abstand der Erinnerungs-E-Mails muss, gemessen am Zweck und mutmaßlichen Interesse orientiert, angemessen sein.

Unter diesen (engen) Voraussetzungen habe ich die „Nudgemail“ als zulässige Form der Bestandskundenkommunikation erachtet.

2.2.21 Inanspruchnahme eines Minderjährigen durch einen Inkassodienstleister

In einem Fall führte ein Petent beziehungsweise dessen Elternsorgeberechtigter gegen eine Inanspruchnahme durch ein Inkassounternehmen an, dass der Betroffene als angeblicher Kunde beziehungsweise Schuldner minderjährig und damit – nach dem anwendbaren österreichischen Recht – nicht geschäftsfähig sei. Diese Behauptung wurde durch einen entsprechenden behördlichen Melderegisterauszug des Heimatlandes belegt. Der Gegenstand des angeblichen Vertrags war die Nutzung einer erotisch orientierten Online-Partnerbörse. Mangels Zahlung lag jedenfalls kein gültiger Vertrag des Inkasso-Auftraggebers mit dem Betroffenen vor (vgl. § 110 Bürgerliches Gesetzbuch beziehungsweise § 170 Abs. 3 Allgemeines Bürgerliches Gesetzbuch). Der Betroffene hatte seinen Sitz in Österreich, daher war der Vertrag nach österreichischem Zivilrecht zu beurteilen.

Das hierzu befragte in Sachsen ansässige Inkassounternehmen gab unwiderlegbar an, die entsprechende direkte Antwort des Betroffenen beziehungsweise dessen Erziehungsberechtigter nicht erhalten zu haben. Erst im Rahmen von nachfolgenden Erörterungen sagte das Unternehmen schließlich zu, die entsprechenden Daten nunmehr zeitlich und sachlich eingeschränkt zu nutzen, soweit im Rahmen zulässiger Ermittlungen wegen behaupteter Betrugshandlungen durch Verwendung fremder Identitäten erforderlich, und anschließend zeitnah zu löschen.

Das datenschutzaufsichtliche Verfahren konnte ohne Verwarnung zum Abschluss gebracht werden, da ein Vorsatz des Inkassounternehmens des Verantwortlichen, nicht belegbar war und der Datenschutzverstoß kooperativ abgestellt wurde. Allerdings wurde das Unternehmen darauf hingewiesen, dass der konkrete Fall Lücken in der Altersüberprüfung des auftraggebenden Unternehmens aufzeigt. Entsprechend trifft das Inkassounternehmen in Bezug auf diesen Auftraggeber eine gesteigerte Sorgfaltspflicht zur Prüfung der Plausibilität der zur Einziehung übertragenen Forderungen und der Berechtigung zur Datenverarbeitung im Rahmen des Inkassos (vgl. eingehender Tätigkeitsbericht 2019, 2.2.18, Seite 54 ff.).

2.2.22 Richtigstellung zu „Anforderungen an Webseiten öffentlicher Stellen“

Im Tätigkeitsbericht 2019, 2.2.1, Seite 31 ff. habe ich dargelegt, unter welchen Voraussetzungen öffentliche Stellen Nutzerdaten für Besucherstatistiken und ähnliche Zwecke datenschutzkonform verarbeiten können. Im Kern ging es dabei um die Auslegung der Rechtsgrundlage des berechtigten Art. 6 Abs. 1 Buchst. f Datenschutz-Grundverordnung (DSGVO), welcher für private Stellen gilt und für öffentliche Stellen nicht anwendbar ist. Daher habe ich die Anwendung des Art. 6 Abs. 1 Buchst. e DSGVO in analoger Auslegung empfohlen. Im Ergebnis war es öffentlichen Stellen damit möglich auch Cookies zur Wiedererkennung von Besuchern zu setzen, wenn dabei die Datenverarbeitung in ausschließlicher Hoheit der öffentlichen Stelle betrieben wird.

Der Bundesgerichtshof (BGH) hat im Urteil vom 28. Mai 2020 in dem Verfahren des Bundesverbandes der Verbraucherzentralen (VZBV) gegen die als Adresshändler und Gewinnspielbetreiber tätige Planet49 GmbH grundlegende Entscheidungen im Zusammenhang mit der datenschutzrechtlichen Bewertung des Einsatzes von Cookies auf Webseiten getroffen. Das Gericht hat erstens § 15 Abs. 3 Telemediengesetz (TMG) richtlinienkonform entsprechend den Vorgaben von Art. 5 Abs. 3 ePrivacy-Richtlinie ausgelegt und festgestellt, dass Diensteanbieter Cookies zur Erstellung von Nutzungsprofilen für Werbezwecke und Marketing nur mit Einwilligung des Nutzers einsetzen dürfen. Zweitens sei mit diesem Inhalt § 15 Abs. 3 TMG neben der seit dem 25. Mai 2018 geltenden DSGVO anwendbar. Drittens stelle ein voreingestelltes Ankreuzkästchen in einem Cookie-Fenster auf einer Webseite keine wirksame datenschutzrechtliche Einwilligung dar. Mit dieser dritten Aussage folgte der BGH wenig überraschend der im Vorlageverfahren eingeholten Vorabentscheidung des Europäischen Gerichtshofs. Dieser hatte bereits am 1. Oktober 2019 geurteilt, dass keine wirksame Einwilligung vorliegt, wenn die Speicherung von Informationen oder der Zugriff auf Informationen, die bereits im Endgerät des Nutzers einer Website gespeichert sind, mittels Cookies durch ein voreingestelltes Ankreuzkästchen erlaubt wird, das der Nutzer zur Verweigerung seiner Einwilligung abwählen muss.

Damit ist klar, dass für nicht technisch erforderliche Cookies eine informierte Einwilligung erforderlich ist. Öffentliche Stellen sollten Ihre Websites daher auf eine Übereinstimmung mit den geltenden Vorschriften hin überprüfen. Mich erreichen nach wie vor zahlreiche Beschwerden von Bürgern, die Websites öffentlicher Stellen überprüfen und Verstöße feststellen müssen. Dabei ist nicht nur die Haupt-Website der öffentlichen Stelle zu betrachten, sondern auch die der Einrichtungen der öffentlichen Stelle, die eigene Webauftritte betreiben, zum Beispiel Bibliotheken und Bäder.

Generell rate ich öffentlichen Stellen davon ab, auf Websites einwilligungsbedürftige Datenverarbeitungen durchzuführen. Die Gründe liegen darin, dass bereits die Freiwilligkeit der abgegebenen Willenserklärung zu hinterfragen ist, da eine Website einer öffentlichen Stelle in aller Regel als Behörde wahrgenommen wird und daher nicht von einer Einwilligung auf Augenhöhe ausgegangen werden kann. Darüber hinaus ist Art. 8 DSGVO zu beachten und geeignete Mechanismen zur Sicherstellung der Einwilligung durch den Träger der elterlichen Verantwortung für ein Kind zu etablieren. Da gerade öffentliche Stellen den Anspruch verfolgen für alle Bürger zur Verfügung zu stehen, ist dieser Aspekt unbedingt zu beachten und in der Praxis mit zahlreichen Problemen, etwa des geeigneten Nachweises und einer technisch komplexen Umsetzung, behaftet.

Wenn dennoch eine Einwilligung eingeholt werden soll, hat diese allen Ansprüchen an die Informiertheit zu genügen. Hinsichtlich der Datenverarbeitung ist vollständige Transparenz herzustellen und technisch sicherzustellen, dass die Datenverarbeitung auch tatsächlich erst nach einer Einwilligung oder eben gar nicht bei fehlender Einwilligung stattfindet. Da in der Praxis dabei häufig Fehler auftreten, möchte ich gesondert auf meine Veröffentlichung zum Einsatz von Consent-Layern auf Webseiten hinweisen, abrufbar auf datenschutz.sachsen.de.

Nach wie vor möglich ist eine Webanalyse, welche ohne Cookies auskommt und sich ansonsten an die im Tätigkeitsbericht 2019 formulierten Anforderungen hält.

Für private Stellen sei ergänzt, dass auch vor der Entscheidung des BGH bei einer Anwendung der Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien (OH Telemedien, abrufbar auf datenschutzkonferenz-online.de) im Ergebnis die meisten der in der Praxis eingesetzten Tracking- und Marketingdienste aufgrund der Übermittlungsproblematik an Dritte und deren Verarbeitung von Nutzungsdaten für eigene Zwecke eine informierte Einwilligung erfordern.

2.2.23 Videoüberwachung sorgt für Nachbarschaftsstreitigkeiten

Fast schon regelmäßig erreichen mich Eingaben wegen einer Videoüberwachung (auch) benachbarter Grundstücke, bei denen sich die Grundstückseigentümer gegenseitig der Video-

überwachung ihres jeweiligen Grundstücks bezichtigen. In der Mehrzahl der Fälle ist die Videoüberwachung in der Nachbarschaft die Folge eines zerrütteten nachbarschaftlichen Verhältnisses, was mir oftmals mehr oder weniger umfangreich auch so von den Beteiligten dargelegt wird. Dabei geht es meistens um zivilrechtliche Fragestellungen, die die Zuständigkeit meiner Behörde nicht betreffen. Daneben dient eine Eingabe den verfeindeten Parteien oft als Ventil, um sich über andere Vorfälle zu beschweren oder dem Nachbarn auf „offiziellem Weg“ Schwierigkeiten zu bereiten.

So bemerkte ein Grundstückseigentümer bei Baumfällarbeiten auf seinem Grundstück eine auf dem Nachbargrundstück befindliche Videokamera mit Ausrichtung auf sein Grundstück. Diese Entdeckung nahm er zum Anlass, bei der Stadtverwaltung die komplette Entfernung oder dauerhafte Demontage der Kamera zu verlangen, von wo aus er an meine Behörde verwiesen wurde. Nach Befragen des Kamerabetreibers bezichtigte dieser seinerseits Nachbarn der Videoüberwachung der davor verlaufenden öffentlichen Straße, die er benutzen müsse, um zu seinem Grundstück zu gelangen. Sein Verdacht ging sogar so weit, dass er dem Nachbarn die Erstellung von Tonaufnahmen zutraute, da jener mündliche Bemerkungen sofort „in die Tat“ umsetzen würde. Hintergrund für die massive Präsenz von Überwachungskameras in dem Umfeld der Grundstückseigentümer war offensichtlich eine Serie von Einbrüchen dort.

Wie sich im Laufe meiner Untersuchungen der „Retourkutsche“ des (zunächst) Verantwortlichen zeigte, waren zwei der vier Kameras auch auf Teile der öffentlichen Verkehrsfläche gerichtet. Zwar waren alle Kameras aufgrund technischer Probleme nicht in Betrieb. Auch sah der Verantwortliche keine Notwendigkeit, die zum damaligen Zeitpunkt auf seinem Grundstück tätigen Baufirmen zu überwachen. Jedoch war eine Wiederinbetriebnahme nach Abschluss der Grundstücksarbeiten angestrebt. Der Verantwortliche wähnte sich dabei im Einklang mit dem Datenschutzrecht.

Grundstückseigentümer nehmen oftmals nicht wahr, dass sie auch außerhalb ihres Grundstücks befindliche Bereiche zumindest am Rande mit überwachen, womöglich weil sie nur einen Blick für das eigene Grundstück haben. Ich kann darüber hinaus nur vermuten, dass sie sich auch mit den technischen Möglichkeiten, die eine Videoüberwachungsanlage bietet – beispielsweise zur Vornahme von Schwärzungen – nicht in jedem Fall hinreichend auskennen. Grundsätzlich bestehen zwar gegen eine Videoüberwachung des eigenen Grundstücks keine Bedenken. Sie ist jedenfalls bei allein zu eigenen Wohnzwecken genutzten Grundstücken von der Haushaltsausnahme des Art. 2 Abs. 2 Buchst. c Datenschutz-Grundverordnung (DSGVO) gedeckt mit der Folge, dass die datenschutzrechtlichen Vorschriften nicht zur Anwendung kommen. Überschreitet der Erfassungsbereich jedoch die Sphäre des eigenen Grundstücks, so richtet sich die datenschutzrechtliche Zulässigkeit nach den in Art. 6 Abs. 1 DSGVO abschließend aufgeführten Erlaubnistatbeständen. Bei der Videoüberwachung kommt dabei regelmäßig nur die umfassende Interessenabwägung des Art. 6 Abs. 1 Buchst. f DSGVO in Betracht.

Zwar ist der Einbruchsschutz von der Rechtsprechung als berechtigtes Interesse anerkannt. Indes fehlt es für die Überwachung von vor dem Grundstück verlaufenden öffentlichen Verkehrsflächen und auch nachbarlichen Grundstücken an der Erforderlichkeit zum Erreichen der verfolgten Zwecke. Außerdem überwiegen die Interessen der sich auf öffentlichen Flächen aufhaltenden und bewegenden Personen regelmäßig das Überwachungsinteresse des Kamerabetreibers. Daher hat sich eine Videoüberwachung grundsätzlich auf das eigene Grundstück zu beschränken.

Von Verantwortlichen wird gelegentlich auch vorgetragen, dass die Videoüberwachung in Absprache mit den Nachbarn erfolge und von diesen sogar der Wunsch geäußert worden sei, auch deren Grundstücke mit zu überwachen. Soweit sich eine Überwachung nur auf private Grundstücke beschränkt und eine nachbarliche Absprache hierzu vorliegt, sehe ich in datenschutzrechtlicher Hinsicht keine Veranlassung zu einem Eingreifen. Jedoch muss sich der einwilligende Nachbar darüber im Klaren sein, dass er damit je nach der Ausgestaltung der Videoüberwachung und der Verhältnisse vor Ort dem überwachenden Nachbarn zahlreiche Einblicke in seinen privaten Bereich ermöglicht. Außerdem besteht immer auch die Gefahr, dass sich ein anfangs gutes nachbarschaftliches Verhältnis wieder ins Gegenteil verkehrt.

Immer wieder konfrontieren mich verantwortliche Kamerabetreiber auch damit, dass sie von der Polizei einen Hinweis beziehungsweise eine Empfehlung zur Installation von Kameras erhalten hätten. Keinesfalls kann eine dahingehende Aussage eines Polizeibediensteten derart gedeutet werden, dass der Kamerabetreiber praktisch nach Belieben auch eine Überwachung öffentlicher Verkehrsflächen vornehmen darf. Ich vermute, dass derartige allgemeine polizeiliche Hinweise von den Grundstückseigentümer oftmals in diesem Sinne „umgedeutet“ werden. Unabhängig davon kann dies selbstredend nicht zu einer Legitimation einer nach der Datenschutz-Grundverordnung unzulässigen Videoüberwachung führen, ganz unabhängig davon, dass einzig meiner Behörde die datenschutzrechtliche Beurteilung in solchen Fällen obliegt und dementsprechend polizeiliche Aussagen keine Bindungswirkung für mich entfalten.

Vergleiche auch die Beiträge unter 2.2.24 und 2.2.25.

2.2.24 Videografie: Die wertvolle Skulptur im Vorgarten

Gerade wenn es um die nachbarschaftlichen Verhältnisse nicht zum Besten bestellt ist, befeuert die Installation und Inbetriebnahme einer Videokamera zumeist noch eine bestehende Auseinandersetzung. In deren Zuge versprechen sich die betroffenen Personen von meiner Behörde oftmals Abhilfe (vgl. 2.2.3). So war es auch in einem Fall, in dem mir die Videoüberwachung eines Vorgartens sowie der angrenzenden öffentlichen Straße angezeigt wurde. Der verantwortliche Grundstückseigentümer hatte im Zuge der Umgestaltung seines Vorgartens

die dortige Bepflanzung entfernt und an deren Stelle eine vorgeblich wertvolle Steinfigur installiert, die er mit einer an der Hauswand angebrachten Videoüberwachung zu schützen beabsichtigte.

Die mir vom Kamerabetreiber vorgelegten Screenshots zeigten, dass die Befürchtung der Nachbarn begründet war. Mit der an der Hauswand befestigten Kamera wurden tatsächlich auch Teile der am Grundstück entlangführenden Straße samt Fußgängerweg erfasst. Der gesamte überwachte Bereich, der Vorgarten und angrenzende Gehsteig, war als Live-Bild auf dem Smartphone des Grundstückseigentümers jederzeit und ortsunabhängig abrufbar. Eine Aufnahme wurde allerdings nur bei einer Bewegung in einem abgegrenzten Bereich des Vorgangs um die Steinfigur herum ausgelöst. Auch nur von diesem Raum wurde letztlich nach Auslösung eine Video- und Tonaufzeichnung erstellt.

Ich habe den Betrieb der Videokamera insoweit als unzulässig bewertet, als sich der Erfassungsbereich des Live-Monitorings auch auf außerhalb des privaten Betreibergrundstücks gelegene Flächen ausgedehnt hatte. Der Eigentümer konnte sich insoweit nicht auf die Haushaltsausnahme des Art. 2 Abs. 2 Buchst. c Datenschutz-Grundverordnung (DSGVO) berufen. Alleiniger Beurteilungsmaßstab war die umfassende Interessenabwägung nach Art. 6 Abs. 1 Buchst. f DSGVO.

Bei der Überwachung über das eigene Grundstück hinausgehender Bereiche scheitert die Zulässigkeit regelmäßig schon am Fehlen eines berechtigten Überwachungsinteresses. Zur Zulässigkeit einer Videoüberwachung muss außerdem das Erforderlichkeitsgebot beachtet werden. Danach muss eine Videoüberwachung geeignet sein, den angestrebten Zweck zu erreichen und es darf keine milderen Mittel geben, mit denen sich der Zweck in gleichem Maße erreichen lässt. Schließlich muss die Überwachungsmaßnahme auch verhältnismäßig sein.

Der Kamerabetreiber führte zunächst an, dass sich die Kamera nicht weiter drehen ließe. Dem ist entgegenzuhalten, dass sich aus einer von einem Kamerabetreiber verantworteten technischen Beschaffenheit kein im Sinne von Art. 6 Abs. 1 Buchst. f DSGVO legitimes Beobachtungserfordernis und demzufolge eine Rechtfertigung des Eingriffs in das Grundrecht auf informationelle Selbstbestimmung der betroffenen Personen (Passanten, Verkehrsteilnehmer) herleiten lässt. Es widerspräche daneben grundlegend dem datenschutzrechtlichen Erforderlichkeitsprinzip, wenn die Notwendigkeit einer Datenverarbeitung allein dem Umstand geschuldet wäre, dass der Verantwortliche eine technische Anlage angeschafft hat, die sich nicht anders betreiben lässt, obwohl der Grundrechtseingriff bei einer anderen Anlage oder einer (mit Kosten verbundenen) Änderung der Anbringungsart oder des Kamerastandorts problemlos hätte vermieden werden können.

Der Betreiber konnte mir nur einen einzigen Schadensfall nennen, der in der Sprengung seines Briefkastens zum Jahreswechsel bestanden hatte. Daraus ließ sich für mich jedoch kein Zusammenhang zu der (damals noch nicht vorhandenen) Steinskulptur herstellen. Schon gar nicht lässt dieser Vorfall den Schluss zu, es liege eine besondere Gefährdungslage vor. In Anbetracht der zu schützenden Steinfigur war eine Beschränkung der Überwachung auf das Privatgrundstück des Kamerabetreibers vollkommen ausreichend. Allein das Vorhandensein einer Videokamera – deren Erfassungsbereich sich ausschließlich auf das eigene Grundstück erstreckt – hat im Regelfall bereits einen ausreichend großen Abschreckungseffekt auf Personen, die das auf einem Privatgrundstück vorhandene Eigentum zu beeinträchtigen suchen. Zudem wurde die abschreckende Wirkung noch durch das am Hoftor angebrachte Hinweisschild verstärkt.

Nachdem ich dies dem Verantwortlichen entsprechend vorgehalten hatte, konnte er plötzlich doch eine Neuausrichtung der Kamera vornehmen, so dass diese nun nur noch den eigenen Vorgarten erfasst. In Anbetracht dessen, dass nur bei einer durch Bewegung ausgelösten Videoaufnahme auch eine (gleichzeitige) Tonaufnahme erfolgte und gerade im Freien durch die zumeist vorhandenen Umgebungsgeräusche (Straßenlärm, Wind, Vogelgezwitscher) sowie die Distanz zum Sprecher nicht von einer Verwertbarkeit entsprechender Aufzeichnungen auszugehen ist, sah ich in dieser Hinsicht keine datenschutzrechtlichen Bedenken.

2.2.25 Klingelkameras als digitale Türspione

In einem kuriosen Fall erreichte mich eine Eingabe zu einem digitalen Türspion in einer größeren Wohneinheit. Der Verantwortliche hatte an seiner Eingangstür den herkömmlichen Türspion durch einen von außen gut sichtbaren digitalen Türspion ersetzt. Die Beschwerdeführerin, die in einem Stockwerk darüber wohnte und die Wohnung des Verantwortlichen und damit auch den dort angebrachten digitalen Türspion regelmäßig passieren musste, sah ihr Persönlichkeitsrecht verletzt. Zuvor hatte sie sich bereits wegen einer „sofortigen Beseitigung“ an die zuständige Hausverwaltung gewandt, jedoch offensichtlich ohne Erfolg. Deshalb reichte sie bei meiner Behörde eine entsprechende Beschwerde ein und unterlegte diese mit der Befürchtung, dass sie stetig gefilmt werde.

Der Sachverhalt sollte sich jedoch schließlich gänzlich anders darstellen, als ihn mir die Hausbewohnerin geschildert hatte. Wie sich nach Befragen des Verantwortlichen herausstellte, hatte sie mir wesentliche Angaben vorenthalten. Es stellte sich heraus, dass die Rollen tatsächlich vertauscht waren und der Wohnungseigentümer als vermeintlicher „Täter“ das eigentliche „Opfer“ war. Denn die Beschwerdeführerin hatte davor mehrmals den digitalen Türspion mit Zeitung und Klebeband zugeklebt. Sie schreckte auch nicht vor dem Einsatz von Schneespray zurück, was letztlich zu einer irreparablen Beschädigung des Türspions führte, so dass dieser vom Wohnungsinhaber ausgetauscht werden musste.

Nachdem die in dem (ursprünglichen) digitalen Türspion integrierte Kamera jeweils nur bei Betätigung der dort gleichfalls integrierten Klingel eine Bildaufzeichnung (Einzelbild) auslöste, blieben dem Wohnungsinhaber jedes Mal nur die Feststellung des Vorfalls sowie die Beseitigung der Schadensfolgen. Er hatte jedoch keine Kenntnis über den Verursacher. Allerdings war die Hausbewohnerin augenscheinlich bei einer der ihr zuzuordnenden Aktionen gegen den Türspion abgerutscht und hatte dabei versehentlich den darin integrierten Klingelknopf betätigt, wodurch eine Bildaufzeichnung ausgelöst wurde. Obwohl sie zu diesem Zeitpunkt die Kameralinse bereits soweit besprüht hatte, dass kein verwertbares Bild mehr aufgezeichnet worden war, konnte der Wohnungsinhaber anhand der Aufzeichnung zumindest die „Tatzeit“ ermitteln. Am darauffolgenden Tag stellte er sich deshalb zu gleicher Zeit hinter die Wohnungstür und konnte so die Petentin auf frischer Tat ertappen. Diese zeigte sich allerdings uneinsichtig und relativierte die Bedeutung ihrer Tat.

Auch wenn dies verdeutlicht, dass bei meiner Behörde eingehenden Eingaben – im Besonderen bei der Videoüberwachung – oftmals weiter zurückreichende Meinungsverschiedenheiten und gar (verbale) Auseinandersetzungen zugrunde liegen, orientiert sich meine datenschutzrechtliche Bewertung strikt an den rechtlichen Vorgaben. Zur Rechtslage vor der Datenschutz-Grundverordnung habe ich mich zur Zulässigkeit digitaler Türspione bereits in meinem 7. Tätigkeitsbericht für den Datenschutz im nicht-öffentlichen Bereich (04/2013 bis 03/2015), 8.1.14, Seite 45 f. geäußert. Die dort aufgestellten Kriterien haben auch unter Berücksichtigung der Datenschutz-Grundverordnung Bestand. Demnach bestehen gegen den Einsatz von digitalen Türspionen dann keine Einwände, wenn folgende Voraussetzungen erfüllt sind:

- Die Kamera darf nur anlassbezogen durch das Klingeln an der Tür aktiviert werden können.
- Die Kamera darf nur den unmittelbaren Eingangsbereich (Nahbereich) vor der Tür erfassen.
- Die Kamera muss nach kurzer Zeit automatisch wieder deaktiviert werden.
- Es darf keine Übertragung des Livebildes über das Internet erfolgen.
- Es darf keine Aufzeichnung der Bilder möglich sein.

Sind diese Voraussetzungen erfüllt, habe ich gegen den Einsatz digitaler Türspione – ebenso wie von Klingelkameras – keine Einwände. Nachdem im vorliegenden Fall durch die neu angeschaffte Türspion-Kamera keine Fotos mehr gespeichert wurden, der Türspion auch nur nach manueller Betätigung der darin integrierten Klingel auslöste und das dargestellte Bild des Bereichs vor der Tür nur für zehn Sekunden sichtbar war, sah ich keinen Anhaltspunkt für einen Datenschutzverstoß. Dies habe ich der Beschwerdeführerin abschließend auch so mitgeteilt.

2.2.26 Videoüberwachung des Eingangsbereichs eines Wohnblockes – Ausnahmen bestätigen die Regel

Ausgangspunkt meiner Befassung war die Beschwerde eines im Erdgeschoss eines Hochhauses ansässigen gewerblichen Mieters. Dieser war – nachdem er unbefugt die der Zutrittskontrolle dienende Automatiktür im Eingangsbereich manuell außer Betrieb genommen hatte – durch den Vermieter telefonisch mit der Mitteilung kontaktiert worden, dass man ihn als Verursacher der Türmanipulationen mithilfe der diesen Bereich erfassenden Videoüberwachungsanlage habe ermitteln können. Der Beschwerdeführer führte mir gegenüber aus, nichts von einer solchen Videoüberwachung gewusst, insbesondere auch keine diesbezüglichen Hinweisschilder wahrgenommen zu haben und bat um Prüfung der Zulässigkeit des Betriebs der Videoüberwachungsanlage. Er habe sich umgeschaut und in dem insgesamt sehr großen Wohngebiet vergleichbare Videoüberwachungseinrichtungen auch noch in drei weiteren, von der Bauart her identischen Hochhäusern feststellen können.

Die Zulässigkeit einer Videoüberwachung in Gemeinschaftsbereichen von Mehrfamilienhäusern ist auf der Grundlage von Art. 6 Abs. 1 Buchst. f Datenschutz-Grundverordnung (DSGVO) zu beurteilen. Danach ist eine Videoüberwachung dann zulässig, wenn die damit verbundene Verarbeitung personenbezogener Daten zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

Diese Vorschrift setzt damit zunächst voraus, dass der Vermieter mit der Videoüberwachung berechtigte Interessen verfolgt und dass die Videoüberwachung zu deren Wahrung geeignet, erforderlich und insoweit auch verhältnismäßig ist. Darüber hinaus darf auch eine sich daran anschließende Interessenabwägung nicht zugunsten der betroffenen Personen, hier also in erster Linie der Mieter und ihrer Besucher, ausgehen.

Der Vermieter hat mir vorgetragen, dass die betreffenden Videoüberwachungsanlagen in den vier Hochhäusern zur Vandalismusprävention einerseits sowie auch zur Aufklärung und Beweissicherung bei Schadensfällen und Straftaten andererseits dienten. Die somit verfolgten Ziele in erster Linie des Eigentumsschutzes aber auch des Schutzes der Mieter waren ohne Weiteres als berechtigte Interessen anzuerkennen. Mit einer mir vorgelegten Auswertung der in den letzten Jahren aufgetretenen Versicherungsschäden wurde auch nachgewiesen, dass es sich nicht nur um eine abstrakte Gefahrenlage handelt, sondern dass innerhalb des Wohngebietes gerade die verfahrensgegenständlichen Hochhäuser in besonderem Maße von Vandalismusschäden betroffen waren.

Eine Videoüberwachung ist geeignet, diese Ziele zu erreichen, mindestens zu unterstützen, denn sie wirkt zum einen – soweit eine entsprechende Kennzeichnung beziehungsweise Erkennbarkeit gegeben ist – präventiv, und sie ermöglicht zum anderen – eine ausreichende Qualität der Aufnahmen vorausgesetzt – zweifelsfrei eine Beweissicherung und damit einen Beitrag zur Sachverhaltsaufklärung und Täterermittlung. Vorliegend war auch die Erforderlichkeit nicht in Frage zu stellen, denn die ergänzend getroffenen Maßnahmen wie etwa die Zutrittskontrolle (Automatiktüren mit Zutrittskontrollsystem) sowie der nächtliche Einsatz eines Sicherheitsdienstes im Wohngebiet haben sich offensichtlich nicht als ausreichend erwiesen, um die Anzahl der Schadensfälle maßgeblich einzudämmen. Dabei war auch zu berücksichtigen, dass ein Teil der festgestellten Schäden sogar auf einzelne Bewohner zurückzuführen war. Insoweit wies die Mieterschaft in den überwiegend mit Ein-Raum-Wohnungen ausgestatteten Hochhäusern eine eher ungünstige soziale Struktur und damit ein überdurchschnittliches Konfliktpotenzial auf. Gleichermaßen wie die Videoüberwachung wirkende mildere Maßnahmen waren nicht erkennbar. Die Videoüberwachung erfasste lediglich die besonders gefährdeten Eingangsbereiche und die Fahrstühle. Die näher an den Wohnungen liegenden Etagenflure sowie das Treppenhaus wurden nicht überwacht. Im Übrigen beschränkte sich die Videoüberwachung tatsächlich auf diese vier Hochhäuser; andere Gebäude wurden nicht überwacht.

In Bezug auf die notwendige Interessenabwägung war Folgendes festzustellen:

Im Regelfall überwiegen bei einer Videoüberwachung des unmittelbaren Wohnumfeldes die schutzwürdigen Belange der betroffenen Personen zwar das Interesse der Betreiber von Videoüberwachungsanlagen insbesondere dann, wenn die Kameras auch den regulären Zugang (hier den Eingangsbereich und die Fahrstühle) zu den Wohnungen erfassen, da sich die Mieter einer solchen Videoüberwachung unmöglich entziehen können. Sie müssen in jedem Fall den Eingangsbereich durchqueren und sind zumeist auf die Benutzung des Fahrstuhls angewiesen. Letzteres gilt jedenfalls für die zahlreichen älteren und oftmals gesundheitlich beeinträchtigten Bewohner der Hochhäuser, für die eine alternative Nutzung des Treppenhauses nicht in Betracht kommt. Bereits die Möglichkeit, dass der Vermieter jederzeit kontrollieren kann, welcher Mieter, wann, welchen Besuch empfängt, kommt oder geht, setzt die Wohnungsmieter einem erheblichen Überwachungs- und Anpassungsdruck aus. In analoger Weise, wenn auch abgeschwächt, gilt dies auch für die wenigen gewerblichen Mieter.

Gleichwohl bin ich in dem hier zu betrachtenden Einzelfall zu dem Ergebnis gekommen, dass das vom Vermieter beschriebene Überwachungsinteresse diese schutzwürdigen Betroffeneninteressen ausnahmsweise dennoch überwiegt. Dafür ausschlaggebend waren zum einen die sehr hohen Schadenssummen, die für die letzten sechs Jahre im sechsstelligen Bereich lagen; zum anderen war auch zu berücksichtigen, dass insbesondere funktionierende Fahrstühle für die – zu einem erheblichen Teil – ältere Mieterschaft von geradezu essentieller Bedeutung sind. Hinzu kommt das Interesse der Mieterschaft an einer funktionsfähigen Briefkastenanlage als zwingende Voraussetzung einer ordnungsgemäßen Zustellung von Postsendungen. Die

Überwachung diente also dem Schutz des Eigentums des Vermieters und lag auch im besonderen Interesse der Mieter selbst. Zudem wird der Eingangsbereich üblicherweise schnell passiert und auch der Aufenthalt im Fahrstuhl ist nur von kurzer Zeitdauer. Es fand weder eine ständige Überwachung per Live-Monitoring noch eine routinemäßige Auswertung ohne entsprechenden Grund statt. Nach der vorgelegten Dienstanweisung war der Zugriff auf die Aufzeichnungen nur bei konkretem Anlass zulässig. Anders als bei kleineren Wohnobjekten war der Großteil der Mieterschaft dem Vermieter nicht persönlich bekannt und daher auch bei anlassbedingter Auswertung (Durchsicht der Aufnahmen zur Täterermittlung) nicht ohne Weiteres identifizierbar, blieb ihm gegenüber in diesem Zusammenhang also weitgehend anonym. Der Eingriff in das Persönlichkeitsrecht der Mieter und ihrer Besucher war damit vergleichsweise gering; deutlich schwerwiegender waren die drohenden (gesundheitlichen) Nachteile insbesondere für die Bewohner der oberen Etagen im Fall nicht einsatzbereiter Fahrstühle. Die Videoüberwachung des Eingangsbereiches diente auch der Umsetzung einer funktionsfähigen Zutrittskontrolle (Automatiktüren mit Prüfung der Zutrittsberechtigung) und funktionsfähiger Briefkastenanlagen. Den Aussagen des Vermieters zufolge waren auch diese Bereiche immer wieder Ziel mutwilliger Sachbeschädigungen. Auch diesbezüglich bestand ein erhebliches Eigeninteresse der (redlichen) Mieter, dass bei der Objektsicherheit ein Mindestmaß an Sicherheit gewährleistet wird.

Im Ergebnis habe ich die Videoüberwachung in den vier Hochhäusern als zulässig und daher rechtmäßig bewertet, möchte an dieser Stelle aber ausdrücklich betonen, dass es sich dabei um eine Einzelfallentscheidung in einem besonderen Ausnahmefall gehandelt hat. Der Beschwerdeführer zeigte sich mit dieser Bewertung nicht einverstanden und hat nach Art. 78 Abs. 1 DSGVO diesbezüglich eine Klage beim Verwaltungsgericht Dresden eingereicht. Über den Ausgang dieses Klageverfahrens werde ich zu gegebener Zeit berichten.

In Bezug auf das vom Beschwerdeführer zugleich thematisierte Fehlen ausreichender Hinweise auf die Videoüberwachung habe ich in der Tat entsprechende Mängel feststellen müssen. Während der Vermieter behauptete, von Anfang an sei die Videoüberwachung durch entsprechende Aufkleber gekennzeichnet gewesen, hatte mir der Beschwerdeführer mitgeteilt, dass erst nach seiner Beschwerde überhaupt erstmalig Kamerapiktogramme angebracht worden seien. Die Wahrheit wird wohl irgendwo dazwischen liegen, insbesondere kann auch nicht ausgeschlossen werden, dass Mieter oder Dritte die Piktogramme wieder entfernt haben. Klar war hingegen, dass neue DSGVO-bezogene, im ersten Anlauf allerdings noch mängelbehaftete Hinweisschilder tatsächlich erst angebracht worden waren, nachdem dies der Beschwerdeführer sowohl gegenüber dem Vermieter als auch gegenüber mir entsprechend thematisiert hatte.

Letztendlich ist dann aber diesbezüglich für eine schnelle Mängelbeseitigung gesorgt worden. Dazu sind sowohl die Inhalte der vorgelagerten Hinweisschilder sowie der vollständigen Datenschutzinformation als auch deren Anbringungs- beziehungsweise Hinterlegungsorte mit mir

entsprechend abgestimmt worden, sodass seitdem von einer vollständigen DSGVO-konformen Kennzeichnung der Videoüberwachung in diesen vier Hochhäusern ausgegangen werden kann. Zur erforderlichen Kennzeichnung vgl. Tätigkeitsbericht 2019, 3.1.1, Seite 71 ff.

2.2.27 Videoüberwachung in einer Zahnarztpraxis

Gleich zwei Eingaben erreichten mich im Zusammenhang mit einer Videoüberwachung in einer zahnärztlichen Gemeinschaftspraxis. Dort waren insgesamt vier Videokameras im Einsatz, die sowohl den Eingangs- und Empfangsbereich, insbesondere auch die Arbeitsplätze der in der Anmeldung tätigen Mitarbeiter, sowie die Flure und damit die Zugänge zu den Sprechzimmern erfassten. Die Bilder der Kameras konnten bei Kenntnis der entsprechenden Zugangsdaten von den Zahnärzten von jedem beliebigen Internet-PC abgerufen werden. Die Praxisbetreiber gaben an, die Videoüberwachungsanlage diene dem Schutz des Eigentums sowie der Sicherheit des Personals und führten hierzu diverse Einbruchsdiebstähle (Rezepte, Bargeld und medizinisches Gerät) und Einbruchsversuche im gesamten Haus an. Außerdem nannten die Verantwortlichen auch Fälle, in denen bei laufendem Praxisbetrieb plötzlich Fremdpersonen in den Sprechzimmern aufgetaucht seien.

Zur datenschutzrechtlichen Beurteilung der Zulässigkeit der Videoüberwachung war zwischen den Öffnungs- und Schließzeiten der Praxis zu unterscheiden. Nachdem sich außerhalb der Praxiszeiten zulässigerweise keine Personen dort aufhalten dürften, stand nur eine datenschutzrechtliche Bewertung des Kamerabetriebs während der Öffnungszeiten an.

Das Bundesverwaltungsgericht hat sich in seinem Urteil vom 27. März 2019 - 6 C 2/18 - eingehend mit der Zulässigkeit einer Videoüberwachung in einer Zahnarztpraxis beschäftigt. Zwar lag der Entscheidung noch die vor Einführung der Datenschutz-Grundverordnung (DSGVO) geltende Rechtslage zugrunde, jedoch hat sich das Bundesverwaltungsgericht dessen ungeachtet auch mit der zum Entscheidungszeitpunkt bereits anzuwendenden Datenschutz-Grundverordnung auseinandergesetzt und eine Zulässigkeitsbeurteilung nach den ab 25. Mai 2018 anzuwendenden Datenschutzvorschriften vorgenommen.

Mit einer (konkludenten) Einwilligung des Patienten allein durch das Betreten der Zahnarztpraxis und der damit einhergehenden zu vermutenden Kenntnisnahme der Videoüberwachung in den Praxisräumen mittels des an der Eingangstür angebrachten Hinweisschilds lässt sich ein Betrieb der Videokameras jedenfalls nicht rechtfertigen (Art. 6 Abs. 1 Buchst. a DSGVO). Dies auch deshalb, weil die gesetzlichen Informationspflichten unabhängig von der datenschutzrechtlichen Zulässigkeit einer Videoüberwachung bestehen und einer an sich rechtswidrigen Verarbeitung personenbezogener Daten nicht zur Zulässigkeit verhelfen können.

Mithin war die datenschutzrechtliche Bewertung auf der Grundlage des Art. 6 Abs. 1 Buchst. f DSGVO vorzunehmen. Diese Vorschrift regelt konkret, dass die Verarbeitung personenbezogener Daten (Videoüberwachung) nur dann zulässig ist, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt. Diese Zulässigkeitsvoraussetzungen waren in dem konkreten Fall allerdings nicht erfüllt.

Es fehlte einerseits (während der Sprechzeiten) bereits an einem berechtigten Beobachtungsinteresse des Arztes. Zwar lagen mit dem Eigentums- und Mitarbeiterschutz präventive Zwecke vor, die auch als berechtigt anzuerkennen waren. Die Videoüberwachung war wegen ihrer insoweit unstreitigen Präventionswirkung sowie der bestehenden Aufzeichnungsmöglichkeit auch geeignet, einen Teil der genannten Zwecke zu erreichen, das heißt Einbruchs- und Diebstahlsversuche einzudämmen und durch die Aufzeichnungen einen Aufklärungsbeitrag zu leisten. Allerdings dürften derartige Vorkommnisse während der Praxiszeiten wenig wahrscheinlich sein. Andererseits war auch das Erforderlichkeitsgebot verletzt. Es standen eine Reihe milderer, nichtsdestoweniger aber gleichermaßen wirksamer Mittel zum Erreichen des beabsichtigten Zweckes zur Verfügung, beispielsweise die ständige Anwesenheit des Personals an der Rezeption, versetzte Pausen, Installation eines elektrischen Türöffners kombiniert mit einer Klingelkamera, verschließbare und vom Personal jeweils mitzuführende Geldkassette, sichere Aufbewahrungsorte für Rezepte, medizinische Apparaturen und so weiter.

Darüber hinaus begegnete die Videobeobachtung auch überwiegenden schutzwürdigen Interessen der betroffenen Patienten. Diese suchen eine Praxis wegen gesundheitlicher Probleme auf, was sich auch in ihrem Auftreten, gelegentlich sogar in ihrem Aussehen widerspiegelt. Sie haben demzufolge ein zu schützendes Interesse daran, dass ihr Verhalten während des Praxisaufenthalts nicht mittels Videokameras beobachtet oder gar aufgezeichnet sowie im Nachgang für eine – aus Patientensicht – unbestimmte Zeit vorgehalten wird, ohne dass sie die weitere Verwendung und Löschung der Videoaufzeichnungen kontrollieren oder beeinflussen können. Das Betroffeneninteresse wiegt umso schwerer, als die Patienten für die rein präventiv erfolgende Überwachung keinerlei Anlass gegeben haben. Ein bei Zahnarztpraxen etwaig vorhandenes besonderes Sicherheits- beziehungsweise Schadensrisiko, das sich vom allgemeinen abstrakten Lebensrisiko abhebt, besteht bei objektiver Betrachtung nicht. Auch sind (Zahn-)Arztpraxen keine Bereiche, für die ein tatsächlich erhöhtes Gefährdungspotential (wie etwa bei Banken) besteht. Einbrüche oder gar Überfälle sind eine geringfügige Gefahr, zumal sich dagegen Schutzvorkehrungen auch mittels anderer, weniger die schutzwürdigen Interessen Betroffener tangierende Maßnahmen ergreifen lassen. Für eine konkrete Gefährdungslage jedenfalls existierten keine Anhaltspunkte. Auch die im letzten Prüfschritt vorzunehmende Interessenabwägung ging daher zugunsten der Patienten aus.

Für die mit der auf Patienten beziehungsweise praxisfremde Personen gerichteten Videoüberwachung zugleich verbundene Mitarbeiterüberwachung, deren Zulässigkeit insoweit ausschließlich nach § 26 Bundesdatenschutzgesetz zu beurteilen gewesen wäre, gab es ebenfalls keine Rechtfertigung. Vor dem Hintergrund, dass sich die Unzulässigkeit der Videoüberwachung bereits aus Art. 6 Abs. 1 DSGVO ergeben hatte, kam es darauf aber nicht mehr an.

Im Ergebnis war die Videoüberwachung in den Praxisräumen nur außerhalb der Praxiszeiten zulässig. Die Verantwortlichen sind meiner Bewertung gefolgt und haben die Videoüberwachungsanlage nunmehr so eingestellt, dass die Kameras nur bei eingeschalteter Alarmanlage aktiviert sind.

2.2.28 Videokamera im Thai-Massage-Studio

Man stelle sich vor, man ist regelmäßiger Kunde in einem Thai-Massage-Studio und bemerkt beim Verlassen des Studios plötzlich eine innen über der Eingangstür auf die Gewerberäumlichkeit ausgerichtete Kamera. Mit diesem Sachverhalt wandte sich ein Studiobesucher an meine Behörde und bat um eine Überprüfung.

Ich habe mir daraufhin selbst einen Eindruck von den örtlichen Gegebenheiten verschafft. Nach meinen Feststellungen befand sich tatsächlich innen auf einer Ablage über der Eingangstür versteckt neben einem Blumenarrangement eine kleine Videokamera. Das Massagestudio hatte von außen gut einsehbare Schaufenster ohne Sichtschutz sowie eine unverschlossene Eingangstür. Ein Hinweis auf die Videoüberwachung war nicht angebracht.

Die gespeicherten Videos sowie ein Live-Bild der Kamera konnte die Inhaberin orts- beziehungsweise zeitunabhängig auf ihrem Smartphone einsehen. Auch wenn zum Kontrollzeitpunkt die Kamera aufgrund technischer Probleme nicht in Betrieb war, konnte ich mir anhand von Videoaufzeichnungen auf dem Smartphone der Inhaberin einen Überblick über den Erfassungsbereich der Kamera verschaffen. Dieser reichte vom Eingangsbereich bis zur Rezeption und dem Wartebereich. Sogar einige Massage-Liegen waren in dem Video zu erkennen; pikanterweise lief in der mir vorgeführten Sequenz sogar ein leicht bekleideter Herr durch das Bild. Auf Befragen gab die Inhaberin allerdings an, dass es sich dabei um ihren Schwiegersohn handelte.

Von den Erlaubnistatbeständen des Art. 6 Abs. 1 Datenschutz-Grundverordnung (DSGVO) kam vorliegend nur Buchst. f in Betracht. Nach dieser Vorschrift ist eine Videoüberwachung zulässig, soweit die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen.

Als Überwachungsinteresse war mir der Schutz der Mitarbeiterinnen benannt worden, da diese gelegentlich bis 21 Uhr im Studio seien und es speziell in den Abendstunden immer wieder zu Belästigungen in Form von verbalen Äußerungen oder einem Klopfen an die Eingangstüre komme. Grundsätzlich ergab sich daraus ein berechtigtes Überwachungsinteresse, jedoch fehlte es an der dafür notwendigen Erforderlichkeit.

Die Videoüberwachung war nach meiner Beurteilung schon deswegen ungeeignet, einen Beitrag dazu zu leisten, dass Belästigungen oder gar Übergriffe unterbleiben, da es an einem Hinweis auf die Videoüberwachung fehlte, zumal die Kamera für Unbefugte optisch nicht wahrnehmbar war. Die äußere Kennzeichnung einer Videoüberwachung wäre bereits ausreichend gewesen, um einen entsprechenden Abschreckungseffekt zu erzielen. Außerdem hätte die Inhaberin durch Verschließen der Eingangstür oder das Anbringen eines Sichtschutzes in den Schaufenstern und der Zugangstür effektivere Maßnahmen ergreifen können, die ungebetene Gäste hätten fernhalten können. Gleichzeitig hätte dies einen weit weniger starken Eingriff in die Rechte der Besucher – ebenso wie der Mitarbeiterinnen – bedeutet. Letztlich hätte ich auch keine Bedenken dagegen gehabt, wenn nur ein kleiner, räumlich klar begrenzter Bereich zwischen der Eingangstür und dem Empfangstresen videoüberwacht worden wäre, zumal die angestellten Mitarbeiterinnen sich nur für kurze Zeit während des Kassiervorgangs hinter dem Empfangstresen aufhalten.

Die Inhaberin des Studios hat sich schließlich entschieden, die Kamera gleich ganz zu entfernen.

2.2.29 Videoüberwachung der Mitarbeiterbereiche bei einem Autohof

In einem Rasthof waren insgesamt 39 Videokameras betrieben worden, die neben Tankfeld, LKW-Parkplätzen sowie Ein- beziehungsweise Ausfahrt auch nahezu den gesamten auf dem Gelände befindlichen Shop (Kundenbereich und Kassen mit Ein- und Ausgängen sowie den Zählraum) umfassten. Im Shop selbst waren insgesamt zehn Kameras angebracht, wovon wiederum vier direkt auf den Kassenbereich gerichtet waren. Dieser Bereich war offen gestaltet und nicht mit einem durchgehenden Tresen vom restlichen Shop abgetrennt. An den Zugängen des Shops waren Hinweisschilder auf die Videoüberwachung und ergänzende Piktogramme angebracht. Nur der Kassenbereich und die diesen erfassenden Kameras waren Gegenstand einer (Mitarbeiter-)Beschwerde.

Die hinter der Theke tätigen Mitarbeiter wurden gleichzeitig von vier Kameras erfasst, die seitlich und an der rückwärtigen Raumwand positioniert waren. Die Kameras waren so eingestellt, dass sie die hinter dem Tresen befindlichen Arbeitsplätze komplett erfassten. Die dort tätigen Mitarbeiter waren dadurch einem ständigen Überwachungsdruck ausgesetzt, dem sie sich praktisch nicht entziehen konnten.

Von den Erlaubnistatbeständen des Art. 6 Abs. 1 Datenschutz-Grundverordnung (DSGVO) kam vorliegend nur Buchst. f in Betracht. Nach dieser Vorschrift ist eine Videoüberwachung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, soweit die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

Als Überwachungsinteresse waren vom Verantwortlichen der Schutz der Mitarbeiter sowie die Verhinderung und Aufklärung von kriminellen Handlungen (Einbruch, Vandalismus, Tankdiebstahl, Überfall und Betrug) benannt worden. Es gäbe neben monatlich durchschnittlich fünf Delikten auf dem Parkplatz auch in etwa gleich viele Fälle von Tankbetrug. Tankbetrüger führten bei der Konfrontation mit ihrem Vergehen regelmäßig an, dass sie bereits bezahlt hätten. Außerdem sei das Gewerbegebiet, in dem sich der Autohof befinde, ein bekannter Kriminalitäts-Hotspot. Grundsätzlich ist auf Basis dieser Vorfälle und Gegebenheiten ein berechtigtes Überwachungsinteresse nicht zu bestreiten. Fraglos unterliegen Tankstellenbetreiber und deren Mitarbeiter einem erhöhten Risiko, Opfer von Straftaten (insbesondere Raubüberfällen) zu werden.

Für die extensive Videoüberwachung des gesamten Arbeitsbereiches hinter der Theke fehlte es vorliegend aber an der Erforderlichkeit. Die Erforderlichkeit bestimmt sich im Sinne einer Verhältnismäßigkeitsprüfung nach den Merkmalen der Geeignetheit, Erforderlichkeit und Angemessenheit einer Maßnahme. Zwar besteht an Kassen vom Grundsatz her ein allgemein erhöhtes Überfallrisiko. Für den beabsichtigten Zweck, insbesondere den Nachweis eines Tankbetrugs, wäre es allerdings ausreichend gewesen, wenn nur die beiden auf dem Verkaufstresen befindlichen Kassen und das Vorfeld des Verkaufstresens überwacht worden wären. Nur insoweit war die Erforderlichkeit der Videoüberwachung in Anbetracht des Überwachungszwecks gegeben. Die Beschäftigten hätten dann einen Rückzugsbereich zur Verfügung, in dem sie ihren Aufgaben nachgehen könnten, ohne sich dabei ständig im Blickfeld der Kameras zu bewegen. Ihren schutzwürdigen Interessen könnte damit in ausreichender Weise Rechnung getragen werden.

Für eine gezielte Überwachung der Mitarbeiter fehlte es überdies an dem Vorliegen der Voraussetzungen des § 26 Bundesdatenschutzgesetz. In Betracht kam hier vor allem die Videoüberwachung zur Aufklärung von Straftaten durch Mitarbeiter. Derartige Verdachtsmomente hat der Rasthofbetreiber aber gerade nicht vorgetragen – ihm ging es ausweislich der von ihm genannten Zwecke stattdessen um den Schutz seiner Mitarbeiter und um mögliche Straftaten anderer Personen, beispielsweise Kunden.

Im Ergebnis war der Betrieb der Videokameras im Thekenbereich also in weiten Teilen unzulässig. Es fehlte insoweit bereits an der Erforderlichkeit der Aufzeichnung zum Erreichen der verfolgten Zwecke. Ich habe dem Betreiber daher aufgegeben, den gesamten Bereich hinter

dem Tresen mit Ausnahme des unmittelbaren Umfelds der Kassen aus den Erfassungsbereichen der Kameras auszublenden. Bei einem Tankbetrug lässt sich mit der ansonsten lückenlosen Überwachung im Shop sowie des eigentlichen Kassenbereichs zweifelsfrei nachweisen, wer den Shop betreten hat und ob ein Zahlungsvorgang erfolgte. Auch wenn die Identifizierung einer Person durch die zum Schutz vor der Coronavirus-Pandemie verhängte Maskenpflicht erschwert wird, bleiben noch genügend Personenmerkmale übrig, die für eine Identifizierung ausreichen.

Der Betreiber ist meinen Forderungen gefolgt und hat die notwendigen Ausblendungen vorgenommen. Seine Mitarbeiter informierte er mittels eines Aushangs am Schwarzen Brett über den Umfang der Videoüberwachung, insbesondere die konkreten Erfassungsbereiche.

2.2.30 Dashcams und Helmkameras

Mit Dashcams und Helmkameras von (Motorrad- und Fahrradfahrern) bin ich regelmäßig im Rahmen der Bearbeitung von Ordnungswidrigkeitenanzeigen befasst (vgl. 6.4). Bei geringfügigen Verstößen oder Problemen bei der Nachweisführung werden diese Verfahren aber eingestellt und in den Aufsichtsbereich überführt.

Zur rechtlichen Bewertung der Zulässigkeit des Dashcam-Betriebs ist Folgendes auszuführen:

Die für den Betrieb einer Dashcam als einer Form der Videoüberwachung einzig in Frage kommende Zulässigkeitsvorschrift ist Art. 6 Abs. 1 Buchst. f Datenschutz-Grundverordnung (DSGVO). Diese Vorschrift regelt konkret, dass die Verarbeitung, mithin der Betrieb einer Dashcam einschließlich der Speicherung von Videoaufnahmen, nur dann zulässig ist, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

Zunächst ist zu prüfen, ob der Anwendungsbereich der Datenschutz-Grundverordnung eröffnet ist. Nach Art. 2 Abs. 1 DSGVO gilt die Verordnung für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

Die mittels einer Dashcam erstellten Aufnahmen enthalten personenbezogene Daten im Sinne des Art. 4 Nr. 1 DSGVO, denn Videoaufnahmen von Personen stellen unzweifelhaft Informationen, zum Beispiel Körperbau, Fahrverhalten, Aufenthaltsort, genutzte Fahrzeuge, Bekleidung, Äußerungen, über diese natürlichen Personen dar. Diese Personen sind auch identifizierbar, entweder über ihr Aussehen (Gesichter), über die von ihnen genutzten Fahrzeuge

(beispielsweise Kennzeichen, Werbe- oder Firmenaufschriften), über (bei aktiviertem Mikrofon) ihre Stimme, die Gesprächsinhalte oder über das berufliche oder private Umfeld des Dashcam-Betreibers. Mit einer Dashcam werden personenbezogene Daten anderer Verkehrsteilnehmer verarbeitet. Verarbeitung ist nach Art. 4 Nr. 2 DSGVO jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, oder die Speicherung. Die auf dem Speichermedium einer Dashcam enthaltenen Videoaufzeichnungen sind das Ergebnis einer solchen Erhebung und Speicherung. Der Betrieb einer Dashcam stellt insbesondere auch eine automatisierte Verarbeitung personenbezogener Daten dar (vgl. Europäischer Gerichtshof, Urteil vom 11.12.2014, C-212/13, Leitsatz 2, juris).

Zudem handelt ein Dashcam-Betreiber, wenn er den öffentlichen Verkehrsraum überwacht, regelmäßig nicht ausschließlich für persönliche oder familiäre Tätigkeiten, das heißt, die Ausnahme des Art. 2 Abs. 2 Buchst. c DSGVO (Haushaltsprivileg) greift an dieser Stelle regelmäßig nicht, wenn als Ziel eines Dashcam-Einsatzes vorgesehen ist, für verschiedene Zwecke (vor allem im Zusammenhang mit Verkehrsunfällen) Beweismittel zu sichern. Auch für gegebenenfalls mit der Dashcam zugleich angefertigte Gesprächsaufzeichnungen gilt: Wenn über die Freisprechanlage geführte Telefonate oder im Fahrzeug geführte Gespräche aufgezeichnet werden, ist dies – mit Ausnahme der mit Familienmitgliedern geführten Unterhaltungen – zweifelsfrei nicht mehr dem persönlichen oder familiären Bereich zuzuordnen.

Etwas anderes kann möglicherweise bei durch Fahrrad- oder Motorradfahrer eingesetzten Actioncams (meist Helmkameras) gelten. Soweit die Kameras in diesen Fällen erkennbar mit der Zielrichtung der Dokumentation einer gemeinsamen Unternehmung (Motorradausfahrt oder Radtour) und/oder einer landschaftlich besonders reizvollen Streckenführung eingesetzt werden und die dabei vordergründig erfassten Personen erkennbar an den Aufnahmen mitwirken, wird man sich auch nach meiner Auffassung erfolgreich auf das Haushaltsprivileg berufen und dies hier zulässigerweise auch auf Freunde und Bekannte ausdehnen können. Nicht darauf beziehen können sich aber Dashcam-Nutzer, die ihre Kamera regelmäßig, also ohne solch einen besonderen Anlass – das könnte bei Kraftfahrzeugen beispielsweise auch ein Hochzeitskorso sein –, auf ihren täglichen Fahrten einsetzen.

Ist die Anwendbarkeit der Datenschutz-Grundverordnung geklärt, muss der Dashcam-Betrieb an der eingangs genannten Vorschrift des Art. 6 Abs. 1 Buchst. f DSGVO gemessen werden. Soweit der Verantwortliche mit dem Betrieb der Dashcam sein Eigentum schützen und Beweise sichern will, überwiegen die schutzwürdigen Interessen der unbeteiligten, sich verkehrsgerecht verhaltenden Passanten und Fahrzeugführer, nicht anlasslos und heimlich durch Privatpersonen auf öffentlichem Grund überwacht zu werden. Mit der heimlichen Videoüberwachung wird in schwerwiegender Weise in das Recht auf informationelle Selbstbestimmung der anderen Verkehrsteilnehmer eingegriffen. Diese sind auf die Nutzung von Gehweg und Straße angewiesen und werden – ohne hierfür einen Anlass oder Grund gegeben zu haben – vom Dashcam-Betreiber unter Generalverdacht gestellt und mittels Videokamera überwacht. Die

Speicherung der Videoaufnahmen birgt ein erhebliches Missbrauchspotential, da sie über das Internet praktisch grenzenlos verbreitet werden können. Allein der Dashcam-Betreiber hat es in der Hand zu entscheiden, wann und wie lange er ohne Wissen der anderen Verkehrsteilnehmer Aufnahmen anfertigt und wie er diese weiter verwendet.

Auch für eine gegebenenfalls erfolgende Audioaufzeichnung der geführten Gespräche ist keine Rechtsgrundlage ersichtlich. In Bezug auf den regelmäßig verfolgten Zweck der Beweissicherung bei Verkehrsunfällen fehlt es schon an der Erforderlichkeit für die Aufzeichnung von im oder neben dem Fahrzeug geführten Gesprächen. Art. 6 Abs. 1 Buchst. f DSGVO scheidet also auch hier als Rechtsgrundlage aus. Der Bundesgerichtshof, Urteil vom 15. Mai 2018, VI ZR 233/17, hat diesbezüglich klar zum Ausdruck gebracht, dass das Grundgesetz davor schützt, dass Gespräche heimlich aufgenommen werden und heimliche Tonaufnahmen (nicht in der Öffentlichkeit geführter Gespräche) noch wesentlich stärker in das Persönlichkeitsrecht der betroffenen Personen eingreifen als schon heimliche Bildaufnahmen der (sich bewusst in der Öffentlichkeit bewegenden) Verkehrsteilnehmer. Das Recht am gesprochenen Wort gewährleistet die Selbstbestimmung über die eigene Darstellung der Person in der Kommunikation mit anderen. Dieses Selbstbestimmungsrecht findet einen Ausdruck in der Befugnis des Menschen, selbst und allein zu entscheiden, ob sein Wort auf einen Tonträger aufgenommen und damit möglicherweise Dritten zugänglich werden soll, womit Wort und Stimme von dem Kommunikationsteilnehmer losgelöst und in einer für Dritte verfügbaren Gestalt verselbstständigt werden. Nach § 201 Abs. 1 Nr. 1 Strafgesetzbuch ist damit sogar ein Straftatbestand erfüllt; regelmäßig fehlt es insoweit – mangels Kenntnis der betroffenen Personen – lediglich an diesbezüglichen Strafanträgen.

Im Übrigen ist festzuhalten, dass die Frage der zivil- beziehungsweise strafrechtlichen Beweisverwertung strikt von der datenschutzrechtlichen Zulässigkeit zu trennen ist. Wenn Zivil- und Strafgerichte im Einzelfall mit Dashcams erstellte Videoaufzeichnungen als Beweismittel anerkennen, lassen sie regelmäßig die datenschutzrechtliche Zulässigkeit des Einsatzes der Dashcams offen und setzten sich allein mit der Frage auseinander, ob aus einer datenschutzrechtlichen Unzulässigkeit des Betriebs der Dashcams ein sogenanntes Beweisverwertungsverbot im konkreten Zivil- oder Strafverfahren folgt. Die stattdessen konkret mit der Frage der datenschutzrechtlichen Zulässigkeit des Betriebs von Dashcams befassten Verwaltungsgerichte haben hingegen klar bestätigt, dass der Einsatz von Dashcams durch Private im öffentlichen Straßenverkehr datenschutzwidrig ist.

In diesem Sinne ist auch das bereits erwähnte Urteil des Bundesgerichtshofs vom 15. Mai 2018 zu verstehen. Einerseits hat der Bundesgerichtshof entschieden, dass Dashcam-Aufnahmen unter gewissen Voraussetzungen als Beweismittel bei Unfall-Prozessen verwertbar sind. Andererseits hat er aber klar festgestellt, dass die im Verfahren vorgelegte Videoaufzeichnung nach den geltenden datenschutzrechtlichen Bestimmungen unzulässig ist. Sie verstoße gegen § 4 Bundesdatenschutzgesetz (BDSG), da sie ohne Einwilligung der Betroffenen erfolgt sei und nicht auf § 6b Abs. 1 BDSG alter Fassung oder § 28 Abs. 1 BDSG alter Fassung hatte

gestützt werden können. Jedenfalls eine permanente anlasslose Aufzeichnung des gesamten Geschehens auf und entlang der Fahrstrecke des Klägers sei zur Wahrnehmung seiner Beweissicherungsinteressen nicht erforderlich, denn es sei technisch möglich, eine kurze, anlassbezogene Aufzeichnung unmittelbar des Unfallgeschehens zu gestalten, beispielsweise durch ein dauerndes Überschreiben der Aufzeichnungen in kurzen Abständen und Auslösen der dauerhaften Speicherung erst bei Kollision oder starker Verzögerung des Fahrzeuges. Inzwischen hat die Datenschutz-Grundverordnung zwar die vom Bundesgerichtshof herangezogenen Vorschriften des Bundesdatenschutzgesetzes abgelöst, jedoch ändert dies nichts an der grundsätzlichen rechtlichen Bewertung, denn Art. 6 Abs. 1 Buchst. f DSGVO schreibt eine vergleichbare Interessenabwägung vor, wie zuvor bereits § 6b BDSG alter Fassung.

Im Ergebnis ist der Einsatz einer Dashcam nur dann als datenschutzkonform zu bewerten, wenn sichergestellt ist, dass damit gefertigte Videoaufzeichnungen – ohne ein eine längere Speicherung rechtfertigendes Ereignis – nach kurzer Zeit; mithin nach maximal drei bis fünf Minuten, wieder gelöscht werden. Tatsächlich sind aktuell noch sehr wenige Dashcams auf dem Markt, die tatsächlich die Einstellung einer solch eng bemessenen Loop-Schleife ermöglichen. Meist erfolgt ein Überschreiben älterer Aufnahmen erst, wenn die Kapazitätsgrenze der eingesetzten Speicherkarte erreicht ist. Dies bedeutet aber zugleich, dass dann regelmäßig schon mehrere Stunden rechtswidrig Videoaufzeichnungen auf der Karte enthalten sind. Wer eine solche Kamera im Straßenverkehr einsetzt, läuft Gefahr, einem Bußgeldverfahren ausgesetzt zu werden. Wer also an dieser Stelle – Billigangebote gibt es viele – beim Erwerb einer Dashcam spart, für den kann es später teuer werden (vgl. 6.4). Dies gilt darüber hinaus immer auch dann, wenn Fahrzeugführer die Mikrofonfunktion der Dashcam aktiviert haben.

2.3 Einwilligungsfragen

2.3.1 Widerruf von gegenüber Kommunen erteilten Einwilligungen

Ein benannter Datenschutzbeauftragter bat mich um Unterstützung bei der Löschung personenbezogener Daten im Zusammenhang mit dem Widerruf von Einwilligungen.

Problematisch sei das nach seiner Darstellung, wenn beispielsweise auf der Grundlage einer Einwilligung Fotos bei den Jubilarenfeiern der Freiwilligen Feuerwehr angefertigt, in einer Broschüre zum Druck gegeben und dann an die Teilnehmer verteilt wurden.

In Art. 17 Abs. 1 Buchst. b Datenschutz-Grundverordnung (DSGVO) heißt es: „Der Verantwortliche ist verpflichtet, personenbezogene Daten unverzüglich zu löschen, sofern einer der folgenden Gründe zutrifft: […] Die betroffene Person widerruft ihre Einwilligung, auf die sich die Verarbeitung […] stützte, und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung.“ Mit Verweis darauf stellte der Datenschutzbeauftragte folgende Fragen:

- Müssen alle Mitglieder, welche die Broschüre erhalten haben, aufgefordert werden, die namentliche Erwähnung des Betroffenen zu schwärzen und ihn auch auf allen Fotos unkenntlich machen?
- Ist das gleiche im Internetangebot der Freiwilligen Feuerwehr durchführen?
- Was passiert mit den noch verbleibenden Broschüren?

Ich habe ihn dazu auf Folgendes hingewiesen: Zunächst betrifft die Löschpflicht nur den Verantwortlichen. Wenn die Broschüren bereits verteilt worden sind, ist er hinsichtlich dieser nicht mehr Verantwortlicher. Auch war die vorherige Übermittlung wegen der noch nicht widerrufenen Einwilligung rechtmäßig. Zwar kann der Betroffene nach Art. 7 Abs. 3 DSGVO die Einwilligung jederzeit widerrufen, aber „durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt“. Es lag und liegt weiterhin somit eine „anderweitige Rechtsgrundlage für die Verarbeitung“ im Sinne des Art. 17 Abs. 1 Buchst. b DSGVO vor.

Sofern aber, wie durch den Datenschutzbeauftragten weiter geschildert wurde, Broschüren noch nicht verteilt wurden beziehungsweise diese parallel auch im Internetangebot der Freiwilligen Feuerwehr (im passwortgeschützten Bereich) den Mitgliedern zur Verfügung gestellt werden, müssten diese entweder gelöscht/vernichtet oder beispielsweise durch Schwärzung bearbeitet werden.

Gleiches gilt hinsichtlich der ebenfalls angefragten Portfolios von Kindern, welche von Kindertagesstätten angefertigt (und auch vom sächsischen Bildungsplan empfohlen) werden.

2.3.2 LernSax – die sächsische Schulcloud

Während der pandemiebedingten Schulschließungen nutzte ein Großteil der sächsischen Schüler LernSax, die vom Landesamt für Schule und Bildung zur Verfügung gestellte internetbasierte Plattform für Kommunikation und Kooperation. Bei deren Konzeption war ich von Anfang an beteiligt. Zunächst war LernSax ein freiwilliges Angebot, das an teilnehmenden Schulen von interessierten Schülern nur mit deren Einwilligung genutzt werden konnte. Dieses Konzept der Freiwilligkeit wurde mit den sich abzeichnenden Schulschließungen durch das Sächsische Staatsministerium für Kultus (SMK) auf den Prüfstand gestellt. Es hätte dazu geführt, dass bei nicht einwilligenden Schülern (beziehungsweise deren Personensorgeberechtigten) eine Unterrichtsteilnahme bei der Entscheidung einer Schule für LernSax faktisch nicht möglich gewesen wäre.

Ich habe mich daher der Auffassung des SMK angeschlossen, dass die schulinterne elektronische Kommunikation zwischen Lehrern und Schülern vom Erziehungs- und Bildungsauftrag nach § 1 SächsSchulG erfasst ist und daher keiner weiteren Einwilligung bedarf, sofern diese nicht außerhalb eines pädagogischen Kontextes oder mit Dritten erfolgt.

Einwilligungsfrei ist die Nutzung von LernSax jedoch nur für unmittelbare Unterrichtszwecke durch Schüler und deren Lehrkräfte. Sofern eine Kommunikation mit Dritten außerhalb des pädagogischen Kontextes erfolgen soll, ist daher ebenso vorab eine Einwilligung einzuholen, wie bei der Nutzung von LernSax durch Personensorgeberechtigte oder externe Bildungspartner.

Auf diese Rahmenbedingungen wird auch unter lernsax.de hingewiesen.

2.3.3 Erhebung von Gesundheitsdaten von Beschäftigten in der Coronavirus-Pandemie

Im Frühjahr des letzten Jahres erhielt ich eine Beschwerde über die Erhebung von Gesundheitsdaten von Beschäftigten einer Behörde sowie der mit diesen Beschäftigten in einem Haushalt lebenden Angehörigen.

Die Beschäftigten der Behörde wurden per E-Mail aufgefordert bis zu einem Stichtag Gesundheitsdaten in Bezug auf chronische Vorerkrankungen von ihnen selbst und auch von Angehörigen, die mit ihnen in einem Haushalt zusammenleben, anzugeben, die auf ein Risiko einer Covid-19-Erkrankung hindeuten. Dabei sollten die Fragen jeweils mit „Ja“ oder „Nein“ beantwortet werden. Die Behörde wollte diese Angaben zur Berücksichtigung individueller Belange der Beschäftigten bei der Wiederaufnahme des regulären Dienstbetriebes nach der Corona-Pandemie verwenden.

Nach § 11 Abs. 1 Sächsisches Datenschutzdurchführungsgesetz (SächsDSDG) dürfen öffentliche Stellen personenbezogene Daten, einschließlich Daten im Sinne des Art. 9 Abs. 1 Datenschutz-Grundverordnung (DSGVO) von Beschäftigten verarbeiten, soweit dies zur Durchführung des Dienst- oder Arbeitsverhältnisses oder zur Durchführung organisatorischer, personeller und sozialer Maßnahmen, insbesondere auch zu Zwecken der Personalplanung und des Personaleinsatzes erforderlich ist oder eine Rechtsvorschrift, ein Tarifvertrag oder eine Dienst- oder Betriebsvereinbarung dies vorsieht. Bei der Verarbeitung von personenbezogenen Daten im Sinne des Art. 9 Abs. 1 DSGVO sind angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person vorzusehen (§ 11 Abs. 2 Satz 1 SächsDSDG).

Die Behörde fragte die Beschäftigten per E-Mail, ob der Beschäftigte oder eine Person, die mit ihm in einem Haushalt lebt, eine chronische Vorerkrankung hat, durch die er bei einer Covid-19-Erkrankung einem erheblichen Gesundheitsrisiko ausgesetzt ist. Es handelt sich dabei um Gesundheitsdaten nach Art. 9 in Verbindung mit Art. 4 Nr. 15 DSGVO, da sich die abgefragte Angabe auf die körperliche Gesundheit einer natürlichen Person, hier des Beschäftigten sowie der mit ihm in einem Haushalt lebenden Personen bezieht beziehungsweise aus denen Informationen über den Gesundheitszustand des einzelnen Beschäftigten beziehungsweise der

Personen, die mit ihm in einem Haushalt leben, hervorgehen. Diese Abfrage per E-Mail stellt eine Datenverarbeitung im Sinne des Art. 4 Nr. 2 DSGVO dar.

Diese Datenverarbeitung ist weder zur Durchführung des Beschäftigtenverhältnisses noch zur Durchführung organisatorischer, personeller und sozialer Maßnahmen, insbesondere auch zu Zwecken der Personalplanung und des Personaleinsatzes, nach § 11 Abs. 1 Satz 1 SächsDSDG erforderlich.

Im Rahmen der Erforderlichkeitsprüfung sind die widerstreitenden Grundrechtspositionen zur Herstellung praktischer Konkordanz abzuwägen. Es sind dabei die Interessen des Arbeitgebers an der Datenverarbeitung und das Persönlichkeitsrecht des Beschäftigten zu einem Ausgleich zu bringen, so dass möglichst beide Interessen so weit wie möglich berücksichtigt werden. Um erforderlich zu sein, muss die vorgenannte Datenverarbeitung den in § 11 Abs. 1 Satz 1 SächsDSDG genannten legitimen Zielen dienen, geeignet, erforderlich im engeren Sinne und angemessen sein.

Geeignet ist die Datenverarbeitung, wenn sie dazu beiträgt, das legitime Ziel zu erreichen. Ziel der Behörde war es, bei der Wiederaufnahme des Dienstbetriebes die individuellen Belange der Beschäftigten, die selbst chronische Erkrankungen haben und/oder Angehörige des Beschäftigten, die mit ihm in einem Haushalt leben und chronische Vorerkrankungen haben, durch die sie bei einer COVID-19-Erkrankung einem erheblichen Gesundheitsrisiko ausgesetzt sind, zu berücksichtigen.

Erhebliche Zweifel bestanden bereits, ob die pauschale Abfrage überhaupt geeignet war, das vorgenannte Ziel zu erreichen. Insbesondere war unklar, welche Vorerkrankungen überhaupt zu einem erheblichen Gesundheitsrisiko führen. Selbst das Robert Koch-Institut (RKI) führte auf seiner Website rki.de unter „Informationen und Hilfestellungen für Personen mit einem höheren Risiko für einen schweren COVID-19-Krankheitsverlauf“ (Stand: 13. Mai 2020) auf, dass aufgrund verschiedenster Einflüsse wie Vorerkrankungen, Alter, Adipositas, Rauchen und deren Kombinationsmöglichkeiten die Risikoeinschätzung sehr komplex sei und daher eine generelle Festlegung zur Einstufung in eine Risikogruppe nicht möglich sei. Laut RKI sei vielmehr eine individuelle Risikofaktoren-Bewertung im Sinne einer (arbeits-)medizinischen Begutachtung erforderlich.

Erforderlich im engeren Sinne ist eine Datenverarbeitung, wenn kein gleich geeignetes, milderes Mittel zur Verfügung steht. Wie bereits ausgeführt, sah das RKI auf seiner Website eine (arbeits-)medizinische Begutachtung als das geeignetere Mittel, die individuellen Risikofaktoren zu bewerten, an. Dies ist für die Beschäftigten aus datenschutzrechtlicher Sicht auch weniger eingriffsintensiv, da der Beschäftigte seine Vorerkrankungen nicht dem Arbeitgeber sondern dem Betriebsarzt mitteilt. Durch die ärztliche Schweigepflicht sind die Gesundheitsdaten vor dem Zugriff des Arbeitgebers, gegebenenfalls auch der Verwendung zu anderen Zwecken,

besonders geschützt. Zum anderen sind den SARS-CoV-2-Arbeitsschutzstandards des Bundesministeriums für Arbeit und Soziales (Stand: 16. April 2020) Arbeitsschutzmaßnahmen zu entnehmen, die der Arbeitgeber zum Schutz seiner Beschäftigten ergreifen sollte. Durch diese Maßnahmen konnte in geeigneter Weise auf die individuellen Belange von Mitarbeitern, die einer erhöhten COVID-19-Erkrankung ausgesetzt waren, eingegangen werden und diese sind gegenüber der Mitteilung, dass der Beschäftigte und/oder Personen, die mit ihm in einem Haushalt leben, eine chronische Vorerkrankung hat/haben, ein milderes Mittel.

Die Verarbeitung von Gesundheitsdaten ist auch nicht mittels Einwilligung nach Art. 9 Abs. 2 Buchst. a DSGVO gerechtfertigt.

Eine Einwilligung im Sinne des Art. 9 Abs. 2 Buchst. a DSGVO kann nur wirksam erteilt werden, wenn die betroffene Person in die Verarbeitung der Gesundheitsdaten für einen oder mehrere festgelegte Zwecke ausdrücklich eingewilligt hat und die Voraussetzungen von Art. 4 Nr. 11 und Art. 7 DSGVO erfüllt sind (vgl. Datenschutzkonferenz, Kurzpapier Nr. 20, Einwilligung nach der DSGVO, abrufbar auf datenschutzkonferenz-online.de; Europäischer Datenschutzausschuss, WP 259 rev. 01: Leitlinien in Bezug auf die Einwilligung gemäß Verordnung EU 2016/679; Tätigkeitsbericht 2019, 2.3.1, Seite 57 f.).

Die an die Beschäftigten gerichtete E-Mail enthielt bereits keine Belehrung über die jederzeitige Widerrufsmöglichkeit.

Zum anderen fehlte es an der Freiwilligkeit der Einwilligungserklärung. Aufgrund der bestehenden Abhängigkeiten im Beschäftigungsverhältnis sind besondere Anforderungen im Hinblick auf die Beurteilung der Freiwilligkeit zu stellen. Dies gilt insbesondere im Hinblick auf die Umstände, unter denen die Einwilligung erteilt worden ist und dass es sich um besonders sensible Daten (Gesundheitsdaten) handelt.

In der E-Mail an die Beschäftigten wurde darauf hingewiesen, dass der Fragebogen innerhalb einer Frist von wenigen Tagen zurückzusenden ist und danach eingehende Rückmeldungen voraussichtlich nicht mehr berücksichtigt werden können.

Die Beschäftigten mussten daher davon ausgehen, dass bei einer Nichtangabe beziehungsweise fehlender Rückmeldung keine weiteren beziehungsweise speziellen Vorkehrungen zum Schutz vor Covid-19 durch die Behörde getroffen werden würden. Vor diesem Hintergrund war nicht von einer freiwilligen Angabe der Gesundheitsdaten auszugehen.

Im Übrigen stellte dies auch einen Verstoß zu dem grundsätzlichen Koppelungsverbot im Sinne des Art. 7 Abs. 4 DSGVO dar. Denn letztlich koppelt der Arbeitgeber die Berücksichtigung individueller Belange bei der Wideraufnahme des Dienstbetriebes an die Angabe von Gesundheitsdaten durch den jeweiligen Beschäftigten, obgleich es, ausweislich des SARS-

CoV-2-Arbeitsschutzstandards des Bundesministeriums für Arbeit und Soziales, andere Möglichkeiten gäbe, diese dennoch zu berücksichtigen.

Aufgrund meines Tätigwerdens wurden sämtliche Daten, die mittels des Fragebogens erhoben wurden, gelöscht. Ich habe die Behörde nach Art. 58 Abs. 1 Buchst. d DSGVO darauf hingewiesen, dass personenbezogene Daten, insbesondere Gesundheitsdaten von Beschäftigten, nur verarbeitet werden dürfen, soweit dies zur Durchführung des Dienst- oder Arbeitsverhältnisses oder zur Durchführung organisatorischer, personeller oder sozialer Maßnahmen, insbesondere auch zu Zwecken der Personalplanung und des Personaleinsatzes, erforderlich ist und bei der Verarbeitung von Gesundheitsdaten zusätzlich angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person vorzusehen sind.

2.3.4 Die obligatorische Einwilligung zur Werbung auf einem Einkaufsportal

Nicht jedes Bemühen, Klarheit herzustellen, gelingt. Damit vertraglich gebundene Kunden sich nicht über spätere E-Mail-Werbung wundern mögen, sondern deren grundsätzliche Zulässigkeit bereits an prominenter Stelle mitgeteilt würde, hatte ein Online-Portal einen Pflicht-Button eingestellt, der lautete: „Ich bin jederzeit widerruflich damit einverstanden, …“ Bei Nichtbestätigung war allerdings technisch eine Online-Bestellung nicht mehr durchführbar. Die Beschwerdeführerin vermutete hierdurch einen Verstoß gegen das Koppelungsverbot nach Art. 7 Abs. 4 Datenschutz-Grundverordnung (vgl. auch Erwägungsgrund 43 der Verordnung).

Die mir von dem Verantwortlichen plausibel erläuterte Zweckbestimmung der Erklärung bestand jedoch mitnichten darin, die bereits gesetzlich bestehende durch Vertrag entstandene Verarbeitungsgrundlage zusätzlich mit einer Einwilligung abzusichern. Das Zustimmungsfeld, das im Ergebnis zu Recht bemängelt worden war, habe keiner Einwilligung gedient, sondern lediglich einer beweisfesten Bestätigung der Kenntnisnahme der bereits gesetzlich geltenden Bestimmungen. Es sollte nach Angaben des Verantwortlichen der Werbewiderspruch bei der ersten Ansprache an den Kunden auch keineswegs unterbunden werden. Bei nur oberflächlichem Verständnis der Klausel war allerdings zu erwarten, dass das Portal nutzende Kunden nicht imstande sein würden, sich entsprechendes zu erschließen.

Die Abweichung vom Standard digitaler Geschäftsbedingungen ist auf mein Betreiben hin allerdings rasch korrigiert worden.

2.3.5 Vorteile gegen Daten – Werbeansprache oder sonstige Datennutzung als Vertragsgegenstand

Das ordnungspolitische Wirken meiner Behörde hat nach meiner Überzeugung auch den Willen an der Datenverarbeitung beteiligte Gruppen und die Privatautonomie zu berücksichtigen.

Auch in datenschutzrechtlichen Fragen ist allerdings eine Entwicklung zu beobachten, die Freiheit des Einzelnen wohlfahrtsrhetorisch einzuhegen. Art. 7 Abs. 4 und Erwägungsgrund 43 der Datenschutz-Grundverordnung (DSGVO) scheinen diese Tendenz im Bereich der Werbung zu verstärken, da sie die Preisgabe von Daten Betroffener im Wege der Freiwilligkeit zu erschweren scheinen. Nicht jedoch bei vollständiger Betrachtung. Es mag zur Bodenhaftung beitragen, sich die Datenschutz-Grundverordnung in Gänze zu Gemüte zu führen, inklusive Art. 1 Abs. 3: „Der freie Verkehr personenbezogener Daten in der Union darf aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten weder eingeschränkt noch verboten werden.“ In Deutschland materialisiert sich diese Freiheit grundgesetzlich auch im Rechtsinstitut der Vertragsfreiheit. In diesem Sinn hat 2019 auch ein Oberlandesgericht entschieden, dass, wenn personenbezogene Daten einen Wert haben (was zum Erlass der Datenschutz-Grundverordnung beigetragen hat), deren Verwendung seitens der betroffenen Person gegenüber einem Unternehmen nicht gehindert sein kann (vgl. Oberlandesgericht Frankfurt vom 27. Juni 2019 - 6 U 6/19, Leitspruch und Rdnr. 18.; vgl. zudem Tätigkeitsbericht 2019, 2.3.5., Seite 62 ff.).

Soll die Inkaufnahme von Werbeansprachen mit Waren oder geldwerten Leistungen entgolten werden, bedarf es dazu keinerlei datenschutzrechtlicher Einwilligung. Erforderlich ist der gemeinsame Wille beider Parteien zum Geschäftsabschluss unter definierten Bedingungen. Aber: Nur die im Vorfeld mit unmissverständlicher Klarheit geführte Einigung mit entsprechenden Willenserklärungen macht die Erforderlichkeit einer Einwilligung zur Datenverarbeitung gemäß Art. 7 DSGVO obsolet. Das Kern-Geschäft kann dann auf Art. 6 Abs. 1 DSGVO gestützt werden. Und die integrale Gegenleistung des datenschutzrechtlich Betroffenen kann insoweit auch in der Hinnahme ihn erreichender Werbeansprachen bestehen.

2.3.6 Einwilligungsformulare von Versicherungsmaklern

Mehrere Beschwerden im Berichtszeitraum zeigten auf, dass verschiedene Versicherungsmakler einheitliche Einwilligungsformulare für sämtliche Versicherungsarten verwendeten. Danach waren auch bei Kfz- beziehungsweise Gebäudeversicherungen et cetera pauschal neben weiteren Daten sensible Gesundheitsdaten von der Einwilligung in die Datenverarbeitung mit umfasst.

Eine derartig weite Einwilligungserklärung ist wegen Verstoßes gegen das Gebot der Erforderlichkeit nach § 7 Abs. 4 Datenschutz-Grundverordnung (DSGVO) unwirksam. Denn ein Grundsatz des Datenschutzrechts ist die Beschränkung der Datenverarbeitung auf den für den konkreten Zweck erforderlichen Umfang (vgl. Art. 5 Abs. 1 Buchst. c DSGVO (Datenminimierung)).

Daneben dürften entsprechende Klauseln auch nach §§ § 305c Abs. 1 BGB, 306 Bürgerliches Gesetzbuch (BGB) unwirksam sein. Danach sind überraschende und unklare Klauseln in Allgemeinen Geschäftsbedingungen (AGB) unwirksam; um solche handelt es sich hier regelmäßig.

Derartige den konkreten Vertragszweck überschießende Verarbeitungen können selbstverständlich auch nicht wirksam als Bestandteil eines Vertrags vereinbart werden. Für die AGB-Vorschriften des BGB folgt dies schon aus dem Geltungsbereich der Normen, für die Datenschutz-Grundverordnung aus Art. 6 Abs. 1 Buchst. b DSGVO aus der dort ausdrücklich vorausgesetzten Erforderlichkeit der Verarbeitung für den Vertrag.

Durch entsprechende Hinweise an die Verantwortlichen konnte ich in allen Fällen entsprechende Klarstellungen in den Formularen beziehungsweise die Verwendung an den jeweiligen Vertragszweck angepasster Formulare bewirken. Die Datenschutzkonformität entsprechender Einwilligungsformulare vermindert entsprechende Risiken aus darauf aufbauenden Datenverarbeitungen und wirkt mangelhaftem Datenschutzbewusstsein der Verantwortlichen entgegen. Vor dem Hintergrund der umfassenden Kooperationsbereitschaft der Verantwortlichen wurde von der Verfolgung der abgestellten Verstöße abgesehen, zumal ein Vorsatz nicht feststellbar war, und plausibel dargelegt wurde, dass keine entsprechenden rechtswidrigen Datenverarbeitungen stattgefunden hätten.

2.4 Sensible Daten, besondere Kategorien personenbezogener Daten

2.4.1 Datenschutzfreundliche Erhebung von Gesundheitsdaten bei Beschäftigten

Eine angestellte Lehrerin einer öffentlichen Schule in Sachsen hat sich wegen der Erhebung von Gesundheitsdaten an mich gewandt. Nach einem unverschuldeten Unfall und darauf folgender Arbeitsunfähigkeit sollte sie ein Formular (Meldebogen für drittverschuldete Ereignisse) über eine Unfallmeldung ausfüllen, mit welchem unter anderem ärztliche Diagnosen erhoben werden. Dieses Formular sollte – über die personalverwaltende Stelle – an das Landesamt für Steuern und Finanzen gesandt werden. Auch die Schule an der sie tätig ist, wollte das von ihr ausgefüllte Formular speichern.

Im Falle von Unfällen von Arbeitnehmern, die durch Dritte verursacht wurden, steht dem Arbeitnehmer gegebenenfalls ein Anspruch auf Schadensersatz wegen des Verdienstausfalles zu, der dem Arbeitnehmer durch die Arbeitsunfähigkeit entstanden ist gegenüber dem Dritten/Unfallverursacher zu. Dieser Anspruch auf Schadensersatz gegenüber dem Dritten/Unfallverursacher geht per Gesetz auf den Arbeitgeber über, soweit dieser an den Arbeitnehmer Lohnfortzahlung geleistet hat (vgl. § 6 Abs. 1 Entgeltfortzahlungsgesetz).

Gemäß § 6 Abs. 3 Entgeltfortzahlungsgesetz hat der Arbeitnehmer dem Arbeitgeber unverzüglich die zur Geltendmachung des Schadensersatzanspruchs erforderlichen Angaben zu machen. Aufgrund dieser gesetzlichen Regelungen ist der Arbeitgeber daher grundsätzlich berechtigt diese Daten, welche auch Gesundheitsdaten erfassen, vom Arbeitnehmer zu verlangen beziehungsweise diese zu verarbeiten. Für verbeamtete Lehrer sieht § 111 Sächsisches Beamtengesetz eine vergleichbare Regelung vor.

Bezüglich der Angaben zu Verletzungsfolgen und Krankenhausaufenthalt, die mit dem Formular für drittverschuldete Ereignisse abgefragt werden, handelt es sich um besondere Kategorien von personenbezogenen Daten nach Art. 9, Art. 4 Nr. 15 Datenschutz-Grundverordnung. Bezüglich dieser Daten sind angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person vorzusehen (§ 11 Abs. 2 Satz 1 Sächsisches Datenschutzdurchführungsgesetz (SächsDSDG)). Derzeit ist dieser Meldebogen über die personalverwaltende Stelle, hier dem Landesamt für Schule und Bildung, an das Landesamt für Steuern und Finanzen zuzuleiten, da dieses den oben genannten Schadensersatzanspruch gegenüber dem Unfallverursacher rechtlich geltend macht. Das Landesamt für Schule und Bildung fügt dem vom Arbeitnehmer ausgefüllten Meldebogen eine Kopie der Krankschreibung und die Höhe des Jahresurlaubsanspruches, in der das schädigende Ereignis fiel, bei. Dieses Verfahren habe ich mit der zuständigen Stelle im Landesamt für Steuern und Finanzen besprochen. Mir wurde eine datenschutzfreundlichere Ausgestaltung des beschriebenen Verfahrens im Hinblick auf die nicht erforderliche Kenntnisnahme von Gesundheitsdaten Beschäftigter durch die personalverwaltende Stelle in Aussicht gestellt. Dies werde ich im Rahmen meiner Aufsichtstätigkeit weiter verfolgen.

Bezüglich der Speicherung des Meldebogens für drittverschuldete Unfälle durch die Schule teilte ich ihr mit, dass eine Speicherung der Daten nicht nach § 11 Abs. 1 und 2 SächsDSDG erforderlich ist. Der vorgenannte Forderungsübergang des Schadensersatzanspruches erfolgt nicht auf die einzelne Schule, sondern auf den Freistaat Sachsen. Für die rechtliche Geltendmachung der oben genannten Schadensersatzansprüche ist innerhalb der öffentlichen Staatsverwaltung des Freistaates Sachsen das Landesamt für Steuern und Finanzen beauftragt und gerade nicht die einzelne Schule. Eine Erforderlichkeit zur Speicherung dieser Daten für die Durchführung des Arbeitsverhältnisses oder zur Durchführung organisatorischer, personeller und sozialer Maßnahmen durch die einzelne Schule ist – aufgrund der beschriebenen Zuständigkeit des Landesamtes für Steuern und Finanzen – daher nicht ersichtlich und dementsprechend nicht datenschutzkonform. Auch im Hinblick auf die Daten Dritter, wie zum Beispiel die Daten des Unfallverursachers, ist der Grundsatz der Datenminimierung nach Art. 5 Datenschutz-Grundverordnung zu berücksichtigen.

2.4.2 Erstattung von Gewerkschaftsbeiträgen durch den Arbeitgeber

Im letzten Berichtszeitraum erhielt ich eine Anfrage zum datenschutzkonformen Prozedere bei der Erstattung von Gewerkschaftsbeiträgen durch den Arbeitgeber.

Hintergrund der Anfrage war die Vereinbarung eines neuen Tarifvertrages. Dieser enthielt eine Regelung, wonach der Arbeitgeber verpflichtet sein sollte, jedem Gewerkschaftsmitglied den jährlichen Gewerkschaftsbeitrag zu erstatten.

Zur Umsetzung dieser tarifvertraglichen Regelung im Unternehmen wollte der Arbeitgeber gegen Vorlage einer Bescheinigung der gewerkschaftlichen Unterstützungseinrichtung, die die Gewerkschaftsmitgliedschaft bestätigt, den Gewerkschaftsbeitrag mit der Lohnabrechnung erstatten. Durch die Vorlage der Beitragsbescheinigung würde jedoch gegenüber dem Arbeitgeber die Mitgliedschaft in der Gewerkschaft offengelegt werden. Als ein Ausfluss der Koalitionsfreiheit nach Art. 9 Abs. 3 Grundgesetz ist die Mitgliedschaft in einer Gewerkschaft ein sensibles personenbezogenes Datum, welches einen besonderen Schutz verdient, da im Zusammenhang mit der Verarbeitung erhebliche Risiken für die Grundrechte und Grundfreiheiten auftreten können. Insoweit handelt es sich bei der Angabe um eine sensible Information im Sinne von Art. 9 Abs. 1 Datenschutz-Grundverordnung (DSGVO), deren Verarbeitung nur im Rahmen der engen Grenzen des Art. 9 Abs. 2 DSGVO gestattet ist.

Es handelt sich bei der Vorlage der Mitgliedsbescheinigung und Geltendmachung des tariflichen Anspruches durch den Arbeitnehmer zwar nicht um eine Einwilligungssituation nach Art. 9 Abs. 2 Buchst. a DSGVO, allerdings ist diese Antragssituation einwilligungsähnlich. Der jeweilige Arbeitnehmer kann selbst entscheiden, ob er den Mitgliedsbeitrag erstattet haben möchte und dementsprechend entscheiden, ob er einen Antrag unter Offenlegung der Gewerkschaftsmitgliedschaft stellt oder auf diese Leistung verzichtet.

Zweifel in Bezug auf die Freiwilligkeit der Entscheidung des jeweiligen Arbeitnehmers, insbesondere im Hinblick auf die im Beschäftigungsverhältnis bestehende Abhängigkeit der beschäftigten Person, bestanden in dem Fall nicht, da die Arbeitnehmer einen wirtschaftlichen Vorteil erlangt haben.

Ich habe daher keine datenschutzrechtlichen Bedenken gegen das beschriebene Verfahren zur Erstattung der Gewerkschaftsbeiträge.

3 Betroffenenrechte

3.1 Spezifische Pflichten des Verantwortlichen

3.1.1 Datenschutzinformation nach Art. 13 DSGVO – One-fits-all-Lösung zulässig?

Im Rahmen der Prüfung der Videoüberwachung eines Großvermieters bin ich damit konfrontiert worden, dass sich der Verantwortliche vom Grundsatz her zwar an das von den Aufsichtsbehörden empfohlene zweistufige Informationskonzept (vgl. Tätigkeitsbericht 2019, 3.1.1, Seite 71 ff.) sowie die Orientierungshilfe Videoüberwachung (abrufbar auf datenschutzkonferenz-online.de) gehalten hat, dabei jedoch die vollständige Information in eine Datenschutzinformation auf seiner Website integriert hatte, die praktisch seine gesamte Verarbeitung personenbezogener Daten abdeckte, sich dabei aber vom Umfang her dennoch immer noch auf eine Seite beschränkte.

Ich habe den Verantwortlichen darauf hingewiesen, dass eine einerseits derart allgemein gehaltene und andererseits derart umfassende Datenschutzinformation einen schwerwiegenden Transparenzmangel aufweist und demzufolge nicht mit den Vorschriften der Datenschutz-Grundverordnung (DSGVO) im Einklang steht (Art. 5 Abs. 1 Buchst. a und Art. 12 Abs. 1 DSGVO).

Speziell auf die Videoüberwachung bezogen war für die Adressierten nur sehr eingeschränkt nachvollziehbar, welche der in diesem Informationsblatt enthaltenen Angaben speziell für die Videoüberwachung gelten. Eine solche „One-fits-all“-Architektur, bei der sich der Adressat erst mühsam die für ihn beziehungsweise die für die ihn interessierende Datenverarbeitung möglicherweise geltenden Aussagen heraussuchen muss, genügt nicht den Transparenzanforderungen der Datenschutz-Grundverordnung. Damit erfährt er nicht zuverlässig, welche Datenverarbeitungen durchgeführt und welche Daten unter welchen Umständen an welche Empfänger übermittelt werden. Insbesondere für Nichtmieter, aber dessen ungeachtet natürlich unter Umständen auch von der Videoüberwachung betroffene Personen, enthielt das Informationsblatt eine Vielzahl irrelevanter Informationen.

Ich habe den Vermieter daher zunächst aufgefordert, für die Videoüberwachung ein separates vollständiges Informationsblatt zu erstellen und ihm dabei natürlich empfohlen, sich dazu an dem von den Aufsichtsbehörden empfohlenen Muster zu orientieren.

Meine obige Kritik an der „One-fits-all“-Architektur dieser Datenschutzinformation gilt im Übrigen über die Videoüberwachung hinaus auch in Bezug auf alle anderen Verarbeitungstätigkeiten. Die Informationspflicht nach Art. 13 DSGVO ist verarbeitungsspezifisch zu erfüllen; eine

einzige Datenschutzinformation für alle Verarbeitungstätigkeiten ist für die betroffenen Personen vollkommen intransparent und widerspricht der Vorgabe des Art. 12 Abs. 1 DSGVO. So muss sich beispielsweise die Mietern bei Abschluss eines Mietvertrags übergebene Information nach Art. 13 DSGVO konkret (und ausschließlich) auf die Verarbeitung der Mieterdaten im Rahmen des Mietverhältnisses beziehen.

3.1.2 Informationspflichten von Rechtsanwälten als Berufsgeheimnisträger

Im letzten Berichtszeitraum erhielt ich eine Anfrage zur Informationspflicht von Rechtsanwälten beziehungsweise einer Rechtsanwaltskanzlei. Im Zusammenhang mit einer Forderung wandte sich eine Anwaltskanzlei an eine beteiligte Partei. Die so betroffene Person monierte, dass der Informationspflicht auf dem mit herkömmlicher Briefpost übersandten Schreiben der Kanzlei gemäß Art. 13 und 14 Datenschutz-Grundverordnung (DSGVO) nicht genügt worden sei. Auf dem Briefbogen der Anwaltskanzlei ließe sich lediglich der Hinweis finden, dass die Daten Verfahrensbeteiligter verarbeitet werden. Die betroffene Person fragte, ob die Rechtsanwaltskanzlei den Betroffenen die datenschutzrechtlichen Informationen gemäß Art. 13, 14 DSGVO beziehungsweise mit dem ersten Schriftsatz hätte zuleiten müssen oder nicht. In einer Stellungnahme äußerte sich die Rechtsanwaltskammer gegenüber der betroffenen Person unter Hinweis auf das für Rechtsanwälte bestehende Berufsgeheimnis und verneinte eine entsprechende Pflichtigkeit.

Im Ergebnis teile ich die Auffassung der Rechtsanwaltskammer. In Betracht kam im konkreten Einzelfall auch aufgrund der Erhebungsweise nur eine Information nach Art. 14 DSGVO, Datenerhebung bei Dritten. Gemäß Art. 14 Abs. 5 Buchst. d DSGVO sind Berufsgeheimnisträger von der Informationspflicht ausgenommen. Der Ausschlusstatbestand hat nach meiner Überzeugung den Schutz der Vertrauensbeziehung des Berufsgeheimnisträgers und des Begünstigten des Berufsgeheimnisses, der Mandantschaft, gegenüber Dritten zum Gegenstand. Zwar umfassen die Informationspflichten des Art. 14 DSGVO nicht die Daten selbst, sondern lediglich die Kategorien der Daten beziehungsweise deren Verarbeitungsweise, gleichwohl werden die Informationspflichten nach dem Wortlaut der Verordnung vollumfänglich ausgeschlossen. Nicht zu verkennen ist zudem auch, dass in einer gewissen Häufigkeit und in nicht voraussehbaren und überschaubaren Bezügen selbst allgemeine Informationen Rückschlüsse auf dem Berufsgeheimnis unterfallenden Inhalte zulassen könnten und dies den Zweck der Ausnahmebestimmung insgesamt gefährden könnte.

Insoweit entfällt im Ergebnis eine Pflichtigkeit von Rechtsanwälten als Berufsgeheimnisträger. Dies gilt jedoch nur gegenüber Dritten, nicht gegenüber der eigenen Mandantschaft beziehungsweise den Begünstigten des Berufsgeheimnisses, so dass gegenüber Letzteren die nach dem Katalog des Art. 14 Abs. 1 und Abs. 2 DSGVO zu erklärenden Inhalte verfügbar beziehungsweise bereitgehalten werden müssen.

Auch sind Rechtsanwälten und Kanzleien im Falle von Internetpräsenzen die Informationspflichten mittels sogenannter leicht zugänglicher „Datenschutzerklärungen“ auf der Webseite abzuverlangen.

Die vorstehenden Überlegungen sind auf andere Berufsgeheimnisverhältnisse nicht-öffentlicher Stellen – Verantwortlicher – grundsätzlich übertragbar. In anderen Verhältnissen, etwa bei Behörden, wird die Ausnahmebestimmung für Berufsgeheimnisträger allerdings besonders und differenzierter zu betrachten sein.

Zu betonen ist letztendlich noch, dass der Ausnahmetatbestand nur für die insoweit geschützte Tätigkeit als Berufsgeheimnisträger gilt. Als Exkurs ist auf eine interessante Entscheidung des Bundesfinanzhofs hinzuweisen, dem die Frage zugrunde lag, ob ein Rechtsanwalt als externer Datenschutzbeauftragter als gewerblicher Unternehmer oder Rechtsanwalt tätig ist. Der Bundesfinanzhof entschied, dass ein Datenschutzbeauftragter keine dem Beruf des Rechtsanwalts vorbehaltene Tätigkeit ausübe, sondern eine von der Rechtsanwaltstätigkeit abzugrenzende gewerbliche Tätigkeit (vgl. Bundesfinanzhof, Urteil vom 14. Januar 2020, VIII R 7 20/17). § 29 Abs. 3 Bundesdatenschutzgesetz verweist auf den Kreis geheimhaltungspflichtiger Personen im Wege des § 203 Abs. 1, 2 a und 3 Strafgesetzbuch. Nach dem neu eingefügten Abs. 2a der strafgesetzlichen Vorschrift werden Datenschutzbeauftragte allerdings selbst wie Berufsgeheimnisträger behandelt, so dass eine andersartige Tätigkeit eines zugelassenen Rechtsanwalts in dem Fall keine Rolle spielen würde. In anderen Fällen ist die außeranwaltliche Tätigkeit aber eben gerade nicht die eines Berufsgeheimnisträgers, sondern bloß gewerblich. In diesen Fällen ist die Person, die auch Rechtsanwalt ist, eben gerade nicht von den Informationspflichten befreit.

Zu der Eigenschaft als Verantwortlicher des externen Datenschutzbeauftragten vergleiche den Beitrag unter 2.1.2.

3.2 Auskunftsrecht

3.2.1 Auskunftsersuchen an die Schule in einer dienstrechtlichen Angelegenheit

Petenten informierten mich über folgenden Sachverhalt: Ihre Tochter, die bis dahin keine Fehltage aufgewiesen habe, wurde am letzten Schultag auf Antrag der Schulleiterin durch die Polizei der Schule zugeführt – ohne dass die Schule vorher versucht habe, die Mutter telefonisch nach dem Verbleib ihrer Tochter zu fragen. Daraufhin sei ein Disziplinarverfahren gegen die Schulleiterin eingeleitet worden. Am vorletzten Schultag hatte eine gemeinsame Übernachtung mit einem freiwilligen gemeinsamen Frühstück stattgefunden. Sowohl an der Übernachtung als auch am Frühstück hatte die Tochter nicht teilgenommen.

Eine Auskunft beziehungsweise Kopie der in diesem Zusammenhang verarbeiteten Daten zu ihrer Tochter nach Art. 15 Datenschutz-Grundverordnung (DSGVO), konkret eine Übersendung der Stellungnahme der Schulleiterin sowie der Klassenlehrerin, sei ihnen jedoch verweigert worden. Das von mir um Stellungnahme gebetene Landesamt für Schule und Bildung (LaSuB) bestätigte diese Darstellung.

Es begründete dies zunächst damit, dass der Anwendungsbereich der DSGVO nicht eröffnet sei, da es sich um keine automatisierte Verarbeitung personenbezogener Daten handelte. Dies war jedoch nicht überzeugend. Nach Art. 2 Abs. 1 DSGVO sind die Vorschriften der DSGVO anzuwenden, wenn personenbezogene Daten ganz oder teilweise automatisiert verarbeitet werden oder wenn personenbezogene Daten nichtautomatisiert verarbeitet werden, die in einem Dateisystem gespeichert sind oder werden sollen. Um eine automatisierte Verarbeitung handelt es sich vorliegend zwar nicht. Es ist aber zu vermuten, da es um personenbezogene Daten geht, die im Rahmen einer Dienstaufsichtsbeschwerde verarbeitet wurden, dass diese Daten in einem Dateisystem (Personalakte oder Sachakte) im oben angeführten Sinn gespeichert sind. Im Übrigen ist Art. 15 DSGVO auf der Grundlage von § 2 Abs. 4 Satz 1 Sächsisches Datenschutzdurchführungsgesetz (SächsDSDG) generell entsprechend anzuwenden, da es sich beim LaSuB unzweifelhaft um eine öffentliche Stelle handelt, für die das SächsDSDG gilt (§ 2 Abs. 1 SächsDSDG).

Weiterhin berief sich das LaSuB auf Art. 15 Abs. 4 DSGVO. Dieser bestimmt, dass das Recht auf Erhalt einer Kopie die Rechte und Freiheiten anderer Personen nicht beeinträchtigen darf. Erwägungsgrund 63 der DSGVO erläutert hierzu:

„Dieses Recht sollte die Rechte und Freiheiten anderer Personen, etwa Geschäftsgeheimnisse oder Rechte des geistigen Eigentums und insbesondere das Urheberrecht an Software, nicht beeinträchtigen. Dies darf jedoch nicht dazu führen, dass der betroffenen Person jegliche Auskunft verweigert wird."

Ob die Voraussetzungen des Art. 15 Abs. 4 DSGVO im konkreten Fall vorliegen, konnte durch mich nicht beurteilt werden, da hierzu Sachverhaltsangaben fehlten. Datenschutzrechte der Schulleiterin und der Klassenlehrerin wären grundsätzlich als Rechte Dritter in Betracht zu ziehen. Ob diese Entscheidungsgrundlage waren und ob sich in diesem Zusammenhang auch mit der Frage auseinandergesetzt wurde, wie weit diese Rechte bei Amtshandlungen reichen, ist jedoch nicht dargetan. Im Übrigen trägt der Verantwortliche die Beweislast für das Vorliegen der Voraussetzungen des Art. 15 Abs. 4 DSGVO.

Schließlich wurde darauf hingewiesen, dass der datenschutzrechtliche Auskunftsanspruch neben einem möglichen Akteneinsichtsrecht bestünde. Es sei jedoch nicht Sinn und Zweck des Auskunftsanspruches, ein nicht bestehendes Akteneinsichtsrecht zu umgehen.

Zutreffend ist, dass das Akteneinsichtsrecht und der datenschutzrechtliche Auskunftsanspruch grundsätzlich zwei nebeneinander stehende Ansprüche vermitteln. Sie verfolgen einerseits unterschiedliche Zwecke und sind andererseits auf unterschiedliche Objekte bezogen. Dieses grundsätzliche Nebeneinander kann aber dann aufgehoben sein, wenn der Gesetzgeber mit den Regelungen zum Akteneinsichtsrecht den Auskunftsanspruch nach Art. 15 DSGVO beschränken wollte. Eine derartige Beschränkung müsste jedoch den Voraussetzungen des Art. 23 DSGVO genügen. In Verfahren zu Dienstaufsichtsbeschwerden gibt es kein Akteneinsichtsrecht. Insbesondere ist § 29 Verwaltungsverfahrensgesetz (VwVfG) nicht anwendbar, da es sich bei diesen Verfahren nicht um Verwaltungsverfahren nach § 9 VwVfG in Verbindung mit § 1 Satz 1 SächsVwVfZG handelt. Es ist daher nicht von einer Einschränkung des Auskunftsrechts auszugehen.

Mein entsprechendes Schreiben an das LaSuB führte dazu, dass die von den Petenten begehrte Auskunft schließlich erteilt wurde.

3.2.2 Verweigerte Auskunft zum Adressbezug beim Lettershop-Modell

In einem Fall hat ein Verantwortlicher, der sich zur Verbreitung seiner Werbung eines Adresspool-Inhabers bedient hatte, einer betroffenen Person gegenüber erklärt, die Werbeagentur aus Datenschutzgründen nicht bezeichnen zu dürfen. Dieses Missverständnis konnte ich ausräumen. Die betroffene auskunftbegehrende Person erhielt die Information.

Generell begrüße ich, wenn in Umsetzung datenschutzrechtlicher Grundsätze Datenbestände reduziert und der Bestand von eigenen Werbedaten auf das erforderliche Minimum eingeschränkt wird. Auffassungen, die generell auf eine gemeinsame Verantwortlichkeit für die Rechtmäßigkeit der unternommenen Verarbeitungen abzustellen suchen, folge ich nicht (vgl. auch zum Lettershop-Modell und zur gemeinsamen Verantwortlichkeit 4.2.3).

Anzuraten ist, dass sich seriöse werbetreibende Unternehmen ihre Datenquellen sehr gut auswählen und für eine ausreichende Dokumentation mittels selbst vorgegebener Stichprobe – insbesondere zum Nachweis von Einwilligungen – sorgen.

3.2.3 Recht auf kostenlose Datenkopie für Kontoauszugsdaten

In mehreren Fällen wandten sich Betroffene an mich, denen das verantwortliche Kreditinstitut unter Berufung auf vertragliche oder gesetzliche Entgeltbestimmungen nur gegen Entgelt Kopien der verarbeiteten Daten erteilen wollte.

Nach Art. 15 Abs. 3 Datenschutz-Grundverordnung (DSGVO) hat der Betroffene das Recht auf Erteilung einer Kopie der von einem Verantwortlichen gespeicherten und verarbeiteten personenbezogenen Daten. Die Kopie ist nach Art. 12 Abs. 5 DSGVO kostenlos zu erteilen.

Das Recht auf kostenlose Datenkopie besteht unabhängig von vertraglichen oder gesetzlichen Regelungen, die für bestimmte Dokumente oder Abschriften ein Entgelt festsetzen. So besteht etwa dieses Recht auch dann, wenn für Kontoauszüge oder deren Kopien vertraglich Entgelte vereinbart sind. Dies gilt etwa auch für den Anspruch des Patienten auf Erteilung einer Kopie der Patientenakte (vgl. Tätigkeitsbericht 2017/2018, Teil 2, 3.2.3, Seite 195).

Der datenschutzrechtliche Anspruch auf Datenkopie umfasst allerdings kein Recht auf eine bestimmte Struktur der Kopie. Der Verantwortliche hat eine Kopie der vorliegenden Akten beziehungsweise Rohdaten in einem gängigen Format zu erteilen, muss diese jedoch nicht in eine bestimmte Struktur bringen. Entsprechend kann der Betroffene keine kostenlosen Kopien von Kontoauszügen verlangen. Geschuldet ist eine strukturierte Auflistung der Zahlungsvorgänge in der Form, in der die Daten dem Kreditinstitut vorliegen, oder einem anderen gängigen Format.

Hintergrund der Bedenken der Banken ist regelmäßig, dass diese für Kopien von Kontoauszügen nicht unerhebliche Gebühren erheben möchten. Die Kostenfreiheit et cetera nach Art. 15 Abs. 3 DSGVO stört diese Erwartungshaltung.

Geschuldet ist nach meiner Überzeugung lediglich eine Kopie, aber eben nicht zwingend in Form der Kontoauszüge. Hat der Verantwortliche eine Kopie der vorliegenden Akten beziehungsweise Rohdaten in einem gängigen Format zu erteilen, muss diese eben nicht in einer – vom Auskunftsuchenden – bestimmten Struktur erbracht werden. Entsprechend kann der Betroffene keine kostenlosen Kopien von Kontoauszügen verlangen, wohl aber eine geordnete Auflistung der Zahlungsvorgänge in der Form, in der die Daten dem Kreditinstitut vorliegen beziehungsweise in einem anderen gängigen Format.

Die Frage, ob der Verantwortliche Kopien von Kontoauszügen zur Verfügung zu stellen hat, wenn er diese – zusätzlich zu den zugrundeliegenden Daten unter anderem in seinem Kontenführungssystem – als solche etwa im PDF-Format gespeichert hat, musste noch nicht beantwortet werden, dürfte aber nach meiner Einschätzung auch zu bejahen sein.

Das von Verantwortlichen und Unternehmensverbänden insoweit angeführte Argument, die Erteilung einer derartigen Kopie sei wegen entgegenstehender Rechte Dritter unzulässig, kann zwar theoretisch zutreffen. Allerdings ist insoweit zu berücksichtigen, dass die entsprechenden Daten dem Betroffenen bereits in Form von Kontoauszügen zur Verfügung gestellt wurden, und die erneute Zurverfügungstellung insoweit die wirtschaftliche Sozialsphäre der Drittbetroffenen allenfalls peripher berühren dürfte. Soweit Rechte Dritter hier tatsächlich entgegenstehen sollten, wird der Anspruch auf Kopie auch nicht vollständig ausgeschlossen, sondern allenfalls insoweit beschränkt. Jedenfalls wenn der Verantwortliche die Erteilung vollständiger Datenkopien in Form von Kontoauszügen gegen Entgelt anbietet, erscheint die Berufung auf Drittrechte zur Verweigerung der entsprechenden kostenlosen Informationen eindeutig als vor-

geschobener Vorwand. Eine derartig widersprüchliche Beeinträchtigung der Betroffenenrechte wäre als Datenschutzverstoß zu gewichten.

Für einen unbeschränkten Auskunftsanspruch haben bereits das OLG Köln, Urteil vom 26. Juli 2019 - 20 U 75/18 (nicht rechtskräftig, beim BGH anhängig unter dem Az. IV ZR 213/19) und das österreichische Bundesverwaltungsgericht, Entscheid vom 10. Dezember 2018, W211 2188383-1, entschieden.

Instanzgerichten, Behörden- und Literaturmeinungen, die den Auskunftsanspruch ohne gesetzliche Stütze beschränken wollen, kann aus grundsätzlichen Erwägungen nicht gefolgt werden:

Einschränkungen finden keine gesetzliche Stütze: Vielmehr sind die Gründe, aus denen das Auskunftsrecht eingeschränkt werden darf, in den Datenschutzgesetzen abschließend aufgelistet. Finanzielle Interessen der Verantwortlichen, mit den entsprechenden Auskünften Einnahmen zu erzielen, fallen eindeutig nicht darunter.

Nicht von der Datenschutz-Grundverordnung vorgesehene Beschränkungen zuzulassen, hätte unvermeidlich einen Graubereich zur Folge, in dem die Verantwortlichen Anfragen der Betroffenen „am langen Arm verhungern lassen“. Faktisch würde so das gesetzlich vorgesehene Auskunftsrecht ausgehöhlt.

Der Zweck des Auskunftsrechts, betroffenen Personen eine Überprüfung zu ermöglichen, würde ebenso konterkariert wie der Zweck des Rechts auf Kopie, Wettbewerbs- und Wechselbarrieren zu senken.

Meine Behörde stellt bei den Rechten auf Erteilung einer Datenkopie nach Art. 15 DSGVO allein ab auf die gesetzlichen Beschränkungen sowie die allgemeine Figur der Rechtsmissbräuchlichkeit, die in Art. 12 Abs. 5 Satz 2 DSGVO als Exzessivität des Begehrens einen gesetzlichen Widerhalt findet. Bequemlichkeit und schlechte Buchführung des Betroffenen zähle ich nicht darunter.

Diese Lösung erscheint auch rechtskongruent, da die Verantwortlichen regelmäßig nach zum Beispiel Handels- und Steuerrecht die Daten strukturiert nachhalten müssen, und eine – regelmäßig elektronische – Kopie kaum (Zusatz-)Kosten verursachen dürfte.

Die Grundfrage nach Reichweite und Grenzen des Anspruchs auf Auskunft und Kopie ist in vielem noch ungeklärt. Auch wenn alle sächsischen Verfahren jedenfalls in Bezug auf Kontoinformationen bislang einvernehmlich gelöst werden konnten, erscheint eine verbindliche höchstgerichtliche Klärung etwa wie in Österreich erstrebenswert, um nachhaltige Klarheit für Verantwortliche und betroffene Personen hervorzubringen.

3.3 Recht auf Löschung

3.3.1 Verpflichtung zur Löschung von Kontoauszügen durch das Jobcenter?

Im Rahmen einer Eingabe befasste ich mich mit der Frage, ob der Petent ein Recht auf die Löschung seiner Kontoauszüge hat, sobald er kein Arbeitslosengeld II (Hartz IV) mehr bezieht.

Der Petent ist der Auffassung, dass ehemalige Hartz-IV-Beziehende das Recht auf unverzügliche Löschung aller personenbezogenen Daten haben. Er beruft sich dabei auf § 84 Abs. 2 Zehntes Buch Sozialgesetzbuch (SGB X) alte Fassung.

Die betroffene Person hat gemäß Art. 17 Abs. 1 Buchst. a Datenschutz-Grundverordnung (DSGVO) das Recht von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden, wenn die personenbezogenen Daten für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind.

Art. 17 Abs. 1 Buchst. a DSGVO entspricht im Wesentlichen dem bis zum Inkrafttreten der DSGVO in Deutschland geltenden Recht. Sozialdaten waren nach § 84 Abs. 2 SGB X alte Fassung dann zu löschen, wenn ihre Kenntnis für die verantwortliche Stelle zur rechtmäßigen Erfüllung der in ihrer Zuständigkeit liegenden Aufgabe nicht mehr erforderlich war und kein Grund zu der Annahme bestand, dass durch die Löschung schutzwürdige Interessen Betroffener beeinträchtigt würden.

Die personenbezogenen Daten, hier Kontoauszüge, müssen nach Art. 17 Abs. 1 Buchst. a DSGVO für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, notwendig sein. Es war zu prüfen, ob das Jobcenter die Kontoauszüge benötigt hat und noch benötigen wird.

Nach § 67b SBG X ist die Speicherung, Veränderung, Nutzung, Übermittlung, Einschränkung der Verarbeitung und Löschung von Sozialdaten durch die in § 35 SGB I genannten Stellen nur erlaubt, soweit es datenschutzrechtliche Vorschriften des SGB X oder eine andere Vorschrift des SGB dies erlauben.

Als bereichsspezifische Rechtsgrundlage für die Verarbeitung kam § 51b SGB II in Betracht. Nach § 51b Abs. 1 SGB II erheben die zuständigen Träger der Grundsicherung für Arbeitssuchende laufend die für die Durchführung der Grundsicherung für Arbeitssuchende erforderlichen Daten. § 51b Abs. 3 SGB II legt fest, dass die nach den Absätzen 1 und 2 erhobenen Daten nur für die dort aufgeführten Zwecke – Nummern 1 bis 5 – verarbeitet und genutzt werden dürfen. Hier kam Nummer 5, Bekämpfung von Leistungsmissbrauch, in Betracht.

Die Verordnung zur Erhebung der Daten nach § 51b des SGB II regelt, welche Daten bei der Durchführung der Grundsicherung für Arbeitssuchende zu erheben sind. Nach § 1 Nr. 2 und 3 dieser Verordnung sind unter anderem Daten über die Art und Dauer der Bedarfe, die Ausgaben und Einnahmen im Rahmen der Grundsicherung für Arbeitsuchende zu erheben. Dazu sind Kontoauszüge zu zählen, die zum Beispiel die Einnahmen und Ausgaben belegen. Nach § 45 SGB X ist die Rücknahme eines rechtswidrigen begünstigenden Verwaltungsakts bis zum Ablauf von zehn Jahren nach seiner Bekanntgabe möglich.

Der Aktenplan SGB II der Bundesagentur für Arbeit vom 1. Oktober 2012 regelt pauschale Aufbewahrungsfristen von zehn Jahren.

Eine Aufbewahrung der Kopien der Kontoauszüge durch das Jobcenter ist nach § 51b Abs. 3 SGB II erforderlich. Ein Recht des Petenten auf Löschung seiner Kontoauszüge nach Art. 17 Abs. 1 Buchst. a DSGVO, nachdem er kein SGB II mehr erhält, besteht somit nicht.

Das Bundessozialgericht (BSG) hat mit Urteil vom 14. Mai 2020 (Az.: B 14 AS 7/19) entschieden, dass Kontoauszüge, die das Jobcenter zur Leistungsakte genommen hat, über einen Zeitraum von bis zu zehn Jahren zur Akte genommen werden dürfen. Die sind in diesem Zeitraum folglich nicht zu löschen. Dafür dürfen die Kontoauszüge auch kopiert werden. Allein den Verweis auf das Fertigen von Aktenvermerken über eine erfolgte Vorlage von Kontoauszügen lässt das Gericht hingegen ausdrücklich nicht ausreichen (vgl. auch 0).

3.3.2 Die Löschung von Kundenprofilen und -konten

Im letzten Berichtszeitraum erreichte mich die Eingabe eines Flirtportal-Kunden, der mitteilte, nach selbst ausgelöster Löschung seines Kundenkontos weitere Erinnerungsmails, sogenannte „Nudgemails“ des Portals erhalten zu haben und fürchtete, dass ihn dies bei seiner neuen Lebensgefährtin in missliche Erklärungsnot bringen würde. Die letztliche Ursache bestand allerdings darin, dass er die vor der Umsetzung der Löschung zu bestätigende E-Mail (im Sinne von Double-Opt-Out) ignoriert hatte und sein Konto mithin nie gelöscht worden war. Die Frage, ob in dem Fall end- wie folgenlose Erinnerungen vertraglich verabredet worden sind, hatte ich angesichts des Eingabevortrags zunächst beiseitegelassen. Sie könnte allerdings neu auftreten, wenn ein Kunde nicht kündigen, sondern nur von „Wir vermissen dich“-Mitteilungen verschont werden will (vgl. auch 2.2.20).

Mit der Löschung des Profil- oder Kundenkontos müssen Betroffene nicht selten davon ausgehen, dass ein etwaiger Werbewiderspruch ebenfalls gelöscht wird. Würde später eine erneute Anmeldung mit identischer E-Mail-Adresse erfolgen, können sie jedenfalls nicht von einem Fortbestehen des (alten) Werbewiderspruchs ausgehen, sondern müssten diesen gegebenenfalls erneut formulieren. Dies gilt freilich nicht im Fall einer Werbesperrdatei, die von den

Verantwortlichen als Service nach Wegfall der Geschäftsbeziehung und einer zivilrechtlich vertretbaren Überliegefrist jedoch nur noch auf Einwilligungsbasis geführt werden dürfte.

3.3.3 Häufige Beschwerden zu unerwünschter Werbung per E-Mail

Auch im aktuellen Berichtszeitraum hat unerwünschte Werbung einen nicht unbeachtlichen Anteil der Eingaben ausgemacht. Strukturelles Versagen von Verantwortlichen ist dafür allerdings meist kaum noch die Ursache. Ich spreche dabei natürlich nur von seriösen Marktteilnehmern, die erreichbar sind und sich mit Unternehmensangaben, Anschriften und Rufnummern zu ihrem Geschäft bekennen.

Was unbekannte Absender angeht, sollten sich betroffene Personen im Fall der Zusendung unerwünschter E-Mail- oder anderer elektronischer Zusendungen über Browser- und Client-Einstellungen behelfen oder bei Rufnummernmissbrauch an die Bundesnetzagentur wenden. Enthalten elektronische Zusendungen Erpressungen oder sensible Betroffenendaten, zum Beispiel Bankinformationen, sollte man sich an die Polizei wenden.

Meine Aufsichtsbehörde hat bislang keine Möglichkeit, gegen nicht mühelos identifizierbare Spammer oder Versender unerwünschter E-Mails zu ermitteln oder gar deren Geschäftsmodell auszutrocknen.

Zur Begrifflichkeit, was „Werbung“ angeht:

„Der Begriff der Werbung umfasst nach dem allgemeinen Sprachgebrauch alle Maßnahmen eines Unternehmens, die auf die Förderung des Absatzes seiner Produkte oder Dienstleistungen gerichtet sind. Damit ist außer der unmittelbar produktbezogenen Werbung auch die mittelbare Absatzförderung – beispielsweise in Form der Imagewerbung oder des Sponsoring – erfasst. Werbung ist deshalb in Übereinstimmung mit Art. 2 Buchst. a der Richtlinie 2006/113/EG über irreführende und vergleichende Werbung jede Äußerung bei der Ausübung eines Handels, Gewerbes, Handwerks oder freien Berufs mit dem Ziel, den Absatz von Waren oder die Erbringung von Dienstleistungen zu fördern“,

so der Bundesgerichtshof in seinem Urteil vom 12. September 2013 (I ZR 208/12, Tz. 17).

Bei Weitem nicht jede als unerwünscht empfundene Werbeansprache bei den mir zugegangenen Beschwerden ist dabei unzulässig gewesen. Erfreulicherweise liegen nach meiner Beobachtung bei seriösen Verantwortlichen keine strukturellen, sondern überwiegend einzelne individuelle Fehler von Beschäftigten bei den eingehenden Beschwerdevorgängen zugrunde. Nicht selten führen auch unzureichende Kenntnisse der Rechtslage bei den Beschwerdeführern zu Eingaben bei meiner Dienststelle. Zum einen werden Werbeansprachen kundenseitig ohne – irrtümlich als Voraussetzung empfundene – Einwilligung als unzulässig angesehen,

zum anderen erkennt man aufgrund von Rechtsvorschriften nicht (vollständig) erfüllte Löschungsverlangen nach Beendigung von Vertragsverhältnissen als Datenschutzverstoß.

Im Bereich E-Commerce wird die beabsichtigte (werbliche) Nachnutzung, der originär zur Vertragsabwicklung erhobenen E-Mail-Adresse, den betroffenen Personen gegenüber mitgeteilt. In vielen Fällen ist dies gleichwohl nicht im Sinne der Vertragskunden, was häufig unter Verkennung der Rechtslage zu Betroffeneneingaben führt. Viele Betroffene geben dabei in ihren Beschwerden an, einer Werbeansprache per E-Mail niemals zugestimmt zu haben und halten diese daher glattweg für unzulässig.

Häufig ist auf Plattformen im Bereich E-Commerce etwa folgender oder vergleichbarer Hinweis zu finden: „Nach Angabe Ihrer E-Mail-Adresse erhalten Sie personalisierte, auf Ihren Einkauf bezogene Angebote und Empfehlungen. Sie können dem jederzeit ohne zusätzliche Kosten widersprechen, zum Beispiel über den Abmeldelink am Ende jeder unserer E-Mails."

Derartige Information nimmt auf die Rechtslage nach § 7 Abs. 3 Gesetz gegen den unlauteren Wettbewerb (UWG) Bezug, die eine Werbung gegenüber (Bestands-)Kunden bei elektronischer Post zulässt, bezieht sich aber nicht auf eine im Bestellprozess erteilte Einwilligung. Auch ist aus „Ihren Einkauf" zu entnehmen, dass der Hinweis sich nur an Bestandskunden richtet.

Werbung ist in diesen Fällen zulässig, aber es besteht die Möglichkeit des Betroffenen, Widerspruch gegen die Direktwerbung zu erheben (vgl. auch Tätigkeitsbericht 2017/2018, Teil 2, 3.4.2, Seite 198 f.).

Ein Werbewiderspruch muss nach meiner Überzeugung gegenüber dem Verantwortlichen dabei zu jeder Zeit – also auch vor dem ersten Newsletter – und in jeder zur Verfügung stehenden Form erklärt werden können, allerdings nicht per Antwort auf No-Reply-Absender. Zweckmäßig sind zudem seitens der Verantwortlichen auf der Internetseite eingerichtete „Opt-Out"-Kästchen oder Sofort-Abmelde-Buttons, die nicht nur als Verbraucher-, sondern auch zur Wahrnehmung des Betroffenenrechts als datenschutzfreundlich anzusehen wären, obwohl ich gegenwärtig keine Handhabe sehe, diese zu verlangen oder vorzuschreiben.

Festzuhalten ist im Ergebnis aber auch, dass Werbung bei abgebrochenen Bestellprozessen, die nicht zu einem gültigen Vertrag geführt haben, unzulässig bleibt.

Nicht selten sind Eingabefälle, in denen die betroffenen Personen nach Eingang von Werbung die „vollständige" Löschung ihrer personenbezogenen Daten beim Verantwortlichen verlangen. Diese enthalten dann Beschwerden über Mitteilungen von Verantwortlichen, dass die von den Betroffenen erwünschte Löschung aus Rechtsgründen nicht stattfinden dürfe.

Tatsächlich stehen einer physischen Löschung bestimmter Datenarten gesetzliche Fristen, insbesondere nach § 257 Handelsgesetzbuch (HGB) und §§ 140 ff. Abgabenordnung (AO) mit bis zu zehn Jahren entgegen. Diese 10-Jahres-Frist umfasst vor allem Buchungsbelege sowie Rechnungen. Die Aufbewahrungsfrist bei Handelsbriefen – also die geschäftliche Kommunikation, gegebenenfalls auch der E-Mail-Verkehr – beträgt sechs Jahre (§ 257 Abs. 4 HGB). Diese Daten unterliegen damit im Ergebnis aber auch einer Nutzungseinschränkung, insbesondere bei Übermittlungen an Dritte und für Werbezwecke.

Wer als Kunde und Betroffener bereits durch eine verbindliche – nicht „freibleibende“ – Anfrage/Bestellung einen Vertrag geschlossen hat, kann im Nachgang keine vollständige Löschung aller ihn betreffenden Daten mehr durchsetzen (vgl. auch Tätigkeitsbericht 2017/2018, Teil 2, 3.3.1., Seite 197).

Nicht selten fordern Betroffene eine schriftliche Bestätigung über die erfolgte Umsetzung. Ein datenschutzrechtlich herzuleitender Anspruch auf die Bestätigung einer Löschung/Nutzungseinschränkung oder Begründung einer Nichtlöschung durch den Verantwortlichen besteht zwar als genuiner Anspruch nicht. Die Verantwortlichen sollten allerdings zumindest auf nicht vollständig erfüllbare Löschungsverlangen mit einer überzeugenden Begründung antworten, auch im eigenen Interesse. Sie vermeiden damit nicht selten den weitaus höheren Aufwand, der sich aus einem Auskunftsverlangen ergibt. Zudem kann auf die Inanspruchnahme meiner Behörde durch den Betroffenen dann auch eher verzichtet werden.

3.3.4 Fortwährende Verarbeitung personenbezogener Daten potenzieller Erben durch einen Verantwortlichen

Ein sächsisches Kreditinstitut war im Rahmen der Erbenermittlung durch ein Nachlassgericht in einem anderen Bundesland informiert worden, dass zu dem betreffenden Erbe weder ein Erbschein erteilt worden war, noch eine Erbausschlagung stattgefunden hatte. Daneben war ohne ersichtliche Rechtsgrundlage darüber informiert worden, dass ein Bruder des Erblassers existierte. Das Kreditinstitut versuchte nunmehr, den Bruder des Erblassers als Erben für die erheblichen Nachlassverbindlichkeiten haftbar zu machen, da dieser grundsätzlich als gesetzlicher (Mit-)Erbe in Betracht kam. Auch nachdem dieser mitgeteilt hatte, kein Erbe zu sein, wurde er weiter kontaktiert und ihm mitgeteilt, nur gegen Nennung des tatsächlichen Erben beziehungsweise nach dessen Bekanntwerden könne von einer weiteren Verarbeitung seiner Daten abgesehen werden.

Der Betroffene hatte sich an meine Dienststelle gewendet, um eine Löschung seiner Daten bei dem Kreditinstitut zu erwirken.

Da die Datenverarbeitung jedoch zur Geltendmachung von Rechtsansprüchen und somit aus legitimen Interessen heraus erfolgte, bestand nach Art. 6 Abs. 1 Buchst. f Datenschutz-Grundverordnung (DSGVO) eine gesetzliche Grundlage dafür. Solange nicht feststeht, dass der Bruder tatsächlich nicht Erbe geworden ist, kann das legitime Interesse auch personenbezogene Daten möglicherweise nur potenzieller Erben umfassen.

Für einen Berichtigungsanspruch war trotz Nachfrage meiner Behörde nicht konkret und nachprüfbar vorgetragen worden, aus welchen Gründen der Beschwerdeführer als gesetzlicher Erbe konkret nicht als Erbe in Frage kam. Ein Anspruch auf Löschung besteht nicht, solange eine Verarbeitungsgrundlage und eine entsprechende Zweckverfolgung bestehen. Dabei kam es hier nicht darauf an, ob das Nachlassgericht die entsprechenden Informationen weiterleiten durfte. Denn konkret lagen jedenfalls die Voraussetzungen einer zulässigen Zweckänderung nach Art. 6 Abs. 4 DSGVO vor.

Auch ein Widerspruchsrecht im Sinne des Art. 21 DSGVO war in der konkreten Sachlage nicht gegeben. Der Beschwerdeführer äußerte zwar Sorgen wegen möglicher Bonitätsrisiken durch die Geltendmachung der Ansprüche. Da jedoch eine Einmeldung untitulierter, bestrittener Forderungen in Auskunfteien nicht zulässig ist (vgl. § 31 Abs. 2 Bundesdatenschutzgesetz), bestand kein konkretes Risiko, dass die Bonität beziehungsweise die entsprechenden Einschätzungen durch Auskunfteien Schaden nehmen könnten. Denn jedenfalls hätten gegen entsprechend rechtswidrige Einmeldungen ein Löschungs- und ein Schadensersatzanspruch bestanden.

Die Möglichkeit nach Art. 18 Abs. 1 DSGVO die (temporäre) Einschränkung der Verarbeitung zu erreichen, war vor dem Hintergrund der nach Art. 18 Abs. 2 DSGVO weiter zulässigen Verarbeitung („zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen“) hier wirkungslos.

Mit dem geltenden Datenschutzrecht werden zivilrechtliche Vorfragen nicht selbst zu lösen versucht, sondern die Datenverarbeitung zu Geltendmachung von Rechtsansprüchen ausdrücklich privilegiert (vgl. etwa Art. 9 Abs. 2 Buchst. f und Art. 18 Abs. 2, 2. Alternative DSGVO).

Der Schwebezustand der Zulässigkeit einer Datenverarbeitung auf Grundlage potenzieller Erbenhaftung konnte vor Verjährung des behaupteten Anspruchs lediglich auf zivilgerichtlichem Weg beendet werden, worauf der Beschwerdeführer hingewiesen wurde.

3.3.5 Viel Lärm um nichts: Grundloser Ärger wegen alter Videokameras

Ausgangspunkt für einen kuriosen Fall waren drei Videokameras, die ein selbst im Bereich des Datenschutzes tätiger Beschwerdeführer bei mir anzeigte. Mit diesem Hintergrund war er der

festen Überzeugung, dass darin ein Datenschutzverstoß vorliege, zumal eine Kamera sogar vollständig auf den öffentlichen Bereich gerichtet war. Weiter stellte er fest, dass es vor Ort – es handelte sich um ein Gewerbeanwesen – keinen Hinweis auf den verantwortlichen Kamerabetreiber gebe. Nicht einmal ein Piktogramm zur Videoüberwachung sei vorhanden. Aufgrund eines gegenüberliegenden Alten- und Pflegeheimes ging er von einer großen Anzahl betroffener Personen aus.

Offensichtlich ließ dem Beschwerdeführer die vermeintliche Videoaufzeichnung seiner Person keine Ruhe, so dass er ungeachtet seiner Beschwerde bei mir noch am gleichen Tag auf eigene Faust weitergehende Recherchen anstellte. Dabei stieß er im Internet unter der betreffenden Anschrift auf eine Sicherheitsfirma, an die er sofort ein Auskunftsersuchen nach Art. 15 Datenschutz-Grundverordnung (DSGVO) richtete. In diesem Zusammenhang wies er – einzig auf Basis seiner Beobachtungen und Feststellungen vor Ort – in der Manier einer Aufsichtsbehörde auf die Rechtswidrigkeit der mit der Videoüberwachung vorgenommenen Verarbeitung personenbezogener Daten hin, sah darin gleich mehrere Bußgeldvorschriften verletzt und forderte zugleich auch die Löschung der ihn betreffenden Aufzeichnungen. Damit brachte er einen Stein ins Rollen, der ihm vor Augen führen sollte, dass er die Sache wohl besser etwas ruhiger hätte angehen und auf die Arbeit meiner Behörde vertrauen hätte sollen.

Ich muss an dieser Stelle klarstellend erwähnen, dass ich mich nicht allein aufgrund der bloßen Existenz einer oder mehrerer Videokameras schon mit ausführlichen Rechtsbelehrungen versehenen Anschuldigungen an den Verantwortlichen wende. Die mir von Gesetzes wegen auferlegte Unparteilichkeit gebietet es vielmehr, dem Verantwortlichen zunächst Gelegenheit zur Stellungnahme zu dem mir vorgetragenen Sachverhalt zu geben. Außerdem hat sich in der Vergangenheit nur zu oft gezeigt, dass sich der Beschwerdesachhalt anders darstellte, als es die Petenten mir gegenüber vortrugen und als es auch für mich zunächst den Anschein hatte.

Zurück zum konkreten Fall: Am darauffolgenden Tag meldete sich der Geschäftsführer der besagten Firma telefonisch beim Beschwerdeführer und versuchte diesem zu erklären, dass die Firma nicht (mehr) Eigentümer oder Nutzer des fraglichen Grundstücks sei und er demzufolge auch die Auskunftsanfrage nicht beantworten könne. Was folgte, war offensichtlich ein verbaler Schlagabtausch, in dem der Beschwerdeführer mit seinen datenschutzrechtlichen Kenntnissen zu punkten versuchte. Am selben Tag noch verfasste er eine schriftliche Zusammenfassung des Telefongesprächs und sandte dieses an die E-Mail-Adresse des Geschäftsführers. In belehrender Art erneuerte er darin nochmals sein Auskunftsbegehren. Der Geschäftsführer indes wiederholte per E-Mail sein vorheriges telefonisches Vorbringen, wonach die Firma nicht Eigentümer oder Nutzer des betreffenden Grundstücks sei und er deshalb auch keine Auskunft erteilen könne.

Daraufhin recherchierte der Geschäftsführer seinerseits nach dem Beschwerdeführer. Da letzterer auch als Datenschutzbeauftragter anderer Unternehmen fungierte, stieß er schnell auf dessen Arbeitgeber. Dessen Geschäftsfeld erstreckte sich auf Datenschutzfragen, was den

Geschäftsführer ein diesbezüglich fragwürdiges Geschäftsmodell sowie einen beruflichen Zusammenhang vermuten ließ. Dementsprechend ging er davon aus, dass der Arbeitgeber auch über den bisherigen „Schlagabtausch“ informiert sei. So sah er sich veranlasst, den Arbeitgeber via E-Mail auf die „Freizeitaktivitäten“ seines Mitarbeiters aufmerksam zu machen. Gleichwohl hatte dieser keine Kenntnis der privaten Aktivitäten seines Mitarbeiters, was zu weiteren Verwicklungen und gegenseitigen Vorwürfen – auf Einzelheiten dazu verzichte ich an dieser Stelle – der nunmehr drei beteiligten Personen und einer erweiterten Beschwerde des Mitarbeiters bei mir führte.

Festzuhalten bleibt, dass meine Behörde im Ergebnis fast grundlos mit einem komplizierten Gemengelage aus persönlichem Fehlverhalten, quasi-aufsichtsbehördlichem Auftreten, datenschutzrechtlichen und auch zivilrechtlichen Fragestellungen konfrontiert worden ist, die bei einem bloßen Abwarten auf der Seite des Beschwerdeführers nicht entstanden wäre. Zudem sind durch dieses Vorgehen weitere datenschutzrechtliche Konflikte, so etwa die Einbeziehung des Arbeitgebers des Beschwerdeführers, regelrecht provoziert worden. Ein einfacher Blick ins Handelsregister hätte zu der Kenntnis verholfen, dass die im Internet zu findenden Angaben nicht mehr aktuell waren und die Sicherheitsfirma als vermeintlicher Verantwortlicher bereits vor Jahren ihren Geschäftssitz verlegt hatte. Damit wäre die ganze Aufregung vermeidbar gewesen.

Ich habe dem Beschwerdeführer deutlich gemacht, dass er in dieser Sache klar über das Ziel hinausgeschossen ist und dem Datenschutz, für den er doch selbst beruflich tätig war, keinen guten Dienst erwiesen hat. Nichtsdestoweniger und trotz allen Ärgers war der Aufsichtsfall aber auch für den Geschäftsführer der Sicherheitsfirma Anlass und Gelegenheit, sich eingehender mit den auch an sein Unternehmen gestellten datenschutzrechtlichen Anforderungen, insbesondere dem Auskunftsrecht nach Art. 15 DSGVO und der Zulässigkeit von Datenübermittlungen zu befassen.

Was die den ganzen Ärger auslösenden Videoüberwachungskameras angeht, habe ich den aktuellen Grundstückseigentümer ermitteln und zum Sachverhalt befragen können. Wie er mir mitteilte, seien die Kameras bereits beim Kauf des Grundstücks vorhanden gewesen, jedoch wären die Anschlusskabel durchtrennt und auch sonst gebe es diesbezüglich keine weitere Technik, mithin handele es sich um Kameraattrappen. Den Beschwerdeführer würde er gern auf eine Tasse Kaffee in seinen in unmittelbarer Nähe befindlichen Gewerbebetrieb einladen. Ich habe dies so an den Beschwerdeführer weitergegeben, allerdings keine Kenntnis darüber, ob es zu einem entsprechenden Treffen gekommen ist.

3.4 Recht auf Datenübertragbarkeit, Sonstiges

3.4.1 Übermittlung der Gehaltsabrechnung

Im Rahmen einer Beschwerde wurde ich mit der Frage konfrontiert, ob Arbeitnehmer gegenüber ihrem Arbeitgeber einen Anspruch auf Erstellung und Übertragung der Gehaltsabrechnung in maschinenlesbarer Form haben.

Nach Art. 20 Datenschutz-Grundverordnung (DSGVO) hat die betroffene Person das Recht, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten.

Ich teilte dem Petenten mit, dass ein derartiger Anspruch gegenüber dem (ehemaligen) Arbeitgeber nicht besteht. Die Übermittlung der Gehaltsabrechnung in maschinenlesbarer Form ist nicht Gegenstand des Auskunftsanspruches im Rahmen von Art. 20 DSGVO, weil diese Daten nicht vom betroffenen Arbeitnehmer dem Arbeitgeber zur Verfügung gestellt werden, sondern der Arbeitgeber erstellt selbständig – lediglich unter Nutzung der Arbeitnehmerdaten – die Gehaltsabrechnung und nutzt dazu unter anderem Angaben des Arbeitnehmers.

4 Pflichten Verantwortlicher und Auftragsverarbeiter

4.1 Verantwortung für die Verarbeitung, Technikgestaltung

4.1.1 Prüfwerkzeuge für Websites und Anforderungen an Betreiber von Websites

Ich bekomme nach wie vor eine hohe Anzahl an Beschwerden über Websites. Typische Beschwerdesachverhalte sind undurchsichtige Datenschutzerklärungen, komplizierte, irreführende oder fehlende Cookie-Banner oder Datenübermittlungen ohne Zustimmung in unsichere Drittländer. Ich gehe allen Beschwerden nach und überprüfe dabei regelmäßig Websites auf ihr Verhalten.

Eines der nützlichsten Werkzeuge ist der vom Europäischen Datenschutzbeauftragten entwickelte Website Evidence Collector, abrufbar unter edps.europa.eu. Das Tool ist als quelloffene Software konzipiert und frei erhältlich. Der Entwickler ist auch für Vorschläge und Ergänzungen offen beziehungsweise kann das Werkzeug mit Hilfe von Skripten für eigene Zwecke angepasst werden. Der Website Evidence Collector wird von mir bei Prüfungen in einer Laborumgebung auf einer Linux-Arbeitsstation eingesetzt. Dem Werkzeug wird dabei die Adresse einer zu prüfenden Website übergeben und im Hintergrund wird die Website von einem Chrome-Browser mit leerem Nutzerprofil angesurft. Der Website Evidence Collector erstellt ein Prüfprotokoll. Daraus ergeben sich alle Verbindungen einer Website zu weiteren Websites – beispielsweise zu Werbenetzwerken, sozialen Medien, von Dritten gehostete Schriftarten – sowie alle im Browser hinterlegten Web-Storage-Objekte (Cookies und DOM-Storage). Zusätzlich werden Screenshots der Website erstellt und alle Objekte in einem Bericht und einer lokalen Ablage zusammengefasst. Das Werkzeug gestaltet die Prüfung von Websites damit sehr effizient. Die Ergebnisse werden dann ausgewertet und geprüft, inwieweit für jede nachgewiesene Verbindung zu Dritten, was einer Datenübermittlung von Nutzungsdaten wie IP-Adresse des Nutzers entspricht, und für jedes Cookie oder Web-Storage-Objekt, was eine Profilbildung erlaubt, eine Rechtsgrundlage vorhanden ist.

Ein Blick in die Datenschutzerklärung hilft in vielen Fällen nicht weiter. Leider erlebe ich es recht häufig, dass Prüfergebnis und damit die Realität wenig mit den mehr oder weniger wortreich gestalteten Datenschutzerklärungen zu tun haben. Entweder werden die eingebundenen Dienste gar nicht benannt oder es werden Dienste benannt, die gar nicht auf der Website eingebunden sind. Oder es werden ein paar allgemeine Aussagen zum Einsatz von Cookies getroffen, was bei genauem Blick auf die Website in den meisten Fällen dann auch nicht stimmt. Eine solche Datenschutzerklärung ist rechtswidrig.

Gleiches gilt für Datenverbindungen und Web-Storage für die eine Einwilligung erforderlich ist. Tauchen solche Angaben im Website Evidence Collector auf, ist ein Rechtsverstoß gegeben, da das Werkzeug eine Website ohne Interaktion ansurft und somit keine Einwilligung erteilt werden kann. In der Praxis erlebe ich häufig Verantwortliche, die sich der Verstöße gar nicht bewusst sind und in aller Regel bemüht sind die beanstandeten Verstöße abzustellen. Dennoch kann ich jedem Verantwortlichen nur empfehlen, das eigene Webangebot und die Datenschutzerklärung einem kritischen Blick zu unterziehen. Eine Website kann von jedem geprüft werden und ist oftmals der erste Kontakt zu einem Kunden oder Bürger. Wenn einem kundigen Besucher bereits an dieser Stelle Datenschutzverstöße auffallen, ist der erste Eindruck schon getrübt. Vor allem dann, wenn eine Datenschutzerklärung mit dem Standard-Satz „Wir nehmen den Schutz Ihrer persönlichen Daten sehr ernst!“ beginnt. Viele Beschwerden bei mir sind vermeidbar, wenn das Thema Website ernst genommen wird. Neben dem Website Evidence Collector setze ich weitere Tools wie die Burp Suite oder in Browsern vorhandene Analyse-Werkzeuge ein, um Datenmittschnitte zu erzeugen und das Verhalten von Websites zu untersuchen.

Zur Zulässigkeit von Datenverbindungen sowie dem Setzen von Cookies und Web-Storage-Objekten finden sich zahlreiche Hinweise in der Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien, abrufbar unter datenschutzkonferenz-online.de. Speziell für den Einsatz von Google Analytics haben die Aufsichtsbehörden Hinweise erarbeitet, welche ebenfalls auf der Website der Datenschutzkonferenz abgerufen werden können. Eine Leseempfehlung möchte ich auch für die FAQ des Landesbeauftragten für Datenschutz und Informationsfreiheit des Landes Baden-Württemberg aussprechen, der häufig in der Praxis anzutreffende Fehler und deren Vermeidung anschaulich darstellt, abrufbar unter baden-wuerttemberg.datenschutz.de.

Mit Blick auf das Urteil des Bundesgerichtshofs vom 28. Mai 2020 in dem Verfahren des Bundesverbandes der Verbraucherzentralen gegen die als Adresshändler und Gewinnspielbetreiber tätige Planet49 GmbH ist insbesondere beim Einsatz von Cookies oder Web-Storage-Objekten, die eine potenzielle Profilbildung erlauben, nach derzeitiger Lage immer eine Einwilligung erforderlich (vgl. 9.4).

4.1.2 Standard-Datenschutzmodell (SDM)

Im Jahr 2020 hat die Unterarbeitsgruppe SDM damit begonnen, Bausteine, welche im Jahr 2018 zunächst als Erprobungsbausteine durch einige der am SDM aktiv beteiligten Aufsichtsbehörden veröffentlicht wurden, der Datenschutzkonferenz (DSK) vorzulegen und damit einen breiten Konsens in der Anwendung zu erwirken. Im Jahr 2020 konnten insgesamt sieben Bausteine verabschiedet und veröffentlicht werden:

- Aufbewahren
- Dokumentieren
- Protokollieren
- Trennen
- Löschen
- Berichtigen
- Einschränken

Diese sind aufgrund des Vorsitzes des Arbeitskreises Technik der DSK auf der Website des Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern in jeweils aktueller Version zu finden: datenschutz-mv.de

Die Bausteine decken verfahrenskritische Bestandteile einer Verarbeitung in Ergänzung zum methodischen Teil des SDM mit geeigneten Maßnahmen und Hinweisen zum Vorgehen ab und können damit ein im SDM beschriebenes ganzheitliches Datenschutzmanagement etablieren helfen.

Im Jahr 2020 sind mir mehrere Datenschutzkonzepte auf Grundlage des SDM zur Stellungnahme vorgelegt worden. Dabei wurde deutlich, dass insbesondere der Teil B des SDM, Anforderungen der DSGVO, Verantwortlichen dabei hilft, die komplexen Anforderungen der DSGVO auf ein konkretes Verfahren anzuwenden und damit eine Prüfbarkeit einer Verarbeitung herzustellen.

4.1.3 „Autofill“-Funktion – Voreinstellung bei E-Commerce-Auftritt

Die Kundin eines Shopping-Portals wandte sich mit einer Beobachtung, die voreingestellte und nur manuell abwählbare „Autofill“-Funktion (eine Daten eintragende automatisierte Ausfüllunterstützung) betreffend, an mich. Mit Einverständnis einer ebenfalls betroffenen Bekannten gab sie an ihrem Endgerät deren E-Mail-Adresse und Postleitzahl ein und erhielt die vollständige Anschrift, das Geburtsdatum und die Telefonnummer ihrer Bekannten angezeigt. Ich hatte dies daraufhin überprüft und feststellen können, dass dies tatsächlich serverseitig ohne Bindung an ein passendes Cookie auf jedem beliebigen Endgerät ausgegeben werden konnte. Bedingung war lediglich, dass die „Autofill“-Funktion bei Ersteingabe durch den Berechtigten nicht abgewählt worden war.

Im Ergebnis wurde für das Shopping-Portal eine datenschutzkonforme Umstellung vorgenommen. Ohne bereits auf dem Gerät befindliche Cookies findet demnach fortan keine automatische Vorausfüllung beziehungsweise namentliche Begrüßung mehr statt.

Es ist nicht auszuschließen, dass Voreinstellungen auch bei anderen Portalen zum Einsatz kommen. Mit Art. 32 Datenschutz-Grundverordnung lassen sich derartige Prozesse nicht in Einklang bringen. Betroffenen Personen ist zu raten, bei noch nicht selbst erprobten E-Commerce-Auftritten sich mit der eigenen Technik und den Funktionalitäten des Anbieters zunächst intensiver vertraut zu machen.

4.1.4 Authentifizierung per IBAN bei telefonischer Zählerstandsmeldung

Das Handeln eines Versorgungsunternehmens war Gegenstand der Beschwerde einer betroffenen Person, die Zählerstände selbst telefonisch mitteilen wollte. Von der Serviceperson des Unternehmens wurde diese am Telefon zur Durchgabe ihrer vollständigen IBAN aufgefordert. Alternative Möglichkeiten zur Feststellung der Authentifizierung seien ihr nicht angeboten worden und man habe sich hierbei auf interne Anweisungen berufen.

Auf Nachfrage wurde mir seitens des Unternehmens bestätigt, dass die vollständige IBAN als geeignetes Instrument zur Authentifizierung des einmeldenden und vertraglich dazu berechtigten Kunden durch das Service-Center geprüft werde und dass zum Beispiel die letzten vier Ziffern der Kontoverbindung als nicht ausreichend befunden würden. Jedoch habe der Beschwerdevorgang insoweit nicht den internen Weisungen entsprochen, wonach Kunden, die sich gegen den Abgleich der IBAN aussprechen, ein Ersatzkriterium (beispielsweise die Höhe des monatlichen Abschlags) angeboten werden sollte. Das Unternehmen hatte mir dazu eine erneute Klarstellung an das Service-Personal zugesichert und in einem späteren Umsetzungsbericht mitgeteilt, dass es sich aufgrund meiner Befassung nochmals grundsätzlich mit der Thematik befasst habe und sich im Ergebnis auf eine Reduktion der IBAN-Abfrage (auf die letzten sechs Ziffern) beschränke.

Dass die Anforderungen an die Authentifizierung von Fernsprech-Teilnehmern im Zuge neuester Entscheidungen von Aufsichtsbehörden und Rechtsprechung in Richtung erhöhter Sicherheit angepasst werden, kann kaum verwundern. Die Kontrolle der IBAN auf die letzten vier Ziffern zu beschränken, genügt aufgrund der weiten Verbreitung dieser Maskierung wohl nicht. Es sollte vom Grundsatz jedoch bei als sensibel empfundenen Daten regelmäßig nur ein zureichender Teildatensatz abgefragt werden. Demgegenüber wird es auf Seiten der Kundenbetreuung, was den Zugang zu vollständigen Informationen betrifft, auf Funktion und den Aufgabenumfang des Mitarbeiters ankommen. Sollen Anrufer möglichst von einem einzigen Ansprechpartner – zum Beispiel auch in Hinblick auf Aktualisierung von Stammdaten – betreut werden, ist der volle Einblick auf die Kundendaten erforderlich. Soweit ein abgestufter Zugang zu Kundendaten umgesetzt worden ist, wird auch eine Reduktion der sichtbaren IBAN auf sechs Stellen vorzuziehen sein.

Das Thema einer sicheren und zugleich datensparsamen Authentifizierung in der Kundenbetreuung befindet sich auch aktuell im Fokus der Datenschutzaufsichtsbehörden und der Gerichte (vgl. 9.5 zu der Entscheidung des LG Bonn vom 11. November 2020 - 29 OWi 1/20).

4.1.5 WhatsApp-Gruppe in Vertriebsstrukturen unter Einbindung Selbständiger

Ein selbständiger Vertriebsmitarbeiter eines Unternehmens hatte sich bei meiner Behörde darüber beschwert, dass sämtliche selbständigen Vertriebsmitarbeiter dieses Unternehmens in einer Chat-Gruppe eines prominenten Messaging-Dienstanbieters teilnahmen, um sich dort über Abschlüsse auszutauschen.

Der berufliche Einsatz von Messaging-Diensten ist zwar grundsätzlich problematisch. Wenn es sich allerdings wie hier um eine freiwillige (!) Teilnahme von Selbständigen handelt, ist dagegen zunächst nichts einzuwenden, solange die tatsächlichen Voraussetzungen einer informierten und freiwilligen Einwilligung vorliegen. Zusätzlich waren auch Kundendaten betroffen, da die geteilten Informationen bisweilen Namen der Auftraggeber, Adressen und Auftragsvolumina umfassten. Derartige personenbezogene Daten unterliegen grundsätzlich dem Datenschutz und sind entsprechend angemessen zu schützen.

Dieser Schutz ist allerdings nicht absolut, sondern hat sich an dem konkreten Gefährdungspotential für die Betroffenen auszurichten. Hier lag standardmäßig eine dem Industriestandard entsprechende Ende-zu-Ende-Verschlüsselung vor, so dass nur Gruppenmitglieder die entsprechenden Daten einzusehen vermochten. Die Einordnung derartiger Datenverarbeitungen hängt entscheidend ab vom Informationsgehalt und der Sensibilität der verarbeiteten Daten sowie dem aus deren konkreter Verarbeitung erwachsenden Risikopotential für die Betroffenen. Vorliegend war ausschlaggebend, dass lediglich Grobdaten zu Solarinstallationen betroffen waren, die allenfalls sehr geringe Rückschlüsse auf die Betroffenen erlaubten.

Ein teaminterner Austausch über Grobinformationen zu Kunden eines gemeinsamen Auftraggebers kann branchenüblich sein und ist aus meiner Sicht nicht zu beanstanden, soweit es sich um lediglich wenig sensible Daten der wirtschaftlichen Sphäre handelt, deren Missbrauchsgefahr begrenzt bleibt. Allerdings sind die so entstehenden datenschutzrechtlichen Risiken durch technische und organisatorische Maßnahmen des Verantwortlichen einzuhegen, insbesondere sind die teilnehmenden Selbständigen datenschutzrechtlich zu sensibilisieren.

4.1.6 Fahrtkostenerstattung: Umgang mit Versichertendaten durch Krankenkasse

Der Umgang mit personenbezogenen Versichertendaten durch den Verantwortlichen, hier eine gesetzliche Krankenkasse, war Gegenstand einer Anfrage im Rahmen der Antragstellung auf Erstattung von Fahrkosten im Zusammenhang mit einer stationären Behandlung.

Zum Sachverhalt: Das Formular auf Erstattung von Fahrkosten wird vorrangig verwendet, wenn Versicherte erstattungsfähige Fahrten, wie hier im Zusammenhang mit einem stationären Aufenthalt, mit öffentlichen Verkehrsmitteln oder einem privaten Pkw durchführen. Es bedarf der ärztlichen Bestätigung auf der Rückseite dieses Antrags, an welchen Behandlungstagen, welches Verkehrsmittel medizinisch notwendig war, um die Höhe des Erstattungsbetrags ermitteln zu können.

Der Antrag ist bereits aus Servicegründen mit den Versichertendaten gefüllt: Name, Anschrift, Krankenversicherungsnummer.

Die Vorderseite füllt der Versicherte selbst aus. Die Möglichkeit, die bei der Krankenkasse gespeicherte Bankverbindung des Kunden maschinell in das Formular zu übernehmen, besteht und wird vordergründig in den Filialen bei persönlicher Übergabe an den Kunden oder bei telefonischer Anforderung genutzt. Auf der Website der Krankenkasse ist der Antrag nur als Blanko-Formular verfügbar. Wird der Antrag auf dem Postweg versendet, erhält der Versicherte dazu ein Anschreiben sowie eine Kundeninformation.

Den mit Versichertendaten und gegebenenfalls Bankverbindung vorausgefüllten Erstattungsantrag erhält immer nur der Versicherte oder sein Betreuer beziehungsweise Bevollmächtigter selbst, nicht der Arzt oder eine andere medizinische Einrichtung seitens der Krankenkasse. Erstattungsanträge mit der Bankverbindung bieten nach Auskunft der betreffenden Krankenkasse den Vorteil, dass weniger Drittempfängerbankverbindungen angegeben werden, die Bankverbindung für den Sachbearbeiter als geprüft und richtig dokumentiert ist sowie die (Beleg-)Lesefähigkeit erhöht wird.

Nach Mitteilung der Krankenkasse können die Kunden dabei dann selbst entscheiden, ob sie diesen Antrag an den behandelnden Arzt weiterreichen wollen oder nicht. Darüber hinaus kann – so die Mitteilung der Krankenkasse – der Versicherte beispielsweise seine Bankverbindung unkenntlich machen oder auch ein Blanko-Formular von der Krankenkasse anfordern, bevor er den Antrag an Dritte weitergibt.

Im Ergebnis wird daher seitens der Krankenkasse das vorausgefüllte Formular nur dem Kunden und nicht einem Dritten zur Verfügung gestellt.

Aufgrund der somit in die Entscheidung des Versicherten gestellten Handlungsweise habe ich keine datenschutzrechtlichen Bedenken gegen die Verfahrensweise geltend gemacht. So der Versicherte Bedenken gegen die Nutzung eines vorausgefüllten Formulars hat, rege ich an, wie seitens der Krankenkasse beschrieben zu verfahren.

4.2 Gemeinsam Verantwortliche

4.2.1 Gemeinsam Verantwortliche bei der Videoüberwachung in Fußballstadien

Höherklassige Fußballvereine (ab Regionalliga) sind aufgrund von Verbandsvorgaben regelmäßig gefordert, auch Videoüberwachungsanlagen in den von ihnen genutzten Stadien vorzuhalten.

In einem konkreten Fall war durch mich im Hinblick auf die inhaltliche Ausgestaltung der diesbezüglichen Hinweisschilder die Frage zu klären, wer auf diesen Schildern als Verantwortlicher zu benennen ist.

Angesichts der Umstände, dass die Vereine oftmals nicht Eigentümer ihrer – auch noch für andere Events genutzten – Spielstätten sind, wobei es neben dem Eigentümer zumeist auch noch eine Betreibergesellschaft gibt, und an den Spieltagen zudem noch die Polizei in den Betrieb der Videoüberwachungsanlagen, mindestens in die Nutzung der Videoaufnahmen, involviert ist, gibt es in Bezug auf die Frage, wer jeweils oder generell Verantwortlicher im Sinnes des Datenschutzrechts ist, keine allgemeingültige Antwort.

In dem mir vorliegenden Fall war es so, dass der Fußballverein im Stadion nur Mieter war. Bei eigenen beziehungsweise nicht polizeilich begleiteten oder geführten Veranstaltungen nutzt der Eigentümer beziehungsweise dessen Betreibergesellschaft die Videoüberwachungsanlage selbst. Ist die Polizei involviert, wie beispielsweise bei Fußballspielen, erfolgt die Anlagennutzung und -steuerung ausschließlich durch die Polizei. Für die Aufzeichnungen, insbesondere deren Sicherheit und Speicherdauer bleibt jedoch die Betreibergesellschaft in der Verantwortung. Die Videoaufzeichnungen werden von der Polizei beziehungsweise der Betreibergesellschaft zur Verfolgung von Straftaten oder Verstößen gegen die Stadionordnung verwendet. Weiterhin zu beachten ist, dass der – durch die Betreibergesellschaft vertretene – Eigentümer bei Fußballspielen regelmäßig das Hausrecht an den Fußballverein als Veranstalter überträgt. Auch dieser hat dann gegebenenfalls natürlich Interesse an den Videoaufzeichnungen, etwa wenn er von seinem Verband infolge durch seine Fans verursachten Vorkommnissen in Haftung genommen wird.

Bei der Vielzahl der Beteiligten (Eigentümer, Betreiber, Veranstalter, Polizei) stellt sich die Frage, wer in Bezug auf die Videoüberwachung im datenschutzrechtlichen Sinne Verantwortlicher ist und damit den Informationspflichten des Art. 13 Datenschutz-Grundverordnung (DSGVO) unterliegt. Nach Art. 4 Nr. 7 DSGVO ist „Verantwortlicher“ die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Grundsätzlich kommen dafür zunächst einmal der Betreiber, der Veranstalter und die Polizei in Betracht.

Die temporäre Übertragung des Hausrechts vom Betreiber an den Veranstalter bedeutet aber nicht zugleich auch die Übertragung der Verantwortung für den Betrieb der Videoüberwachungsanlage. Diese verbleibt beim Betreiber einerseits beziehungsweise geht in den betreffenden Fällen zum Teil auch an die Polizei andererseits über. Ein Zugriff auf die Videoaufzeichnungen durch den Hausrechtsinhaber zur Verfolgung eigener Zwecke, etwa zur Identifizierung und Inanspruchnahme von Störern, ist nach Absprache möglich und auch zulässig, Art. 6 Abs. 1 Buchst. f DSGVO. Dies impliziert aber keine Entscheidungsbefugnis in Bezug auf die Zwecke und Mittel der Videoüberwachung (Art. 4 Nr. 7 DSGVO).

Im Übrigen handelt es sich aber um einen Fall der gemeinsamen Verantwortlichkeit von Betreiber und Polizei. Als Besonderheit ist hier zu beachten, dass sich der Eigentümer im Anwendungsbereich der Datenschutz-Grundverordnung (DSGVO) bewegt, während für die Polizei die Vorgaben der Richtlinie (EU) 2016/680, das heißt hier des Sächsischen Datenschutz-Umsetzungsgesetzes (SächsDSUG) beziehungsweise des Sächsischen Polizeivollzugsdienstgesetzes, maßgebend sind. Im Anwendungsbereich der Datenschutz-Grundverordnung ist die gemeinsame Verantwortlichkeit in Art. 26 DSGVO geregelt, im Anwendungsbereich der Richtlinie (EU) 2016/680 ist die Regelung des § 19 SächsDSUG einschlägig.

Die gemeinsame Verantwortlichkeit muss aus den Hinweisschildern auf die Videoüberwachung hervorgehen. Eine Variante wäre ein spezielles Hinweisschild nur für die polizeiliche Videoüberwachung und damit nur auf bestimmte Veranstaltungen bezogen, was aber an praktischen Fragen scheitert. Zum einen führte das zu einer eher unübersichtlichen Doppelbeschilderung, denn auch der Betreiber muss natürlich über seine Videoüberwachung informieren, zum anderen sind vorliegend die Einsatzfälle der (auch) polizeilichen Videoüberwachung nicht so klar definierbar und voraussehbar. Insbesondere beschränkten sie sich nicht auf Fußballspiele des Stadionhauptmieters. Nur temporär beziehungsweise veranstaltungsbezogen sichtbar zu machenden Hinweisschilder wurden von den Verantwortlichen wegen Unpraktikabilität ausgeschlossen. Als Lösung wurde daher ein Hinweisschild präferiert, welche sowohl Betreiber als auch Polizei als Verantwortliche ausweist.

Als Gemeinsam Verantwortliche haben Betreiber und Polizei auch zusammen die sich aus der Datenschutz-Grundverordnung beziehungsweise dem Sächsischen Datenschutz-Umsetzungsgesetz ergebenden Verpflichtungen zu erfüllen. Dies bedeutet auch, dass betroffene

Personen bei der Wahrnehmung ihrer Rechte nicht gegenseitig zwischen den beiden Verantwortlichen verwiesen werden dürfen, auch wenn sich der angesprochene Verantwortliche sachlich nicht zur Erfüllung der Betroffenenrechte berufen sieht (vgl. Art. 26 Abs. 3 DSGVO, § 19 Satz 4 SächsDSUG). Die gemeinsam Verantwortlichen haben also die Realisation der Betroffenenrechte intern zu organisieren und diesbezüglich eingehende Anträge gegebenenfalls an den anderen Verantwortlichen weiterzuleiten. Betroffene Personen können frei wählen, an welchen Verantwortlichen sie sich mit ihrem Anliegen wenden. Eine entsprechende abzuschließende Vereinbarung gemäß Art. 26 Abs. 1 DSGVO ist auch hierfür erforderlich.

4.2.2 Gemeinsam Verantwortliche: Eigentümer und Hausverwaltung

Eine Hausverwaltung einer Eigentümeranlage legte mir mit der Bitte um Beratung einen Vertragsentwurf vor, der einer „Vereinbarung über die gemeinsame Verarbeitung von Daten nach Art. 26 DSGVO“ zwischen Eigentümern und Hausverwaltung dienen sollte. Darin sollten die Eigentümer für den „Zweck der gemeinsamen Verarbeitung personenbezogener Daten“ unter anderem zur Übernahme einer diesbezüglichen Vergütung zugunsten des Verwalters gebracht werden. Eine weitere vertragliche Bestimmung enthielt die Klausel, wonach die Parteien gemäß Art. 82 Abs. 5 DSGVO entsprechend ihrer Anteile zu haften hätten.

Ich habe der Hausverwaltung zur Aufgabe des Vorhabens aufgefordert und darauf hingewiesen, dass die Hausverwaltung einer Wohnungseigentümergemeinschaft alleiniger Verantwortlicher für die Verarbeitung personenbezogener Daten in Zusammenhang mit den Tätigkeiten ist, die ihr aus dem Hausverwaltungsvertrag übertragen wurden. Dies gilt im Übrigen unabhängig davon, ob es sich um die Verwaltung von Gemeinschafts- oder Sondereigentum handelt.

Dass die im Gesetz über das Wohnungseigentum und das Dauerwohnrecht genannte Gemeinschaft der Wohnungseigentümer datenverarbeitende Stelle und Verantwortlicher ist, ist auch zutreffend. Diese setzt aber durch Beschluss gemäß § 19 einen Verwalter ein, der umfangreiche Aufgaben für die Eigentümergemeinschaft beziehungsweise den einzelnen Eigentümer selbständig wahrnimmt. Die Eigentümer übertragen diese Verantwortlichkeit damit auf den Verwalter. Dieser ist daher datenschutzrechtlich auch allein Verantwortlicher für die mit seiner Tätigkeit verbundene Datenverarbeitung. Die gemeinsame Verantwortung nach Art. 26 DSGVO zeichnet sich hingegen gerade dadurch aus, dass die Verantwortlichen gemeinsam die Zwecke der Verarbeitung und die hierfür eingesetzten Mittel festlegen (vgl. Kurzpapier Nr. 16 – Gemeinsam für die Verarbeitung Verantwortliche, abrufbar auf datenschutzkonferenz-online.de, Art. 26 DSGVO). Eine derartige Verbindung, die auch zu einer Gesamtschuldnerschaft führen würde, besteht im Verhältnis Eigentümer und Hausverwaltung aber eben gerade nicht. Die Eigentümer verarbeiten zudem auch weiterhin personenbezogene Daten für eigene Zwecke und separiert von der Hausverwaltung.

Diese Einschätzung gilt im Ergebnis nicht allein für die WEG-Verwaltung, sondern auch für die vertraglich festgelegte Verwaltung sonstiger Immobilien.

Eine entgegenstehende Entscheidung des Amtsgerichts Mannheim überzeugt nicht in den Gründen (vgl. AG Mannheim, Urteil vom 11. September 2019 - 5 C 1733/19).

4.2.3 Lettershop-Verfahren – keine Gemeinsam Verantwortlichen

Vereinzelt wird die Auffassung vertreten, dass Auftraggeber und Werbebrief-Versender Gemeinsam Verantwortliche seien.

Bei dem sogenannten „Lettershop"-Verfahren handelt es sich um einen Prozess, bei dem der Auftraggeber einer Werbesendung den Auftragnehmer, den „Lettershop" damit betraut, die Sendung zu personalisieren. Zum Teil stellen die Auftraggeber die Daten der Kunden oder Adressdaten zur Verfügung. Zum Teil verfügt das werbende Unternehmen aber gar nicht über die Adress- und Kommunikationsdaten, sondern nur der Auftragnehmer, der die Beschriftung der Umschläge oder die Versendung einer E-Mail-Sendung an Adressaten durchführt oder dieser erhält die Adressen zeitweise von einem dritten Unternehmen.

Die Arbeitsteilung und die Verteilung der personenbezogenen Daten betrachte ich als im Grunde genommen datenschutzfreundlich. Voraussetzung ist allerdings auch, dass die Informationspflichten eingehalten werden und die Datenverarbeitung, was die einzelnen Verantwortlichkeiten der datenverarbeitenden Stellen angeht, transparent gemacht wird. Ansonsten finden sich betroffene Personen in Anbetracht der verteilten Aufgaben beteiligter Unternehmen nicht zurecht und sind dann nicht imstande, ihre Betroffenenrechte, insbesondere Auskunft und Widerspruch gegen Werbesendungen auszuüben (vgl. Art. 15 und 21 Abs. 2 und 3 Datenschutz-Grundverordnung (DSGVO)).

Gleichwohl können auftretende Probleme nach meiner Überzeugung nicht über eine konstruierte Gesamthaftung beziehungsweise Art. 26 DSGVO gelöst werden, so dass über einen ausschließlich über den Adresspool verfügender Verantwortlicher hinaus auch die nicht Daten verarbeitende Stelle in Anspruch genommen werden kann. Eine von einer personenbezogenen Datenverarbeitung entkoppelte datenschutzrechtliche Verantwortung kennt die Datenschutz-Grundverordnung nicht. Verantwortlicher ist allein, wer die Voraussetzungen nach Art. 4 Nr. 7 DSGVO erfüllt. Gemeinsam Verantwortliche sind die am „Lettershop"-Verfahren beteiligten Stellen hingegen regelmäßig nicht. Sonstige zivilrechtliche Zurechnungen können hingegen unter Umständen weitergehend sein.

Zu raten ist den am „Lettershop" beteiligten Stellen gleichwohl, prozessuale Vereinbarungen zur Beantwortung von Betroffenenanliegen einzugehen, um deren bestmögliche und effektive Bearbeitung sicherzustellen.

4.3 Auftragsverarbeitung

4.3.1 Beauftragung eines IT-Dienstleisters durch Kommune

Eine Gemeinde konsultierte mich zur Notwendigkeit einer datenschutzrechtlichen Regelung bei der Beauftragung eines IT-Dienstleisters. Beabsichtigt war, einen solchen zur Einführung, Wartung und Pflege sowie Erweiterung der IT Infrastruktur vertraglich zu binden. Neben den „normalen“ Dienstleistungsbeschreibungen war in dem Vertragsangebot auch eine Verschwiegenheitsverpflichtung integriert, gleichzeitig eine Verpflichtung zur Einhaltung des Datenschutzgesetzes aufgrund der Verarbeitung personenbezogener Daten.

Fraglich war aus Sicht der Gemeinde nun, ob nicht die Verschwiegenheitsverpflichtung ausreichend ist. Begründet wurde dies damit, dass der Dienstleister keine personenbezogenen Daten verarbeiten soll, sondern nur die Einsicht in diese Daten, aufgrund der oben beschriebenen Dienstleistungen nehmen kann. Man wolle daher den Vertrag nicht mit unnötigen Regelungen überfrachten.

In meiner Antwort wies ich darauf hin, dass gemäß Art. 28 Abs. 3 b Datenschutz-Grundverordnung in einem Vertrag zur Auftragsverarbeitung zu gewährleisten ist, „dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen“. Dies gilt auch dann, wenn der Auftrag nicht auf die Verarbeitung personenbezogener Daten gerichtet ist, aber die (technische) Möglichkeit zur Verarbeitung personenbezogener Daten besteht – um auch in diesen Fällen den Datenschutz zu gewährleisten.

Der Bürgermeister übermittelte mir einen „herzlichen Dank für die schnelle Rückantwort“ und teilte mit: „Das hat uns sehr geholfen.“ Ich gehe daher davon aus, dass meine Antwort bei dem Vertragsschluss berücksichtigt wurde.

4.4 Verzeichnis der Verarbeitungstätigkeiten, Kooperationspflicht mit der Aufsichtsbehörde

Zum Verzeichnis der Verarbeitungstätigkeiten vergleiche den Beitrag unter 1.2 zur Umsetzung der Dokumentation bei Kommunen.

Art. 31 Datenschutz-Grundverordnung (DSGVO) normiert eine allgemeine Pflicht der Verantwortlichen und der Auftragsverarbeiter mit meiner Behörde zu kooperieren. Aufsichtliche Verfahren werden seitens meiner Dienststelle regelmäßig mit einer formlosen Aufforderung zur Auskunft oder Stellungnahme eingeleitet. In Einzelfällen ergeht auch direkt ein Hinweis. Lediglich bei gravierenden Verstößen oder soweit der Verantwortliche der

Auftragsverarbeiter nicht die zu meiner Aufgabenerfüllung notwendigen Auskünfte bereitstellt, was in selteneren Fällen durchaus geschieht, ordnet meine Behörde im Wege des Verwaltungsakts mit formellem Heranziehungsbescheid an. Insgesamt ist zu konstatieren, dass sich die pflichtigen Stellen bemüht und normgemäß verhalten. Zwar ist ein Verstoß gegen Art. 31 gemäß Art. 83 Abs. 4 Buchst. a (DSGVO) bußgeldbewehrt. Allerdings wurde seitens meiner Dienststelle deswegen noch kein Ordnungswidrigkeitenverfahren eingeleitet.

4.5 Sicherheit der Verarbeitung

4.5.1 Datenschutzgerechte Entsorgung von Geräten im medizinischen Bereich

Eine freiberufliche Hebamme fragte an, wie Sie ihre beruflich genutzten technischen Geräte, Smartphone, Laptop et cetera datenschutzgerecht entsorgen beziehungsweise sicherstellen könne, dass personenbezogene Daten datenschutzkonform gelöscht werden.

Ich teilte ihr mit, dass im Falle einer Aussonderung dieser Geräte entsprechende Maßnahmen zur datenschutzgerechten Entsorgung getroffen werden müssen (vgl. Art. 5 und 32 Datenschutz-Grundverordnung).

Werden auf den Datenträgern personenbezogene Daten ohne Gesundheitsbezug und mit überschaubarem Risiko gespeichert, kommt im Einzelfall eine Löschung nach Stand der Technik und die anschließende Möglichkeit einer Weitergabe (zum Beispiel Verkauf) in Frage. Dies kann (zum Beispiel für Smartphones) gegebenenfalls unter Beiziehung eines Dienstleisters bewerkstelligt werden. Für detailliertere Hinweise habe ich auf die entsprechenden Informationen des Bundesamtes für Sicherheit in der Informationstechnik verwiesen.

Für Datenträger auf denen Gesundheitsdaten verarbeitet werden, ist es in aller Regel risikoadäquat eine professionelle Datenträgervernichtung in Anspruch zu nehmen und die Vernichtung entsprechend zu dokumentieren. Entsprechende Dienstleiter sind am Markt verfügbar. Aus Wettbewerbsgründen kann ich jedoch keine Empfehlungen für bestimmte Unternehmen aussprechen. Der Dienstleiter sollte jedoch mindestens nach DIN 66399 „Büro- und Datentechnik – Vernichtung von Datenträgern“ zertifiziert sein und Schutzklasse 2/Sicherheitsstufe 4 anbieten können.

Generell ist eine Vollverschlüsselung sämtlicher mit der Verarbeitung personenbezogener Datenträger anzuraten, um auch für Fälle ungeplanten Verlusts (zum Beispiel Diebstahl/Einbruch) entsprechende Vorkehrungen getroffen zu haben.

4.5.2 Einsatz von privaten Messenger-Accounts und privaten Endgeräten zu beruflichen Zwecken im Beschäftigungsverhältnis

Neuartige Kommunikationsmethoden finden zunehmend bei Unternehmen Verwendung. Der Einsatz derartiger Mittel durch Selbständige oder kleine Gewerbetreibende soll nicht Gegenstand der nachstehenden Betrachtung sein (vgl. dazu aber 4.1.5 zu einer WhatsApp-Gruppe in Vertriebsstrukturen bei Selbständigen). Zurückliegend hatte ich mich bereits zu Messenger-Diensten im Schulbereich geäußert (vgl. Tätigkeitsbericht 2019, 4.1.2., Seite 79 ff.)

Im letzten Berichtszeitraum war ich auch mit der Frage konfrontiert gewesen, ob der Einsatz privater Messenger-Accounts und privater Endgeräte, Smartphones und Tablets, zu dienstlichen Zwecken durch Beschäftigte in Unternehmen statthaft ist. Hierbei wird man Kommunikation ohne weitergehende Verarbeitung personenbezogener Daten betroffener Personen, etwa bei einer Abstimmung zur internen Personalplanung, von einer tiefergehenden Informationsverarbeitung zu unterscheiden haben. Eine beförderte Messenger-Kommunikation über private Systeme mit der damit verbundenen Möglichkeit auch Dateianhänge und voluminöse Inhalte zu verarbeiten, stellt jedenfalls in technischer und organisatorischer Hinsicht eine sicherheitsrelevante Frage dar. Verantwortliche haben zu gewährleisten, dass mit Zugang zu personenbezogenen Daten betraute Beschäftigte nicht in der Lage sind, schutzwürdige Daten in deren private Systeme und Infrastruktur zu transferieren.

Zudem sind Arbeitgeber beziehungsweise Dienstherrn als Verantwortliche grundsätzlich pflichtig, den Beschäftigten die erforderlichen Arbeitsmittel zur Verfügung zu stellen. Wird arbeitgeberseitig entsprechende Informationssicherheitsanforderungen genügende Infrastruktur eingerichtet, ist dies grundsätzlich nicht zu beanstanden. Eine Auslagerung der Datenverarbeitung auf private Endgeräte hingegen, die zudem dazu führen würde, dass Informationen zu privaten Rufnummern und Accounts der Beschäftigten mitverarbeitet werden, ist aber regelmäßig nicht erforderlich und statthaft. Soweit sie einzelarbeitsvertraglich vereinbart und geschuldet ist, ist dies im konkreten Fall und datenschutzrechtlich genauer zu betrachten. In jedem Fall stellt die Verwendung privater Endgeräte, soweit besonders sensible Daten durch den Verantwortlichen verarbeitet werden, zum Beispiel im öffentlichen Dienst oder im Pflege- und Krankenhausbereich, einen gravierenden technisch-organisatorischen und informationssicherheitstechnischen Mangel dar (vgl. Art. 25, 32 Datenschutz-Grundverordnung (DSGVO)). Kommen nämlich private Endgeräte zum Einsatz und werden darüber oder über private Messenger-Accounts personenbezogene, einer Vertraulichkeit unterliegende oder besonders schützenswerte Daten im Sinne von Art. 9 DSGVO verarbeitet, begibt sich der Verantwortliche der Steuerung und Überwachung der Verarbeitung der ihm anvertrauten Daten und der Systemsicherheit. Insbesondere im Bereich des Gesundheitswesens oder anderen Bereichen, in denen sensible Daten verarbeitet werden, ist gemäß Art. 5 DSGVO entsprechendes auszuschließen.

Bei dem Einsatz privater Betriebsmittel ergibt sich zudem das Problem, dass gegebenenfalls die Kontrolle privater Endgeräte der Beschäftigten erforderlich würde, um einen datenschutzgerechten Umgang mit personenbezogenen Daten sicherzustellen und zu kontrollieren. Dabei müssten bei Zugriff des Arbeitgebers oder Dienstherrn auf das private Endgerät oder private angelegte Konten wiederum die datenschutzrechtlichen Vorgaben zum Beschäftigtendatenschutz, insbesondere im Hinblick auf den Grundsatz der Rechtmäßigkeit der Datenverarbeitung, die Freiwilligkeit einer Einwilligung, Verhaltens- und Leistungskontrollen sowie die bestehenden Informations- und Auskunftspflichten eingehalten werden. Zudem wäre eine Verantwortlichkeit der Beschäftigten im Sinne von Art. 4 Nr. 7 der DSGVO für die entsprechenden Datenverarbeitungen auszuschließen.
Meine Behörde hält entsprechendes nicht mit privaten Endgeräten und Konten für datenschutzkonform umsetzbar.

4.6 Meldung von Datenschutzverletzungen

4.6.1 Zuwachs bei gemeldeten Datenpannen

Nach Art. 33 Datenschutz-Grundverordnung (DSGVO) sind Verantwortliche verpflichtet, im Falle der Verletzung des Schutzes personenbezogener Daten unverzüglich und möglichst binnen 72 Stunden nach Bekanntwerden der Verletzung diese der Aufsichtsbehörde zu melden, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.
Im Berichtszeitraum sind bei mir 635 solcher Meldungen eingegangen. Im Vergleich zum vorjährigen Berichtszeitraum entspricht dies einer Steigerung um über 40 Prozent. Damit ist erneut eine erhebliche Zunahme der Meldungen von Datenschutzverletzungen zu verzeichnen.

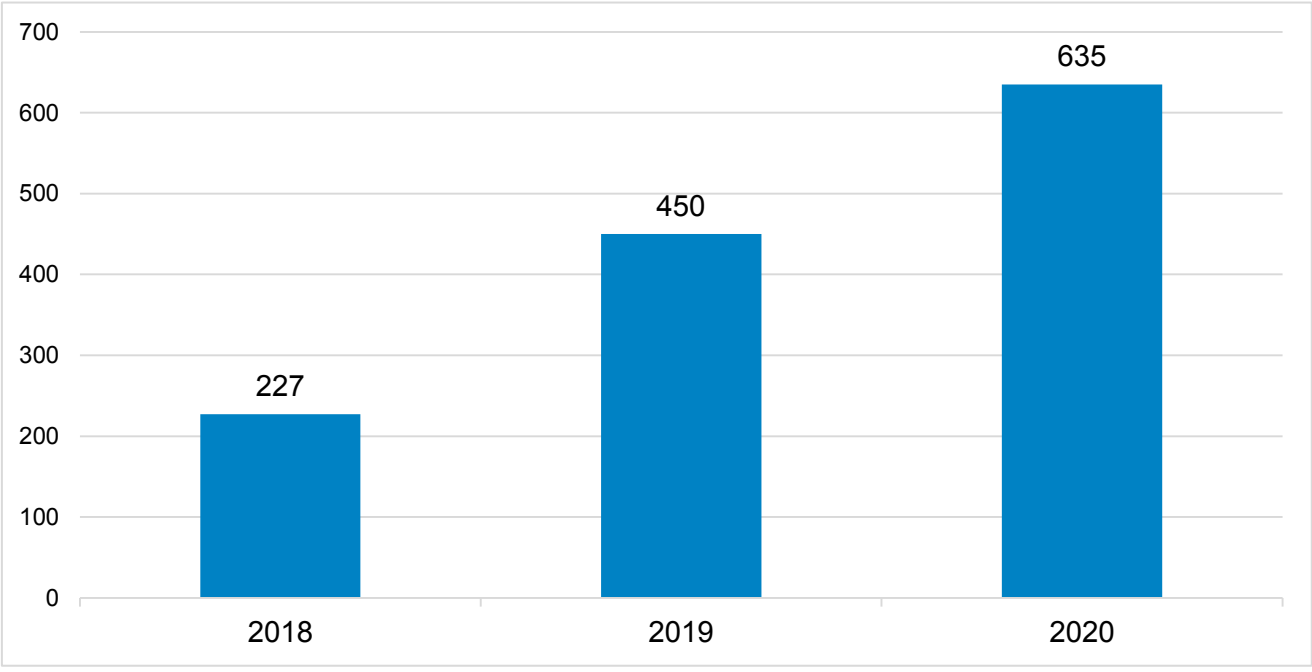


Abbildung 6: Meldungen von Datenschutzverletzungen

Die folgenden Fallgruppen sind im Berichtszeitraum besonders häufig gemeldet worden:

Fehlversand
Der Fehlversand von Unterlagen aufgrund falscher Zuordnung, fehlerhafter Kuvertierung oder Verwechslung der Empfängerperson ist nach wie vor eine der häufigsten Fallgruppen, die gemäß Art. 33 DSGVO bei mir gemeldet wird. Kritisch festzustellen ist, dass in dieser Kategorie der Fallgruppen vielfach Gesundheitsdaten betroffen sind, die an falsche Empfänger übersandt werden. Besonders im Bereich der Gesundheitsdaten ist aufgrund der hohen Sensibilität der Daten und der besonderen Vertraulichkeit grundsätzlich ein besonders hohes Maß an Sorgfalt von der verantwortlichen Stelle zu fordern. Ein hohes Risiko für die Betroffenen ist jedoch glücklicherweise in der Regel nicht festzustellen, da die falschen Empfänger dies regelmäßig der verantwortlichen Stelle anzeigen, die Unterlagen vernichten oder zurücksenden und sich damit die Folgen für die Betroffenen in überschaubaren Grenzen halten.

Offener E-Mail-Verteiler
Der offene E-Mail-Verteiler stellt nach wie vor den Klassiker der Datenschutzverletzung dar. Auch wenn hierbei in der Regel das Risiko für die Betroffenen als durchaus gering eingeschätzt werden kann, ist eine solche Datenschutzverletzung nach Art. 33 DSGVO meldepflichtig, da die Datenschutz-Grundverordnung ein gegebenenfalls nicht meldepflichtiges geringes Risiko eben nicht kennt. Die Meldung nach Art. 33 DSGVO ist lediglich dann entbehrlich, wenn mit der Datenschutzverletzung voraussichtlich kein Risiko für die Rechte und Freiheiten natürlicher Personen verbunden wäre, was jedoch bereits dann nicht ausgeschlossen werden kann, wenn sich die E-Mail-Adresse vor der Domainangabe aus Vorname und Nachname zusammensetzt und für deren Übermittlung in Abhängigkeit des Adressatenkreises regelmäßig gerade keine Rechtsgrundlage gegeben ist.

Verlust auf dem Postweg
Eine meldeerhebliche Fallgruppe, die in besonderem Maße in diesem Berichtsjahr aufgetreten ist, stellt der Verlust von Unterlagen auf dem Postweg dar. Besonders kritisch festzuhalten ist der Umstand, dass diese Fallgruppe vornehmlich im Bereich des Bankenwesens in Erscheinung getreten ist, was für die betroffenen Personen mit besonderen Folgen verbunden sein kann. Hier ist bei Bekanntwerden einer solchen Problematik, eine kritische Bewertung des Versanddienstleisters geboten.

Einbruch und Diebstahl
Eine weitere häufige Fallgruppe der Meldungen von Datenschutzverletzungen stellen Einbrüche und Diebstähle dar. Besonders problematisch ist diese Fallgruppe, da sie in den Bereich der kriminellen Handlungen fällt und damit das verbundene Risiko für die betroffenen Personen besonders hoch ist. Im Rahmen dieser Fallgruppe sind als technisch-organisatorische Maßnahmen geboten, sämtliche Datenträger stets ordnungsgemäß zu verwahren und regelmäßige Backups durchzuführen, um die Verfügbarkeit der Daten durch die Möglichkeit einer Wieder-

herstellung zu gewährleisten. Darüber hinaus sind personenbezogene Daten auf digitalen Datenträgern durch geeignete Verschlüsselung zu schützen. Die Funktionalität der vollständigen Festplattenverschlüsselung ist heute bereits in vielen Betriebssystemen integriert, so dass in vielen Fällen gar keine zusätzliche Spezialsoftware erforderlich wäre.

Cyberkriminalität
Eine weitere Fallgruppe ist unter dem allgemeinen Begriff der Cyberkriminalität zusammengefasst. Unter diesen sehr unspezifischen Begriff fallen generell sämtliche Handlungen/Straftaten, die durch die Nutzung von Kommunikations- und Informationstechniken begangen werden. Typische Handlungsfelder sind die Verschlüsselung und das Abgreifen von personenbezogenen Daten aus E-Mail-Postfächern, von Servern oder anderweitigen Datenträgern. Insbesondere im Bereich der Cyberkriminalität ist hinsichtlich der erforderlichen technisch-organisatorischen Maßnahmen besonderer Wert auf die Informations-/Datensicherheit zu legen sowie die involvierten Personen stets zu sensibilisieren.

Zur Vermeidung von Meldefällen ist es geboten, sich stets mit möglichen technisch-organisatorischen Maßnahmen zum Schutz personenbezogener Daten auseinanderzusetzen, die erforderlichen Maßnahmen entsprechend umzusetzen sowie auf aktuellem Stand zu halten. Soweit die Meldefälle auf menschliches Versagen zurückzuführen sind, ist es stets erforderlich, die involvierten Personen bezüglich entsprechender Fehlerquellen zu sensibilisieren sowie – soweit möglich – technische und organisatorische Vorkehrungen zur Vermeidung zu implementieren.

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

Im Zusammenhang mit Meldungen von Datenschutzverletzungen war ich im Berichtsjahr unter anderem wie folgt prüfend und beratend tätig:

4.6.2 Cyberangriff auf Hochleistungsrechenzentrum

Der Betreiber eines Hochleistungsrechenzentrums meldete im Berichtszeitraum, die Kompromittierung mehrerer Systeme. Unter Ausnutzung einer bis dahin unbekannten Schwachstelle sowie mittels Verwendung gestohlener SSH-Schlüssel und Zugangsdaten erfolgte die gezielte Installation eines Backdoors durch einen Angreifer. Zudem wurde eine wurmartige Ausbreitung des Angriffs zwischen mehreren Hochleistungsrechenzentren in Europa festgestellt.

Über die Existenz und potenziellen Ausnutzung der Schwachstelle wurde der Verantwortliche vom Hersteller des Softwaresystems informiert. Im Rahmen einer diesbezüglichen forensischen Analyse wurde die Kompromittierung festgestellt. Der Verantwortliche reagierte mit Maßnahmen zur Beseitigung der Schwachstelle. Im Rahmen eines umfassenden IT-Sicherheitsmanagementprozesses wurden die betroffenen Systeme analysiert und meine Behörde informiert.

In einem Vor-Ort-Termin wurde der Vorfall ausführlich bewertet. Hierbei wurden insbesondere der ermittelte Infektionsverlauf sowie Maßnahmen zur Wiederinbetriebnahme und Prävention diskutiert.

Angriffsziel waren nicht vordergründig personenbezogene Daten. Auf einem System wurde ein sogenannter Crypto-Miner entdeckt. Kryptowährungen erfahren eine zunehmende Beliebtheit und dienen seit einiger Zeit auch als Spekulationsobjekte. Hinsichtlich spektakulärer Wertsteigerungen und Anonymität beim Erzeugen sowie Einsatz blockchainbasierter Währungen besteht ein hoher Anreiz für Cyberkriminelle.

Digitale Währungen werden durch rechenintensive kryptographische Berechnungen erzeugt. Durch den Einsatz sehr großer Rechenleistungen ist es möglich digitale Werte zu generieren. Cyber-Kriminelle zielen darauf ab, durch das Einschleusen der Crypto-Miner in leistungsstarke Rechenzentren, digitale Werte zu generieren. Die Kosten der Erzeugung resultierend aus den Energiekosten, den Hard- und Softwareeinsatz sowie der qualitativen Beeinträchtigung der IT-Services trägt der Betreiber des kompromittierten Rechenzentrums.

4.6.3 Schwachstelle in Hochschulinformationssystem

Mehrere Hochschulen meldeten eine Softwareschwachstelle im betriebenen Hochschulinformationssystem. Die Meldungen ließen keinen eindeutigen Schluss auf die Wirkungsweise der Schwachstelle und die Risikobewertung zu.

Im Rahmen eines Vor-Ort-Termins bei einer der Verantwortlichen wurde die grundlegende Architektur und Infrastruktur des Hochschulinformationssystem dargelegt. Hieraus konnten Rückschlüsse auf die Auswirkung und die Risiken der Schwachstelle gezogen werden.

Grundsätzlich wurde festgestellt, dass die Schwachstelle vom Hersteller im Rahmen der eigenen Qualitätskontrolle aufgedeckt wurde. Die betroffenen Kunden wurden vom Hersteller informiert und ein entsprechendes Sicherheitspatch zur Fehlerbehebung zur Verfügung gestellt. Eine tatsächliche Ausnutzung der Schwachstelle ist bei keinem der Verantwortlichen bekannt geworden.

Eine Informationspflicht nach Art. 34 Datenschutz-Grundverordnung wurde nicht festgestellt. Den Verantwortlichen wurde dennoch empfohlen, die Betroffenen über die Entdeckung der Schwachstelle und deren Behebung in einem allgemeinen Rahmen zu informieren – im Sinne einer transparenten Informationspolitik.

Das zuständige Staatsministerium wurde aufgefordert, für alle Einrichtungen im Geschäftsbereich, die das betroffene Hochschulinformationssystem einsetzen, zu prüfen und sicherzustellen, dass die Schwachstelle bei allen Verantwortlichen durch Installation des bereitgestellten Sicherheitspatches geschlossen wird. Ein entsprechender Vollzug wurde mir gemeldet.

4.6.4 Offener Webserver

Ein Medienunternehmen meldete mir eine Datenschutzverletzung, wonach die Syntax eines Freigabelinks nachvollzogen werden konnte und durch Änderung des Freigabelinks der Zugang zu Daten Dritter auf dem Webserver des Verantwortlichen möglich war.

Bei einem Vor-Ort-Termin konnte die gesamte Problemstellung erörtert werden. Es stellte sich heraus, dass es sich bei den auf dem Webserver gespeicherten Daten um keine unverarbeiteten Rohdaten mehr handelte, sondern um endbearbeitete Daten, die von den Betroffenen zur Veröffentlichung freigegeben werden sollten. Somit war das mit der Datenschutzverletzung verbundene Risiko nicht mehr als hoch, sondern vielmehr sogar als gering zu bewerten. Es wurde mit dem Verantwortlichen erörtert, dass die verwendete Technik keine Benutzerauthentifikation enthielt und zudem die Syntax des Freigabelinks unproblematisch nachvollzogen werden konnte. Damit waren die technisch-organisatorischen Anforderungen nicht erfüllt. Der Verantwortliche teilte mit, dass er nach Kenntnis der Sicherheitslücke den Webdienst unverzüglich abgeschaltet hatte. Während des Vor-Ort-Termins besprachen wir die künftige datenschutzkonforme Umsetzung des Webdienstes. Die Lösung sah eine benutzerbezogene Freigabe vor. Außerdem war gewährleistet, dass die Syntax eines Freigabelinks nicht mehr nachvollzogen werden konnte.

4.7 Datenschutzbeauftragter

Vergleiche die Beiträge unter 1.2 und 2.1.2 sowie die statistischen Informationen unter 6.2.6.

4.8 Verhaltensregeln und Zertifizierung

4.8.1 Zum Stand von Akkreditierungen und Zertifizierungen

Die Datenschutz-Grundverordnung (DSGVO) hat mit den Art. 42 und 43 DSGVO die Grundlagen für eine einheitlich geregelte Zertifizierung von Produkten, Prozessen und Dienstleistun-

gen für die Verarbeitung von personenbezogenen Daten und damit der Vergabe von Datenschutzsiegeln und -prüfzeichen geschaffen. Hierdurch soll im besonderen Maße die Datenschutzkonformität von Verarbeitungen personenbezogener Daten gewährleistet werden. Für Betroffene wird durch die Verwendungen eines Datenschutzsiegels oder -prüfzeichens ein rascher Überblick über das Datenschutzniveau einschlägiger Produkte und Dienstleistungen ermöglicht sowie die Einhaltung des geltenden Datenschutzrechts sichtbar. Aber auch für Verantwortliche wird damit die Wahl von einzubindenden Dienstleistern als auch ihre eigene Rechenschaftspflicht hinsichtlich der Einhaltung des geltenden Datenschutzrechts erleichtert.

Zertifizierungen und damit die Vergabe von Datenschutzsiegeln und -prüfzeichen im Bereich der Datenschutz-Grundverordnung erfordern eine vorherige Akkreditierung der Zertifizierungsstellen. Dies erfolgt in Deutschland durch die hierfür zuständige Deutsche Akkreditierungsstelle GmbH (DAkkS) in Zusammenarbeit mit den deutschen Aufsichtsbehörden. Einen Überblick mit weitergehenden Hinweisen sowie eine umfassende Darstellung des gesamten Akkreditierungsprozesses findet man auf der Internetseite der DAkkS: dakks.de

Zu Beginn des Berichtsjahres wurde zwischen allen deutschen Aufsichtsbehörden eine Verwaltungsvereinbarung geschlossen, um die Zusammenarbeit im Rahmen des Akkreditierungsprozesses zu regeln. Dies umfasst unter anderem die Zusammensetzung von Gremien, die Möglichkeit der gegenseitigen Unterstützung sowie die deutschlandweite Geltung von Zertifizierungen, Datenschutzsiegeln und -prüfzeichen.

Des Weiteren wurden von den Aufsichtsbehörden im Arbeitskreis Zertifizierung die Akkreditierungsanforderungen als Ergänzungen zur DIN EN ISO/IEC 17065 erarbeitet und gemäß Art. 64 DSGVO zur Stellungnahme dem Europäischen Datenschutzausschuss vorgelegt. Das Stellungnahme-Verfahren konnte erfolgreich abgeschlossen werden, so dass für den Akkreditierungsvorgang nunmehr ergänzende Anforderungen vorliegen. Das PDF-Dokument kann auf datenschutzkonferenz-online.de heruntergeladen werden.

Seitens der deutschen Aufsichtsbehörden ist für 2021 geplant, ein Dokument als Hilfestellung für Zertifizierungsstellen und Programmeigner fertigzustellen, welches die Mindestanforderungen an Zertifizierungskriterien darlegt. Dieses Dokument wird zudem den deutschen Aufsichtsbehörden als Grundlage einer einheitlichen Bewertung und Genehmigung von Zertifizierungsprogramm dienen.

Aktuell liegen mehrere Zertifizierungsprogramme bei der DAkkS beziehungsweise den zuständigen Aufsichtsbehörden zur Programmprüfung und Genehmigung der Zertifizierungskriterien vor. Für meinen Zuständigkeitsbereich ist ein solches Verfahren bislang nicht eingeleitet. Bundesweit ist für 2021 davon auszugehen, dass die ersten Akkreditierungsverfahren abgeschlossen sein werden und akkreditierte Zertifizierungsstellen mit der Zertifizierung von Verantwortlichen und Auftragsverarbeitern beginnen werden.

5 Internationaler Datenverkehr

5.1 Konsequenzen aus der Entscheidung des Europäischen Gerichtshofs zum internationalen Datentransfer

Die Entscheidung des Europäischen Gerichtshofs vom 16. Juli 2020 – C-311/18 – („Schrems II“) hat für die Datenverarbeitungsprozesse insbesondere der Unternehmen, die bisher auf Grundlage des Privacy Shield personenbezogene Daten in die Vereinigten Staaten von Amerika übermittelt haben, entscheidende Auswirkungen. Diese Unternehmen sollten sich auf Standarddatenschutzklauseln einrichten und umstellen.

Aber auch die Verwendung der Standarddatenschutzklauseln sind nach der Entscheidung des Europäischen Gerichtshofs mit einer gewissen Rechtsunsicherheit belegt worden. So wird den Verantwortlichen und Auftragsverarbeitern abverlangt, zu prüfen, ob das Recht des Drittlandes, in das die Daten transferiert werden nach Europarecht „einen angemessenen Schutz der auf der Grundlage von Standarddatenschutzklauseln übermittelten personenbezogenen Daten gewährleistet“ (vgl. Rdnr. 134 der Entscheidung). Dennoch werden Verantwortliche aufgrund ihrer geschäftlichen Prozesse über keine Alternativen zu den Standarddatenschutzklauseln verfügen, da auch individuelle Verträge oder Einwilligungslösungen aus vielfachen praktischen Gründen ausscheiden dürften. Auch Verlagerungen der Datenverarbeitung aus den Vereinigten Staaten und Drittländern in den europäischen Wirtschaftsraum werden nicht ohne Weiteres und von heute auf morgen umsetzbar sein. Die gemäß Art. 49 Datenschutz-Grundverordnung (DSGVO) vorgesehenen Ausnahmebedingungen, unter denen personenbezogene Daten in Drittländer übermittelt werden, dürften in der Breite keine Lösung darstellen.

Den Verantwortlichen, die auf eine Verarbeitung in Drittländern nicht verzichten können, ist insoweit in jedem Fall anzuraten, ihre Datenverarbeitungsprozesse zu verfeinern und die vom Europäischen Gerichtshof vorgesehene Prüfung des Datenschutzniveaus im Drittland zu realisieren. Technisch-organisatorische Maßnahmen können gegebenenfalls parallel intensiviert werden, wie zum Beispiel eine Reduzierung des Datenumfangs, die Anwendung von Verschlüsselungstechnik. Die Vorgehensweise sollte in granularer Weise wie bei einem Datenschutz- und Informationssicherheitskonzept dokumentiert werden.

Die unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder arbeiten mit den anderen europäischen Datenschutzbehörden gemeinsam an möglichen Verfahrensverbesserungen und inhaltlichen Lösungen. Eine entsprechende Ad-hoc-Arbeitsgruppe wurde hierzu eingerichtet.

Nach der Entscheidung des Europäischen Gerichtshofs sind die Aufsichtsbehörden, so auch meine Behörde, allerdings auch im Beschwerdefall verpflichtet, bei Angemessenheitsentschei-

dungen die bestehenden Garantien für Datentransfer zu prüfen (vgl. Rdnr. 120 der Entscheidung). Erforderlichenfalls ist, soweit keine wirksame Angemessenheitsentscheidungen vorliegen und keine geeigneten Garantien eine Datenübermittlung gestatten, diese gemäß Art. 58 Abs. 2 Buchst. f DSGVO zu verbieten. Es kann auch, so das Gericht, eine Aussetzung gemäß Abs. 2 Buchst. j DSGVO zur Abhilfe erfolgen.

Vergleiche auch den Beitrag unter 9.3.

6 Sächsischer Datenschutzbeauftragter

6.1 Zuständigkeit und Anforderungen an Beschwerden

6.1.1 Zuständigkeit des Sächsischen Datenschutzbeauftragten nach der DSGVO

Mehr als zwei Jahre nach Einführung der Datenschutz-Grundverordnung (DSGVO) hat sich durch Bearbeitung unterschiedlichster Fallkonstellationen die Aufsichtspraxis zur Feststellung der federführenden Behörde im Sinne von Art. 56 Abs. 1 DSGVO bereits soweit gefestigt, um ein zumindest vorläufiges Resümee ziehen zu können.

Zur Feststellung der federführenden (inländischen) Aufsichtsbehörde, § 40 Abs. 2 Bundesdatenschutzgesetz, hatte ich bereits im Tätigkeitsbericht 2019 (6.1.2, Seite 111) Ausführungen gemacht. Art. 4 Nr. 16 Buchst. a DSGVO lässt sich die Vorstellung vom Ort der „Hauptverwaltung“ eines Verantwortlichen als maßgebliches Zuordnungskriterium entnehmen. Erwägungsgrund 36 der DSGVO stellt konkretisierend auf die „effektive und tatsächliche Ausübung von Managementtätigkeiten“ ab.

Die ergänzende Erläuterung im vorbezeichneten Erwägungsgrund legt nahe, das bislang in der Mehrzahl der Vorgänge zutreffende innerdeutsche Kriterium vom Register- beziehungsweise vorgeblichem Hauptsitz in besonderen Fällen zu hinterfragen. Wie so oft setzt ein vertieftes Nachdenken dann ein, wenn ein Einzelfall nach dem herkömmlichen Schema unlösbar wird. So hatte ich mich im Berichtszeitraum mehrfach mit einer Konzerntochter auseinanderzusetzen, die sich am ehemaligen Sitz ihrer (selbständigen) Vorgängerin als Kapitalgesellschaft niedergelassen hatte, dort aber tatsächlich kaum mehr als Traditionspflege betreibt, quasi ein goldenes Firmenschild auf Glanz hält, während die gesamte Datenverarbeitung am Sitz der Konzernmutter in einem anderen Bundesland stattfindet. Eine wirksame Kontrolle durch mich – gegebenenfalls mit Inaugenscheinnahme am Ort – im Sinne einer federführenden Aufsicht war in dieser Konstellation nicht mehr durchführbar gewesen.

Dass dabei, wie von dem Unternehmen dargetan, Daten aller Unternehmen und Konzernteile voneinander getrennt verarbeitet werden und die Entscheidung über Mittel und Zwecke der Verarbeitung jede Gesellschaft für sich trifft, besagt über die innere Struktur einer formell selbständigen Tochter allein noch zu wenig. Viel entscheidender ist der Ort, wo sich der tatsächliche Schwerpunkt der Geschäftstätigkeit und Verarbeitung befindet; oft genug liegt bei den Geschäftsführungen von Mutter- und Tochterunternehmen auch eine Personalunion vor. So war es auch in dem von mir zu entscheidenden Vorgang. Maßgeblich war demnach allein die tatsächliche Geschäftsanschrift, auch bei der Datenschutzerklärung und mit der für den Ort der Konzernanschrift zuständigen Datenschutzaufsichtsbehörde konnte insoweit Einigung in Bezug auf eine Übernahme der Vorgänge erzielt werden.

Bei dieser Art der Firmierung handelte es sich noch um einen Einzelfall und eine bisher seltene Ausnahme. Sie betraf allerdings ein großes Unternehmen und eine Vielzahl betroffener Personen. Insoweit ist zu verlangen, dass der Verantwortliche in den Datenschutzhinweisen bereits für Klarheit sorgt. Zu raten ist dabei auch, die zuständige Datenschutzaufsichtsbehörde in den zu machenden Informationen gemäß Art. 13 und 14 DSGVO zu benennen, um unnötigen Aufwand und Zeitverzug zu vermeiden.

Auch zu bereichsspezifischen Zuständigkeiten hatte ich mich schon geäußert (vgl. hierzu ebenso Tätigkeitsbericht 2019, 6.1.1., Seite 110 f.). Nach Maßgabe von Art. 85 DSGVO können die Mitgliedsstaaten eigenständige Regelungen für den journalistischen Bereich treffen. Davon hat der sächsische Gesetzgeber mit § 11a Satz 4 Sächsisches Gesetz über die Presse Gebrauch gemacht und die Kontrolle gemäß DSGVO bei der Datenverarbeitung für journalistische und literarische Zwecke nur sehr eingeschränkt beibehalten. Aufgrund dieses sogenannten Medienprivilegs und der fortgesetzten Rechtsprechung des Bundesverfassungsgerichts (vgl. unter anderem die Entscheidungen vom 6. November 2019, 1 BvR 16/13 und 1 BvR 276/17) sehe ich mich auch nicht als befugt an, redaktionelle Inhalte auf Bewertungsportalen und berichterstattenden Auftritten zu kontrollieren. Die Einstufung hat bei Bejahen journalistischer Zwecke auch unbeschadet von Qualität oder ihrer Stetigkeit zu erfolgen. Dies betrifft auch Löschungsbegehren zu gegebenenfalls veralteten Inhalten. Für bestimmte Sachverhalte beachtlich ist auch eine Entscheidung des Europäischen Gerichtshofs, die einen weiten Maßstab der Verarbeitung zu journalistischen Zwecken anlegt (Europäischer Gerichtshof vom 14. Februar 2019, C-345/17).

Betroffene können ihre Beschwerden zudem – soweit die Verantwortlichen sich einer Selbstkontrolle unterworfen haben – auch an den Trägerverein des Deutschen Presserats e. V., Fritschestraße 27/28, 10585 Berlin, richten.

Im Falle der Verarbeitung personenbezogener Daten liegt für Postunternehmen die Zuständigkeit aufgrund § 42 Abs. 3 Postgesetz und bei der geschäftsmäßigen Erbringung von Telekommunikationsdiensten aufgrund des § 115 Abs. 4 Telekommunikationsgesetz beim Bundesbeauftragten für den Datenschutz.

Im Hinblick auf die Datenschutzerklärung und der Nennung des Verantwortlichen bei Internetangeboten ist erneut anzumerken, dass die Anbieterhinweispflicht – „Impressumpflicht“ – davon zu unterscheiden ist. Für die ordnungsgemäße Angabe nach dem Telemediengesetz ist, auf Sachsen bezogen, die Landesdirektion Sachsen zuständig.

In Fällen, in denen die Verantwortlichen innerhalb des Geltungsbereichs der Datenschutz-Grundverordnung keinerlei Niederlassung unterhalten, verfüge ich, auch dem Marktortprinzip

folgend zumeist nicht über Möglichkeiten des Eingriffs. Eingaben können daher leider, abgesehen von Rat für die betroffenen Personen, den ich geben kann, aufsichtsrechtlich nicht zufriedenstellend erledigt werden.

Unternehmen, Vereine, Verbände, Einrichtungen aller Art, allgemein: sämtliche meiner Datenschutzaufsicht unterfallende Verantwortliche können sich im Rahmen meiner Beratungspflichten nach Art. 57 Abs. 1 Buchst. l DSGVO sowie § 40 Abs. 6 Satz 1 Bundesdatenschutzgesetz mit ihren Anliegen an mich wenden. Nach dem Wortlaut der bundesdatenschutzgesetzlichen Vorschrift gilt die Beratung nur für betriebliche Datenschutzbeauftragte. Allerdings bin ich selbstverständlich bemüht, auch Anfragen von Verantwortlichen zu beantworten, die keinen Datenschutzbeauftragten zu benennen hatten.

Beratungsanliegen können allerdings nur bearbeitet werden, wenn der Ratsuchende sich namentlich zu erkennen gibt. Die Beratung eines anonym bleibenden Verantwortlichen ist mir nicht möglich. Ich bitte daher auch von entsprechenden Anfragen, die häufig von Kanzleien und Datenschutzbeauftragten an mich erfolgen, abzusehen.

Auch berate ich nur die in Sachsen ansässigen Verantwortlichen. Übrige Anfragen, wie etwa die an sämtliche Aufsichtsbehörden, ohne dass der Verantwortliche im Freistaat sitzt, weise ich regelmäßig mit Hinweis auf die Zuständigkeit der jeweiligen Datenschutzaufsichtsbehörde ab.

Auf Vorgänge mit ausschließlichem Auslandsbezug beabsichtige ich in meinem nächsten Tätigkeitsbericht vertieft einzugehen. Zunächst nur dies: Betroffene können sich dazu an die für den Verantwortlichen zuständige Behörde (Auslandsbehörde) oder im Bundesland des Wohnsitzes des Betroffenen tätige Aufsichtsbehörde (Wohnsitzbehörde) wenden. Eine Übersicht der ausländischen Datenschutzaufsichtsbehörden ist im Übrigen über meine Internetpräsenz erreichbar. An den Bundesbeauftragten gerichtete Beschwerden mit ausschließlichem Auslandsbezug haben lediglich eine Überweisung an die für ihren Wohnsitz zuständige Datenschutzaufsichtsbehörde zur Folge.

6.1.2 Sachliche Unzuständigkeit bei einem Online-Lexikon

Mich erreichte eine Beschwerde wegen einer Eintragung auf der Website dewiki.de.

Bei dieser Website beziehungsweise den abrufbaren Inhalten handelt es sich – ähnlich wie bei Wikipedia – um eine frei zugängliche Enzyklopädie, die durch freiwillige und ehrenamtliche Autoren erstellt wird.

Der Petent rügte, dass ihn betreffende personenbezogene Daten unter dieser Website im Internet abrufbar wären und der Betreiber der Website keine Veranlassung zur Löschung sehe.

Ich musste dem Petenten mitteilen, dass ich sachlich nicht zuständig bin und personenbezogene Eintragungen auf dieser Website im Wesentlichen nicht dem Schutzbereich der Datenschutz-Grundverordnung (DSGVO) unterfallen. Ich konnte den Petenten daher nur auf die Möglichkeit der Inanspruchnahme zivilrechtlichen beziehungsweise gerichtlichen Rechtsschutzes hinweisen.

Dieser Mitteilung lag folgende rechtliche Einschätzung zugrunde: Der Schutz der Datenschutz-Grundverordnung zu Gunsten der einzelnen Betroffenen besteht in Fragen des informationellen Selbstbestimmungsrechts beziehungsweise Persönlichkeitsrechts nicht lückenlos. Die Datenschutz-Grundverordnung sieht Ausnahmen des sachlichen Anwendungsbereiches vor, wie zum Beispiel in Art. 2 Abs. 2 DSGVO. Insbesondere mit Art. 85 DSGVO hat der europäische Gesetzgeber eine Öffnungsklausel mit weitreichenden Spielräumen für nationale Regelungen zum Schutz der Meinungs- und Informationsfreiheit geschaffen. Zweck ist es, das der Datenschutz nicht zu Lasten der Meinungs- und Informationsfreiheit gehen darf, da beide grundrechtlich geschützte Belange sind.

Ausweislich des geänderten Wortlautes von Art. 85 Abs. 1 DSGVO im Vergleich zur Vorgängerregelung in Art. 9 der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr ist klargestellt, dass auch Datenverarbeitungen die nicht privilegierten Zwecken dienen, dennoch unter Art. 85 DSGVO fallen können.

Für die Verarbeitung, die zu journalistischen Zwecken oder zu wissenschaftlichen, künstlerischen oder literarischen Zwecken erfolgt, sehen die Mitgliedstaaten Abweichungen oder Ausnahmen von Kapitel II (Grundsätze), Kapitel III (Rechte der betroffenen Person), Kapitel IV (Verantwortlicher und Auftragsverarbeiter), Kapitel V (Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen), Kapitel VI (Unabhängige Aufsichtsbehörden), Kapitel VII (Zusammenarbeit und Kohärenz) und Kapitel IX (Vorschriften für besonderer Verarbeitungssituationen) vor, wenn dies erforderlich ist um das Recht auf Schutz der personenbezogenen Daten mit der Freiheit der Meinungsäußerung und der Informationsfreiheit in Einklang zu bringen (Art. 85 Abs. 2 DSGVO). Mit § 11a Sächsisches Gesetz über die Presse hat der Landesgesetzgeber eine entsprechende Regelung umgesetzt. Die Vorschrift gilt für „Unternehmen der Presse“. Allerdings lege ich den Anwendungsbereich aufgrund der Rechtsprechung des Europäischen Gerichtshofs weit aus (vgl. auch 6.1.1 zur Zuständigkeit des Sächsischen Datenschutzbeauftragten nach der Datenschutz-Grundverordnung).

In das zuvor beschriebene Privileg ist auch die literarische Zweckbestimmung aufgenommen worden. Danach sind Daten, die ausschließlich der Herstellung von belletristischer oder Sachliteratur dienen, aus dem Anwendungsbereich der Datenschutz-Grundverordnung ausgenommen. Der Begriff der „Literatur“ ist weit auszulegen und umfasst sowohl wissenschaftliche Literatur als auch Unterhaltungsliteratur. Unter der oben genannten Website wird ein Online-Lexikon beziehungsweise Enzyklopädie vorgehalten beziehungsweise veröffentlicht. Dieses

zählt als Nachschlagwerk zur Sachliteratur und ist vom Anwendungsbereich der Datenschutz-Grundverordnung weitgehend ausgenommen.

In dem vorliegenden Fall konnte daher dahingestellt bleiben, ob die weiteren Privilegierungen nach Art. 85 Abs. 2 DSGVO, wie zum Beispiel zu wissenschaftlichen oder journalistischen Zwecken, gleichfalls vorliegen und daher ebenso die sachliche Unzuständigkeit meiner Behörde begründen würden.

Vergleiche auch Tätigkeitsbericht 2019, 6.1.1, Seite 110 f. zu einem Vorgang mit journalistischem Hintergrund.

6.1.3 Änderung der aufsichtsbehördlichen Zuständigkeit für Bundesautobahnen und Bundesstraßen

Das Fernstraßen-Bundesamt (FBA) ist eine neue Bundesoberbehörde im Geschäftsbereich des Bundesministeriums für Verkehr und digitale Infrastruktur (BMVI) und wurde im Oktober 2018 errichtet. Diese unabhängige Aufsichts- und Genehmigungsbehörde für die Bundesautobahnen und sonstige Bundesfernstraßen hat am 1. Januar 2021 ihre Tätigkeit mit Hauptsitz in Leipzig vollständig aufgenommen. Bundesautobahnen werden nun nicht mehr in Auftragsverwaltung durch die Länder, sondern in Bundesverwaltung geführt. Das FBA soll im Wesentlichen hoheitliche Aufgaben übernehmen und insbesondere die zuständige Anhörungs- und Planfeststellungsbehörde in Planfeststellungsverfahren für Autobahn-Projekte in Bundesverwaltung sein.

Infolgedessen ändert sich die Zuständigkeit der Datenschutzaufsicht. Die aufsichtsbehördliche Zuständigkeit der Landesbehörden für Datenschutz (zum Beispiel des Sächsischen Datenschutzbeauftragten) für die Bundesautobahnen, welche im jeweiligen Bundesland (hier Sachsen) liegen, endete somit am 31. Dezember 2020, da nur bis zu diesem Zeitpunkt bezüglich der Bundesautobahnen die gegenwärtige Bundesauftragsverwaltung durch die Länder fortbestand.

Seit dem 1. Januar 2021 ist ausschließlich der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) datenschutzrechtliche Aufsichtsbehörde für Bundesautobahnen.

Abweichend davon ist der Sächsische Datenschutzbeauftragte zuständige datenschutzrechtliche Aufsichtsbehörde bezüglich der Bundesautobahnen, wenn für die Entscheidung gemäß § 74 Abs. 7 Verwaltungsverfahrensgesetz von der Ausnahmeregelung nach § 3 Abs. 3 Fernstraßen-Bundesamt-Errichtungsgesetz Gebrauch gemacht wird und somit das Land zuständige Behörde, Anhörungs- und Planfeststellungsbehörde in Planfeststellungsverfahren, Plangenehmigungsbehörde in Plangenehmigungsverfahren ist.

Für die Bundesstraßen bleibt es weiterhin bei der Auftragsverwaltung durch die jeweiligen Länder. Daher behält der Sächsische Datenschutzbeauftragte weiterhin bezüglich der Bundesstraßen seine aufsichtsbehördliche Zuständigkeit für diejenigen Bundesstraßen, die in Sachsen liegen – auch nach dem 1. Januar 2021.

6.1.4 Inkassobereich: Mindestanforderungen an Beschwerden

Im Inkassobereich erreichen mich fortlaufend Beschwerden, denen oftmals ein konkreter, mitunter jeglicher, Datenschutzbezug fehlt. Stattdessen weisen die Petenten regelmäßig pauschal darauf hin, dass der einer geltend gemachten Forderung zugrundeliegende Vertrag nicht bestehe, gekündigt oder widerrufen sei.

In diesen Fällen erfolgt regelmäßig die Information der Beschwerdeführer, dass das Datenschutzrecht kein übergeordnetes Verbraucherschutzrecht ist, sondern ausdrücklich das legitime Interesse zur Durchsetzung von Forderungen privilegiert behandelt – auch und gerade in Zweifelsfällen (Art. 18 Abs. 2 Datenschutz-Grundverordnung).

Selbstverständlich erfolgt eine eingehende Prüfung substantiiert vorgetragener Beschwerden auf die mögliche Verletzung datenschutzrechtlicher Pflichten durch die Verantwortlichen. Diese Pflichten umfassen auch eine zumindest kursorische Prüfung auf Plausibilität und tatsächliches Bestehen der Forderung. Bei zuvor aufgetretenen Problemen kann die Prüfpflicht des Inkassounternehmens gesteigert sein (vgl. Tätigkeitsbericht 2019, 2.2.18., Seite 54 ff.).

Soweit die Verletzung inkassorechtlicher Pflichten vorgetragen wird oder sich aufdrängt, wird der Betroffene auf die Zuständigkeit des Amtsgerichts Chemnitz als Inkassoaufsicht hingewiesen; ähnliches gilt für Vorwürfe oder Anzeichen von strafbaren Handlungen außerhalb des Datenschutzrechts.

6.2 Zahlen und Daten zu den Tätigkeiten 2020

6.2.1 Überblick zu den Arbeitsschwerpunkten

Bei Beschwerdeeingaben und Beratungsanfragen verzeichnete meine Dienststelle 2020 die meisten Vorgänge – zusammen rund 43 Prozent. In der Statistik spiegelt sich auch die inhaltliche und organisatorische Arbeit als Vorsitzender bei der Datenschutzkonferenz (DSK) wieder. Fast ein Fünftel der Vorgänge entfiel darauf.

Auffällig gegenüber dem Vorjahr: Es gingen mehr Meldungen von Datenschutzverletzungen nach Art. 33 der Datenschutz-Grundverordnung ein (siehe 4.6.1). Außerdem gab es Zuwächse bei den internationalen Angelegenheiten. Sie betrafen hauptsächlich den EU-Bereich.

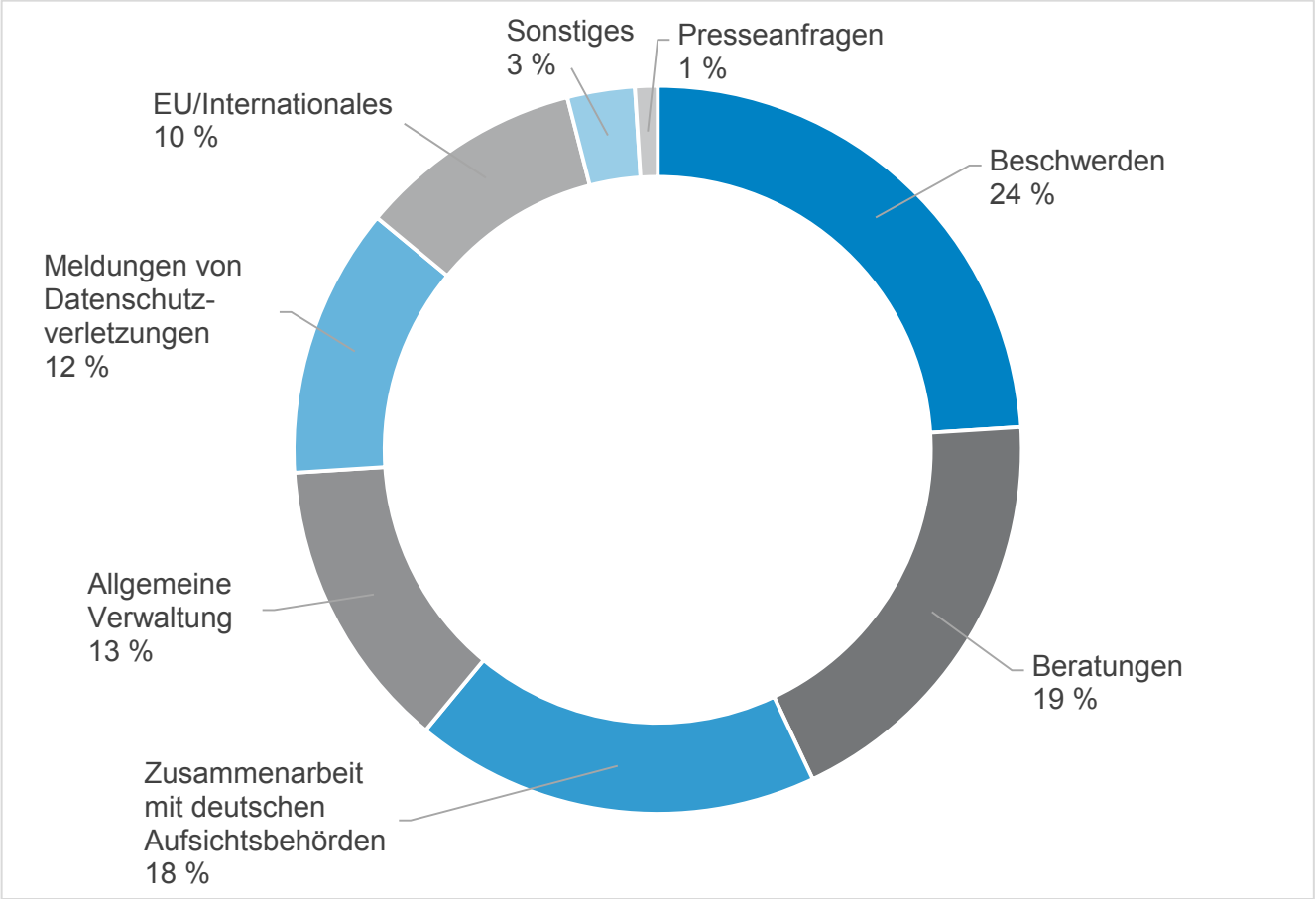


Abbildung 7: Arbeitsschwerpunkte nach Anzahl der Vorgänge

6.2.2 Beschwerden und Hinweise

Das Beschwerdeaufkommen lag im Berichtszeitraum weiterhin auf hohem Niveau. Seit Wirksamwerden der Datenschutz-Grundverordnung im Jahr 2018 haben sich die jährlich eingehenden Beschwerden und Hinweise mehr als verdoppelt. Sanken 2020 die Eingaben im nichtöffentlichen Bereich, legten sie im öffentlichen Sektor gegenüber 2019 deutlich zu (Abbildung 8).

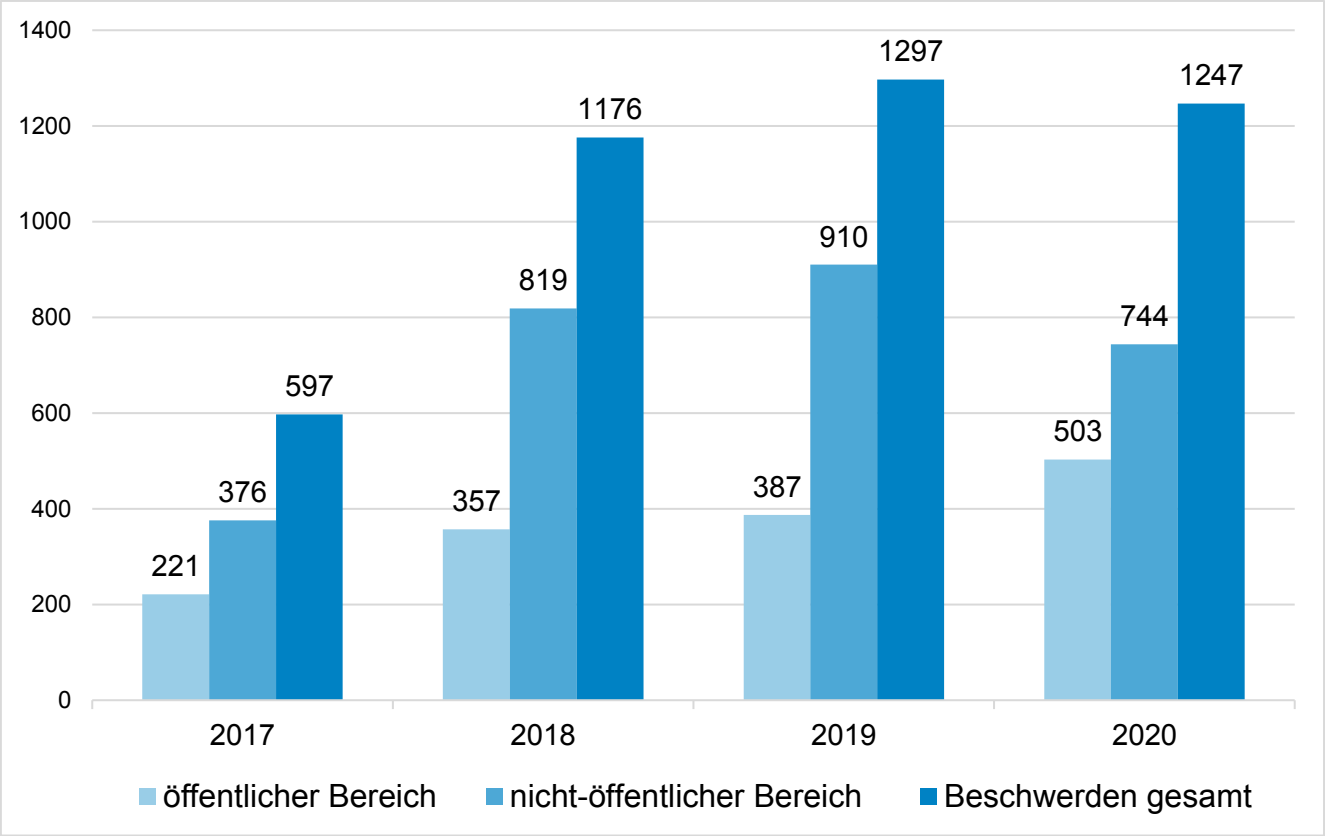


Abbildung 8: Beschwerden und Hinweise

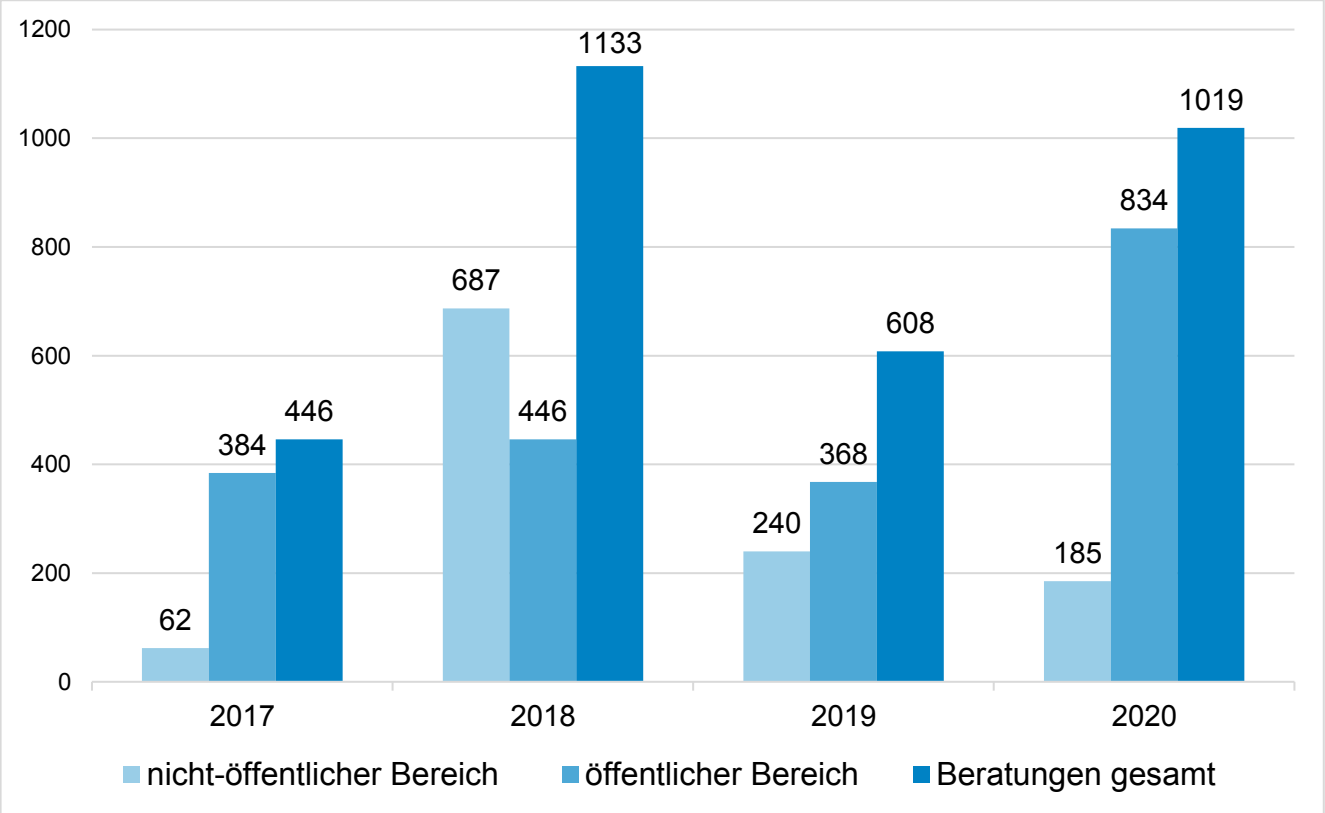


Abbildung 9: Beratungen

6.2.3 Beratungen

Gegenüber dem Vorjahr stiegen die Beratungen um 68 Prozent. Das starke Wachstum geht ausschließlich auf Auskünfte gegenüber dem öffentlichen Bereich zurück (Abbildung 9). Diese standen häufig im Zusammenhang mit der Coronavirus-Pandemie. Einige Anfragen sind exemplarisch in diesem Tätigkeitsbericht aufgeführt (vgl. unter anderem 2.2.1 bis 2.2.7).

6.2.4 Datenschutzverletzungen

Die Einmeldung von Datenschutzverletzungen gemäß Art. 33 DSGVO hat sich in den Jahren seit Wirksamwerden der Datenschutz-Grundverordnung stetig erhöht. Neben der Registratur der Vorgänge sind die Meldungen auszuwerten und gegebenenfalls für eine aufsichtliche Nacharbeit zu kategorisieren. Einen Überblick zu den inhaltlichen Vorgängen liefert der Beitrag 4.6.1.

6.2.5 Europäische Verfahren

Regelmäßig stimmen sich die europäischen Datenschutzaufsichtsbehörden bei grenzüberschreitenden Fällen ab. Dabei kommt das elektronische Binnenmarkt-Informationssystem (IMI) zum Einsatz. Im Berichtszeitraum waren dort 2.364 Vorgänge eingestellt. Alle Fälle werden von meiner Dienststelle gesichtet. Zunächst gilt es zu klären, ob wir für den jeweiligen Vorgang „federführend“ oder eine betroffene Aufsichtsbehörde sind. Es ist grundsätzlich die Aufsichtsbehörde zuständig, in dem sich die Hauptniederlassung oder die einzige Niederlassung des betroffenen Unternehmens in der EU befindet. Bei der Entscheidungsfindung im jeweiligen Fall werden auch andere Aufsichtsbehörden eingebunden, sofern sie betroffen sind. Das ist beispielsweise der Fall, wenn das Unternehmen auch eine Niederlassung in einem anderen Land hat oder bereits entsprechende Beschwerden bei der jeweiligen Aufsichtsbehörde eingegangen sind. Nach Abschluss der Ermittlungen legt die federführende Aufsichtsbehörde den betroffenen Aufsichtsbehörden einen Beschlussentwurf zur Stellungnahme vor. Im Jahr 2020 war meine Dienststelle in einem Fall federführend.

6.2.6 Register der benannten Datenschutzbeauftragten

Im Berichtszeitraum 2020 gingen 1.281 Meldungen zu benannten Datenschutzbeauftragten in meiner Dienststelle ein (Abbildung 10). 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; nicht öffentliche Stellen unter bestimmten Bedingungen) die Pflicht vor, einen Datenschutzbeauftragten zu benennen. Nach Art. 37 Abs. 7 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.

Erfreulich: Immer mehr Verantwortliche nutzen für die DSB-Meldungen inzwischen den Online-Formular-Service auf meiner Website. Der Anteil, der per Webformular eingegangen Meldungen, stieg im Vergleich zum Vorjahr um 14 Prozent. Diese Art der Übermittlung beschleunigt die Abarbeitung der DSB-Meldungen in meiner Behörde. Zudem bekommt die meldepflichtige Stelle nach Absenden des Webformulars sofort eine Kopie als PDF-Dokument per E-Mail zugeschickt. Bei Meldungen, die per E-Mail, Fax oder Post in der Dienststelle eingehen, werden – um Verwaltungsaufwand zu reduzieren – keine Eingangsbestätigungen verschickt.

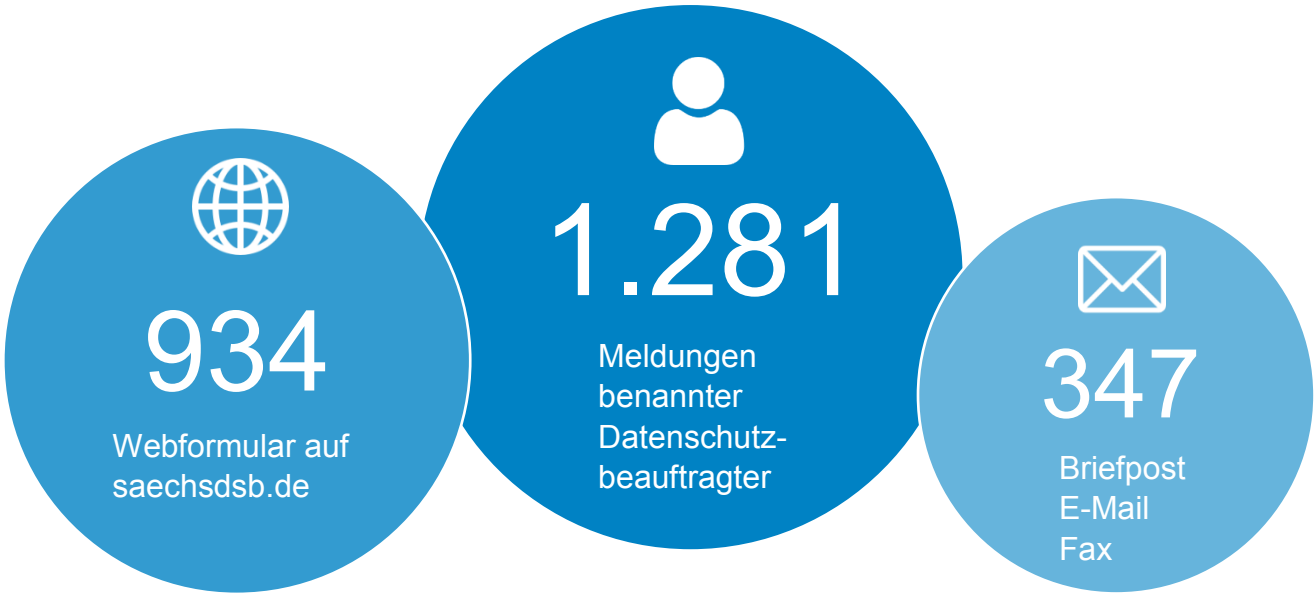


Abbildung 10: Meldungen benannter Datenschutzbeauftragter

6.3 Ressourcen

Das Arbeitsaufkommen in meiner Dienststelle hat sich durch die Datenschutz-Grundverordnung (DSGVO) drastisch erhöht. Im Berichtszeitraum verzeichnete meine Dienststelle abermals einen Rekord. Registriert wurden 17.152 Posteingänge, rund 23 Prozent mehr als 2019 (Abbildung 11).

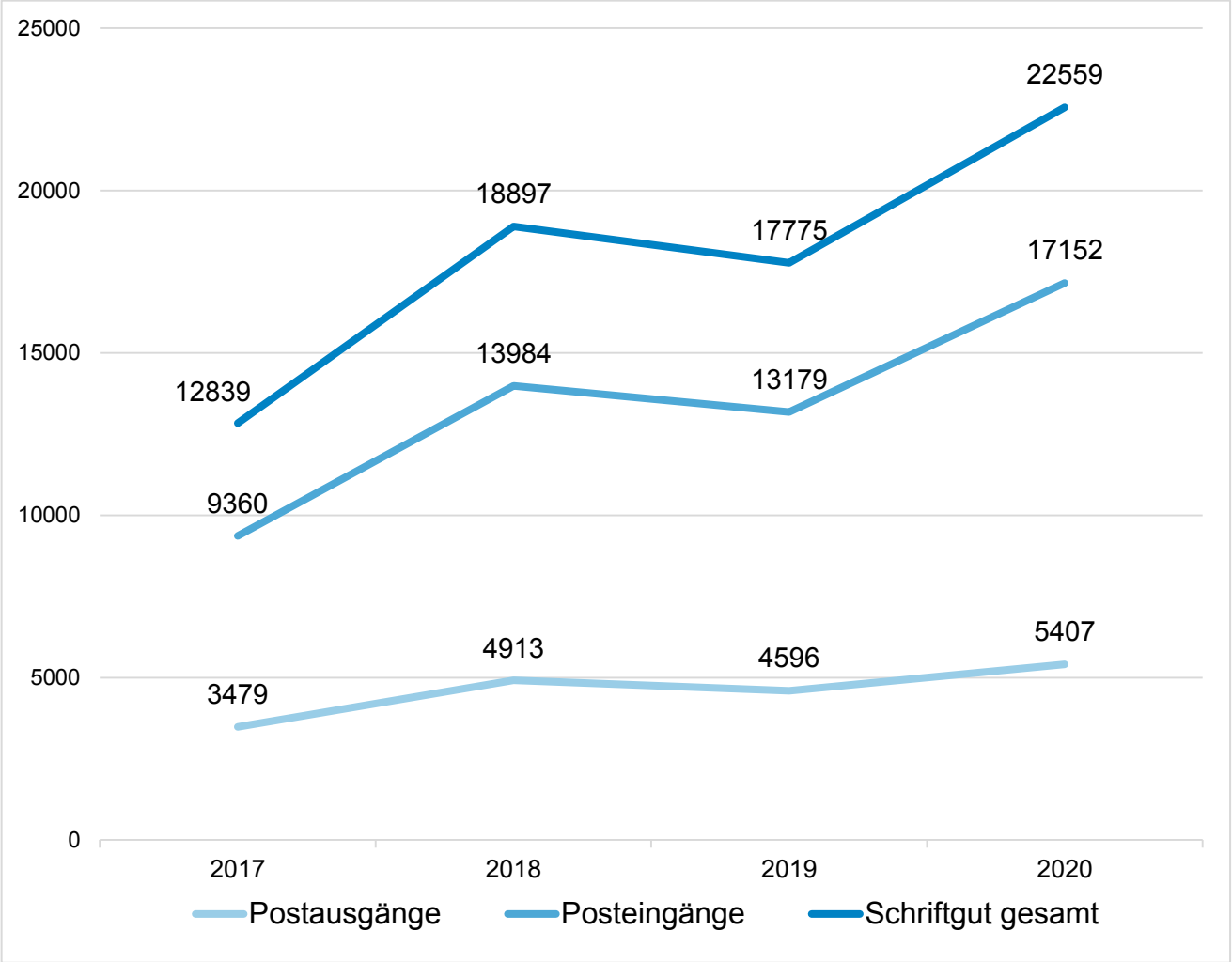


Abbildung 11: Schriftgutaufkommen

Im 18. Tätigkeitsbericht des Sächsischen Datenschutzbeauftragten für den öffentlichen Bereich (2017), also noch vor Wirksamwerden der DSGVO, schrieb ich:

„Die Neuregelungen werden erhebliche Auswirkungen auf meine Organisationsstruktur, meine Befugnisse und Aufgaben haben. Letztere werden sich enorm ausweiten; je nach Zählart kommt man auf 50 bis 60 neue Aufgaben für meine Behörde. Hieraus resultiert ein erheblicher Personalmehrbedarf. Meine Behörde verfügt derzeit, Anfang 2017, über fast die gleiche Anzahl von Stellen (21) wie zur Anfangszeit ihres Bestehens (1993 19 Stellen), obwohl sich die Aufgaben seither [….] enorm ausgeweitet haben. Gleiches gilt – als Zeichen eines gestiegenen Datenschutzbewusstseins zu begrüßen – für die stark gewachsene Anzahl der Bürgeranfragen. Ich bin aber deshalb derzeit nicht in der Lage, meine gesetzlichen Aufgaben vollumfänglich und mit der eigentlich notwendigen Breite und Tiefe zu erfüllen. Dies ist ein konkreter Nachteil für die sächsischen Bürger und Unternehmen.“

Auch 2020 konnte ich den gesetzlichen Aufgaben immer noch nicht vollumfänglich nachkommen. Es bestand weiterhin eine Schieflage zwischen personeller Ausstattung und dem Arbeitsaufkommen. Ein Blick auf die Zahlen verdeutlicht das.

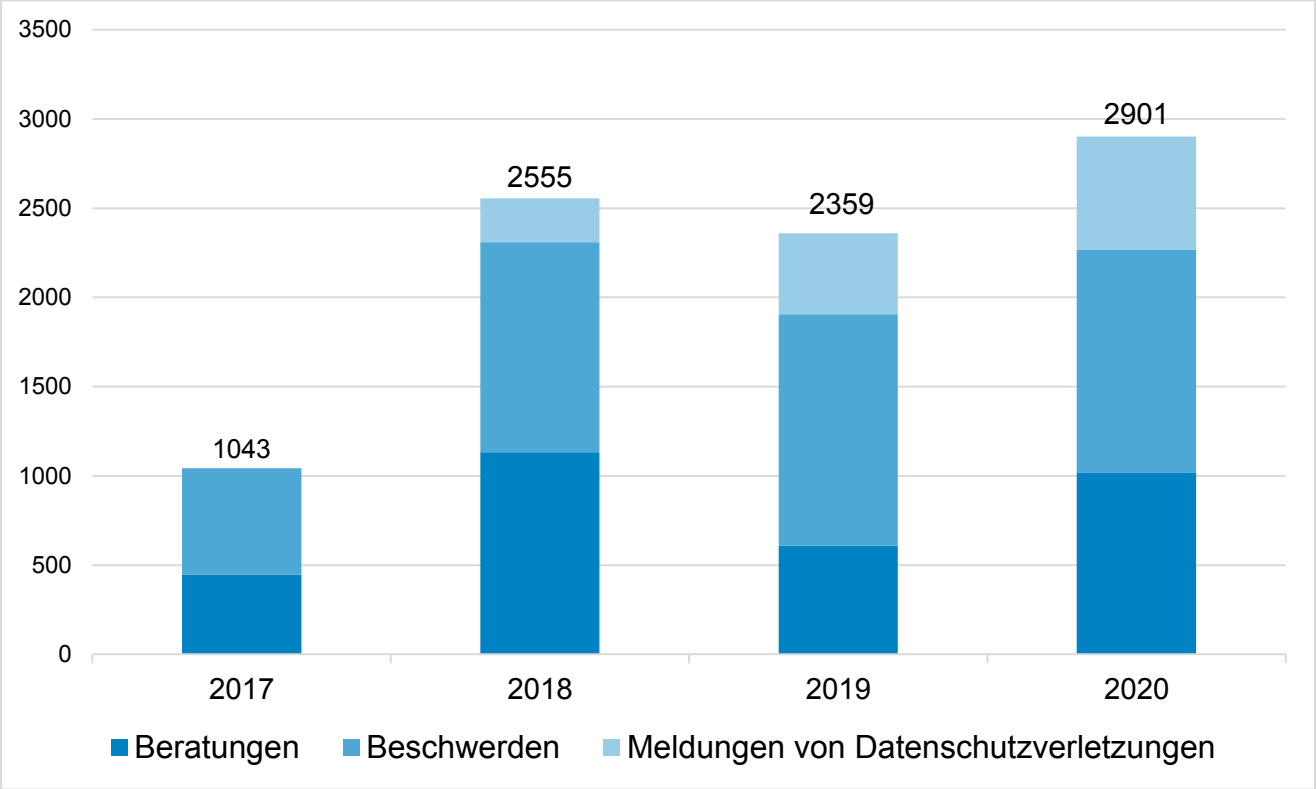


Abbildung 12: Zuwächse in wichtigen Tätigkeitsbereichen

Die Personalentwicklung der letzten Jahre, jeweils zum 31. Dezember:

2017: 22 Planstellen
2018: 24 Planstellen
2019: 28 Planstellen
2020: 31 Planstellen

Von 2017 bis Ende 2020 erhielt meine Dienststelle neun zusätzliche Stellen und verfügte somit zum 31. Dezember 2020 über insgesamt 31 Stellen. Dem gegenüber verdreifachten sich die jährlich neu eingehenden Vorgänge in wichtigen Tätigkeitsbereichen (Abbildung 12). Diesem Umfang war 2020 nicht vollends beizukommen – zumal der übernommene „Schuldenberg“ mit Fällen aus 2019 noch abzuarbeiten war. Nicht zu vergessen: Neue Mitarbeiter, die auch im Rahmen der normalen Personalfluktuation in meine Dienststelle wechselten, benötigen die übliche Einarbeitungszeit, was die Abarbeitung der Vorgänge anfänglich verzögert.

Die Folgen der zu knapp bemessenen personellen Unterstützung: Bearbeitungszeiten von einem Jahr waren weiterhin keine Seltenheit, anlasslose Kontrollen wurden bis auf zwei gezwungenermaßen ausgesetzt, Referententätigkeiten bei verschiedenen Fach- und Fortbildungsveranstaltungen konnten nur in geringem Umfang wahrgenommen werden (siehe 6.5.1).

Im Zuge der Coronavirus-Pandemie hat die Digitalisierung einen kräftigen Schub erfahren. Sie schreitet rasant voran und damit auch die elektronische Verarbeitung personenbezogener Daten. Zugleich hat die DSGVO Menschen für Datenschutz sensibilisiert. Es ist daher davon auszugehen, dass die eingereichten Beschwerden und Meldungen von Datenschutzverletzungen weiter zunehmen; der personelle Engpass wird sich also nicht durch einen Wegfall an Vorgängen lösen lassen.

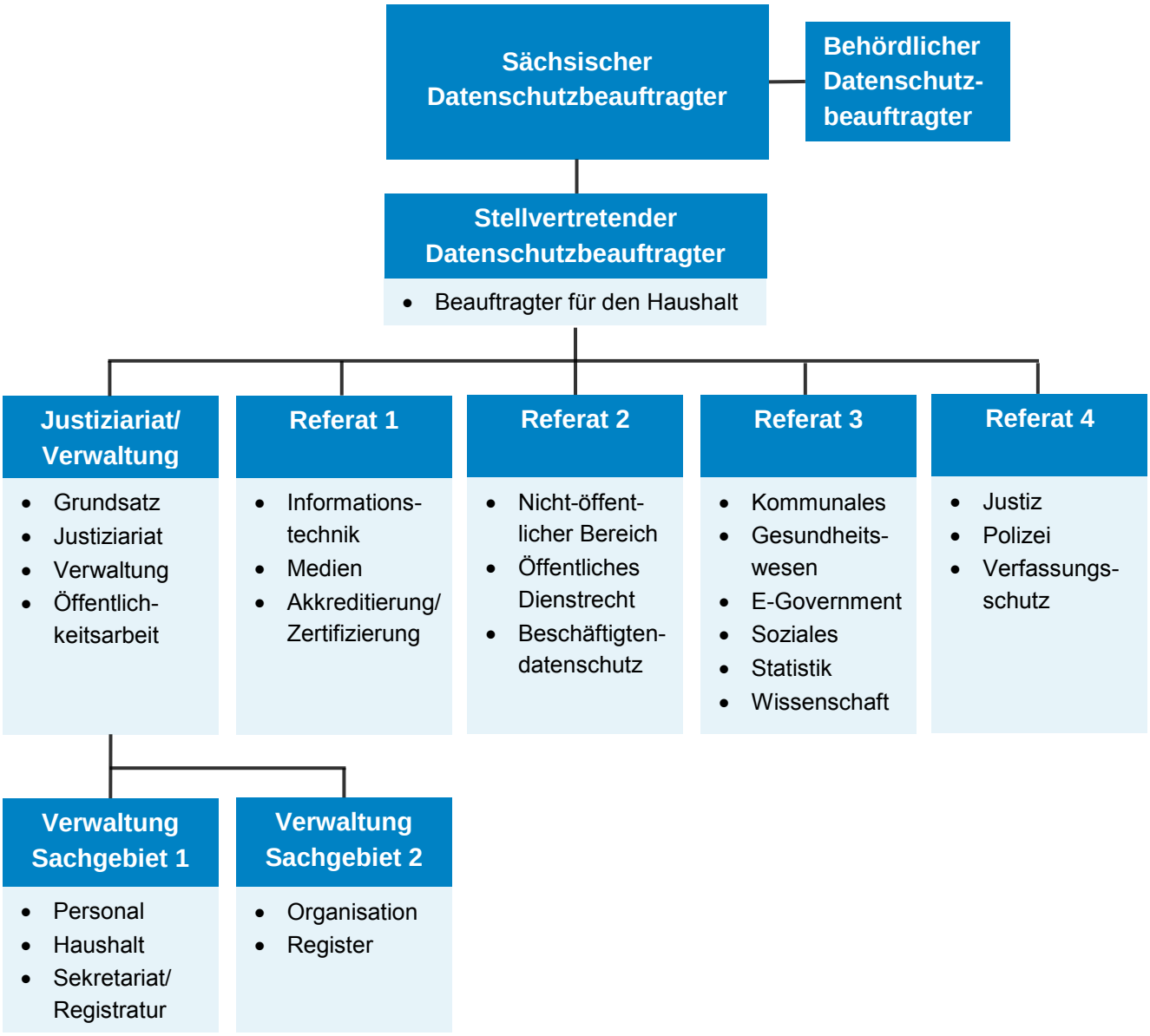


Abbildung 13: Vereinfachtes Organigramm der Behörde

6.4 Geldbußen und Sanktionen, Strafanträge

6.4.1 Ordnungswidrigkeitenverfahren im öffentlichen Bereich

Der 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)
- § 85a Zehntes Buch Sozialgesetzbuch – Sozialverwaltungsverfahren und Sozialdatenschutz – in Verbindung mit § 41 Bundesdatenschutzgesetz, Art. 83 Abs. 5 DSGVO (Art. 58 Abs. 2 Buchst. i DSGVO, § 14 Abs. 1 SächsDSDG)

Im Berichtszeitraum waren im öffentlichen Bereich insgesamt 74 Bußgeldverfahren anhängig. Davon wurden 4 mit einem rechtskräftigen Bußgeld abgeschlossen. In 15 Verfahren erfolgte eine Einstellung beziehungsweise wurde von der Verfolgung abgesehen. 55 Verfahren befanden sich zum Ende des Berichtszeitraumes noch in Bearbeitung.

Berichtszeitraum		**01.01. – 31.12.2020**
anhängig gesamt		**74**
davon	Verfahren aus vorherigem Berichtszeitraum	53
	neu eingegangene Verfahren	21
abgeschlossen		**19**
davon	mit Bußgeld	4
	mit Verwarnungsgeld	0
	eingestellt/von Verfolgung abgesehen	15
noch in Bearbeitung		**55**
Summe rechtskräftige Bußgelder/ Verwarnungs-gelder in Euro		**4.040**

Die Summe der rechtskräftigen Buß- und Verwarngelder belief sich auf 4.040 Euro.

Gegenüber dem vergangenen Berichtszeitraum ist die Anzahl der neu eingegangenen Ordnungswidrigkeitenverfahren leicht zurückgegangen. Sowohl der im Berichtszeitraum andauernde personelle Engpass als auch die wegen der Coronavirus-Pandemie vorübergehend eingeschränkte Funktionsfähigkeit der Behörde sowie der stetig steigende Bearbeitungsaufwand im Bereich der Ordnungswidrigkeiten wirkten sich negativ auf die Dauer der Verfahren aus. Es konnten im Vergleich zum Berichtszeitraum 2019 etwa gleichbleibend viele Verfahren abgeschlossen werden. Im Vergleich zu vergangenen Berichtszeiträumen gelangten jedoch weniger Verfahren zum Abschluss, was wiederum erneut zu einer niedrigeren Summe der festgesetzten Geldbußen führte.

Grundsätzlich musste im Berichtszeitraum bei den Ordnungswidrigkeiten im öffentlichen Bereich unterschieden werden in:

- Vorgänge, die in den Anwendungsbereich der DSGVO fallen – Verstöße nach Art. 83 Abs. 4 bis 6 DSGVO – und
- Vorgänge, die nicht in den Anwendungsbereich der DSGVO fallen.

Vorgänge, die in den Anwendungsbereich der DSGVO fallen – Verstöße nach Artikel 83 Abs. 4 bis 6 DSGVO

Besondere Schwierigkeiten bestanden weiterhin bei der Bearbeitung von Vorgängen, denen teilweise Sachverhalte aus der Zeit vor der unmittelbaren Anwendbarkeit der DSGVO zugrunde lagen und für die jeweils zu klären war, welches Recht zur Anwendung kommt (vgl. Tätigkeitsbericht 2019, 6.4.2, Seite 128 ff.).

Nach einer vorgenommenen Abwägung, ob die bisher geltenden nationalen Ordnungswidrigkeiten-Normen oder die DSGVO anzuwenden waren, stellten in diesen Fällen regelmäßig die bisher geltenden nationalen Ordnungswidrigkeiten-Normen das jeweils mildere Gesetz dar. Dafür sprach insbesondere der geringere Bußgeldrahmen (§ 38 Abs. 2 SächsDSG alte Fassung mit bis zu 25.000 EUR, § 85 Abs. 3 SGB X alte Fassung mit bis zu 300.000 EUR) gegenüber der DSGVO mit Geldbußen bis zu 20.000.000 EUR.

Vorgänge, die nicht in den Anwendungsbereich der DSGVO fallen – Verstöße durch Bedienstete von Staatsanwaltschaften, Polizei- und Justizvollzugsdienst, Ordnungswidrigkeitenbehörden

Für die Verarbeitung personenbezogener Daten durch die für die Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Straftaten oder Ordnungswidrigkeiten sowie für die Strafvollstreckung zuständigen öffentliche Stellen des Freistaates Sachsen, soweit sie Daten

zum Zweck der Erfüllung dieser Aufgaben verarbeiten, gilt seit dem 1. Januar 2020 das Sächsische Gesetz zur Umsetzung der Richtlinie (EU) 2016/680 (Sächsisches Datenschutz-Umsetzungsgesetz – SächsDSUG).

Für die am häufigsten im öffentlichen Bereich vorkommende Ordnungswidrigkeit – die unbefugte Verarbeitung von personenbezogenen Daten beziehungsweise der unbefugte Abruf personenbezogener Daten aus den polizeilichen Auskunfts- beziehungsweise Informationssystemen durch Polizeivollzugsbedienstete – gelten somit seit 1. Januar 2020 die Bußgeldvorschriften des § 48 SächsDSUG.

Bei der Bearbeitung von Vorgängen, denen teilweise Sachverhalte aus der Zeit vor dem Inkrafttreten des SächsDSUG zugrunde lagen, war jeweils zu klären, welches Recht zur Anwendung kommt.

In Ordnungswidrigkeitenverfahren, bei denen der Tatzeitpunkt vor dem 1. Januar 2020 liegt, ist § 4 Abs. 3 Gesetz über Ordnungswidrigkeiten (OWiG) zu beachten. § 4 Abs. 3 OWiG bestimmt für den Fall, dass das Gesetz, das bei Beendigung der Tat gilt, vor der Entscheidung der Verwaltungsbehörde geändert wird, das mildeste Gesetz anzuwenden ist.

Somit war in diesen Fällen abzuwägen, ob das bisher geltende SächsDSG alte Fassung oder das SächsDSUG anzuwenden war.

Regelmäßig stellte dabei das zum Tatzeitpunkt gültige SächsDSG das mildere Gesetz dar. Dafür sprach insbesondere der geringere Bußgeldrahmen des SächsDSG alte Fassung (§ 38 Abs. 2 SächsDSG mit bis zu 25.000 EUR) gegenüber dem SächsDSUG (§ 48 Abs. 2 SächsDSUG mit bis zu 50.000 EUR).

Bezüglich der einschlägigen Rechtsnormen für die polizeiliche Datenverarbeitung sowie für die Aufgaben und Befugnisse des Polizeivollzugsdienstes wurde in diesen Fällen auf das zum Tatzeitpunkt gültige Sächsische Polizeigesetz (SächsPolG) abgestellt, welches zum 31. Dezember 2019 außer Kraft trat und dessen Bestimmungen sich nunmehr im Wesentlichen im Sächsischen Polizeivollzugsdienstgesetz (SächsPVDG) wiederfinden.

In einem Großteil, circa 76 Prozent, der Ordnungswidrigkeitenverfahren standen/stehen nach wie vor Bedienstete der sächsischen Polizei in Verdacht, unbefugt personenbezogene Daten verarbeitet und/oder aus den polizeilichen Auskunfts- beziehungsweise Informationssystemen abgerufen zu haben. Auch in diesem Berichtszeitraum handelte es sich dabei regelmäßig um privat motivierte Datenabrufe zu Freunden, Kollegen, Nachbarn oder anderen Bekannten, aber auch um Recherchen zur eigenen Person.

Der hohe Anteil von Ordnungswidrigkeitenverfahren gegen Polizeibedienstete resultiert dabei hauptsächlich aus dem überdurchschnittlichen Anzeigeverhalten der Polizeidienststellen, welche ein datenschutzrechtliches Fehlverhalten ihrer Bediensteten auch weiterhin konsequent verfolgen.

In den übrigen Ordnungswidrigkeitenverfahren, circa 24 Prozent, bestand/besteht gegenüber Bediensteten unterschiedlichster sächsischer (Sozial-)Behörden der Verdacht, nicht offenkundige personenbezogene Daten unbefugt verarbeitet zu haben.

Bei vier der im Berichtszeitraum mit einem Bußgeld abgeschlossenen Verfahren handelte es sich um unbefugte Abrufe nicht offenkundiger personenbezogener Daten aus den polizeilichen Datenbanken (§ 38 Abs. 1 Nr. 1 a SächsDSG alte Fassung), und/oder unbefugte Verarbeitungen nicht offenkundiger personenbezogener Daten (§ 38 Abs. 1 Nr. 1 a SächsDSG alte Fassung) durch Polizeivollzugsbedienstete. Bei einem Verfahren handelte es sich um ein Bußgeld gegen einen Bediensteten eines öffentlichen Sozialleistungsträgers wegen einer unbefugten Verarbeitung nicht allgemein zugänglicher Sozialdaten (§ 85 Abs. 2 Nr. 1 SGB X alte Fassung).

Bereits die anhaltend große Anzahl an Ordnungswidrigkeitenverfahren gegen sächsische Polizeibedienstete zeigt, dass nach wie vor Unklarheiten im Zusammenhang mit der Nutzung polizeilicher Datenbanken bestehen.

Noch immer werden privat motivierte Abrufe von personenbezogene Daten aus den polizeilichen Informationssystemen durch einzelne Beschuldigte mit der allgemeinen Funktion als Polizeibeamter und der Pflicht zur Gefahrenabwehr gerechtfertigt und/oder damit begründet, dass aufgrund der Stellung als Bediensteter der Polizei allgemein die Befugnis besteht, die zugänglichen Daten abzurufen.

Das Abrufen nicht offenkundiger personenbezogener Daten ist jedoch nur zulässig, wenn deren Kenntnis zur Aufgabenerfüllung der abrufenden Person erforderlich ist, das heißt nur dann, wenn die Erfüllung der gesetzlichen − also die sich aus einem dienstlichen Anlass ergebende − Aufgabe ohne die konkrete Datenerhebung nicht möglich ist. Selbst wenn die polizeilichen Auskunfts- beziehungsweise Informationssysteme zu den täglichen Arbeitsmitteln eines Polizeibeamten zählen und die darin gespeicherten Daten generell zugänglich sind, muss für jede Datenverarbeitung und für jeden Datenabruf eine dienstliche Notwendigkeit gegeben sein (Urteil Oberlandesgericht (OLG) Bayern vom 12. August 1998, Az.: 5St RR 122/98; OLG Bamberg, Beschluss vom 27. April 2010 − 2 Ss 531/10).

Auch wenn Polizeibeamte gemäß § 2 SächsPVDG generell die Aufgabe haben, vom Einzelnen und dem Gemeinwesen Gefahren abzuwehren, haben sie sich dabei grundsätzlich innerhalb ihrer konkreten Aufgabenzuweisung und Zuständigkeiten zu bewegen. So wie der gesamte

Polizeivollzugsdienst nur die personenbezogenen Daten verarbeiten darf, die zur Erfüllung seiner Aufgaben erforderlich sind (§ 53 SächsPVDG in Verbindung mit § 3 SächsDSUG), ist auch der einzelne Polizeibedienstete nur berechtigt, die zur Erfüllung seiner konkreten dienstlichen Aufgabe erforderlichen Daten zu verarbeiten.

Dies ergibt sich klar aus dem Sächsischen Polizeivollzugsdienstgesetz und dem für die sächsische polizeiliche Datenverarbeitung einschlägigen Sächsischen Datenschutz-Umsetzungsgesetz (§§ 53, 54 SächsPVDG, §§ 3, 4, 5, 9 SächsDSUG; vgl. auch Urteil Bayerisches Oberstes Landesgericht vom 12. August 1998, Az.: 5St RR 122/98).

Die Entscheidung des OLG Bamberg (Beschluss vom 28. August 2018, Aktenzeichen: 2 Ss OWi 949/18) stellt ebenfalls klar:

„Der Abruf nicht offenkundiger Daten in polizeilichen Recherchesystemen durch einen Polizeibeamten ist nur dann zulässig, wenn die Datenkenntnis aus seiner Sicht zur polizeilichen Aufgabenerfüllung notwendig ist. Fehlt ein dienstlicher Anlass oder handelt der Betroffene im privaten Interesse, erfolgt der Datenabruf unbefugt…“.

Auch wenn laut der vorgenannten Entscheidung des OLG Bamberg im Bereich der Gefahrenabwehr eine abstrakt bestehende Gefahr ausreichend sein kann, geht aus den weiteren Ausführungen hervor, dass für die Zulässigkeit eines Datenabrufes das Bestehen eines Anfangsverdachtes erforderlich ist, „mithin ein über bloße Vermutungen hinausreichender, auf bestimmte tatsächliche Anhaltspunkte gestützter konkreter Verdacht, dass eine Straftat begangen worden ist und der Verdächtige als Täter oder Teilnehmer an dieser Tat in Betracht kommt.“

Beweisanzeichen für eine rein privat motivierte Datenabfrage können sich zudem auch aus dem konkreten Vorgehen des Betroffenen im Nachgang zu den einzelnen Datenabrufen ergeben. Wenn ein Polizeivollzugsbeamter außerhalb seines örtlichen und sachlichen Zuständigkeitsbereichs handelt, so dürfte es demnach den dienstlichen Gepflogenheiten entsprechen, wenn er entweder selbst einen entsprechenden Vorgang anlegt und diesen zu gegebener Zeit an die dafür zuständige Stelle abgibt oder jedenfalls einen Aktenvermerk über Anlass, Gegenstand und Ergebnis der Ermittlungen fertigt und diesen an die örtlich und sachlich zuständige Polizeidienststelle zur Einleitung eines Vorganges weiterleitet (OLG Bamberg, Beschluss vom 28. August 2018, Aktenzeichen: 2 Ss OWi 949/18).

Ausschließlich die pure Eigenschaft Polizeibeamter zu sein, welcher selbstredend zur Abwehr von Gefahren und zur Verfolgung von Straftaten nach § 2 SächsPVDG verpflichtet ist, reicht demnach regelmäßig nicht aus, um einen dienstlichen Anlass und sämtliche technisch möglichen Datenabrufe zu rechtfertigen.

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

6.4.2 Ordnungswidrigkeitenverfahren im nicht-öffentlichen Bereich

Im Berichtszeitraum hatte ich 80 neue Ordnungswidrigkeitenanzeigen zu verzeichnen. Die Anzahl bewegte sich damit im Wesentlichen auf dem Niveau des Vorjahres. Mehr als ein Viertel der Anzeigen (25) bezogen sich auch dieses Mal auf – von der Polizei im Rahmen üblicher Verkehrskontrollen festgestellte – Dashcams. In weiteren 20 Fällen richteten sich die Anzeigen gegen den Betrieb sonstiger Videokameras. Damit liegt der Schwerpunkt, 56 Prozent, der bei mir eingehenden Ordnungswidrigkeitenanzeigen erneut klar bei der Videoüberwachung.

Insgesamt waren damit im Berichtszeitraum 180 Ordnungswidrigkeitenverfahren bei mir anhängig. Von diesen konnte ich 54 Fälle abschließen und habe dabei 29 Bußgelder festgesetzt.

Alle Bußgelder betrafen den rechtswidrigen Einsatz von Dashcams durch Privatpersonen. Die Bußgeldhöhe lag zwischen 100 und 1.000 Euro (insgesamt 11.870 Euro). Soweit es sich bei Dashcams nur um geringfügige Verstöße gehandelt hat beziehungsweise 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 erteilt, Art. 58 Abs. 1 Buchst. d DSGVO.

In einem Fall betraf die Bußgeldfestsetzung einen rumänischen Staatsbürger. Gemäß der Vorgaben des Aufenthaltsgesetzes (AufenthG) habe ich daher nach Abschluss des Verfahrens die zuständige Ausländerbehörde über die Festsetzung eines Bußgeldes unterrichtet. Dem lag die Vorschrift des § 87 Abs. 4 Satz 1 AufenthG zugrunde, wonach die für die Einleitung und Durchführung eines Bußgeldverfahrens zuständigen Stellen die zuständige Ausländerbehörde unverzüglich über die Erledigung des Bußgeldverfahrens zu unterrichten haben. Die Mitteilungspflicht gilt für alle nicht-deutschen Staatsangehörigen, wenn – was bei Datenschutzverstößen immer der Fall ist – die Ordnungswidrigkeit mit Geldbuße von mehr als 1.000 Euro bedroht ist (§ 87 Abs. 4 Satz 3 AufenthG). Insbesondere gilt sie auch für EU-Ausländer (vgl. § 11 Abs. 1 Satz 1 Freizügigkeitsgesetz/EU). Maßgeblich ist das in der Datenschutz-Grundverordnung festgelegte Höchstmaß für Geldbußen; auf die tatsächliche Bußgeldhöhe kommt es nicht an.

Den bereits im Tätigkeitsbericht 2019 (6.4.1, Seite 126 ff.) geschilderten Fall einer Hausdurchsuchung im Zusammenhang mit einem offensichtlich sehr extensiven Einsatz von Dashcams habe ich 2020 mit einem Bußgeldbescheid in Höhe von 1.000 Euro abschließen können. In Dashcam-Fällen stellt die den Verstoß feststellende Polizei regelmäßig schon die jeweilige

Speicherkarte als Beweismittel sicher, so dass der Nachweis einer Ordnungswidrigkeit zumeist problemlos möglich ist. Hier lag der Fall aber etwas anders, da der Betroffene zunächst nur mit zahlreichen Ordnungswidrigkeitenanzeigen betreffend vermeintliche Verkehrsverstöße Dritter auffällig geworden war. Diesen Ordnungswidrigkeitenanzeigen waren zumeist – nur sehr kurze – Videosequenzen beigefügt, aus denen nicht ohne Weiteres ein permanenter anlassfreier und damit rechtswidriger Dashcam-Betrieb mit anschließender längerfristiger Speicherung der Videoaufzeichnungen abzuleiten war, jedenfalls ein solcher aber nicht gerichtsfest hätte nachgewiesen werden können. Als letztes Mittel war damit nur eine – natürlich gerichtlich angeordnete – Hausdurchsuchung verblieben. Von Kollegen aus anderen Bundesländern ist mir bekannt, dass auch dort in vergleichbaren Fällen Gerichte entsprechende Durchsuchungsbeschlüsse erlassen und dies mit der hohen Bußgeldandrohung der Datenschutz-Grundverordnung einerseits und der erheblichen Bedeutung des Schutzes des Persönlichkeitsrechts der von der Videoaufzeichnung betroffenen Personen andererseits begründet haben. Dashcam-Betreiber sollten sich dieses Risikos bewusst sein.

Nachdem im Rahmen der Hausdurchsuchung dann die benötigten Beweismittel beschlagnahmt worden waren, war nun auch die Führung des Tatnachweises möglich. Dabei musste ich feststellen, dass der Betroffene die Videoaufzeichnungen nicht nur dazu genutzt hatte, um vermeintliche Verkehrsverstöße Dritter zu dokumentieren und zur Anzeige zu bringen, sondern auch um gegenüber seinem seinerzeitigen Arbeitgeber Beweismittel für durch ihn im Rahmen seiner Tätigkeit als Kurierfahrer geleistete Mehrarbeit zu sammeln. Zu diesem Zweck hatte er von seinen diesbezüglichen Fahrten längere Videozusammenschnitte erstellt, die dokumentieren sollten, wie lange er zur Erfüllung einzelner Fahrtaufträge auf welchen Routen unterwegs gewesen war und welche Ursachen (zum Beispiel Staus) zu einer erheblichen Verlängerung der Fahrtdauer geführt hatten. Diese Aufzeichnungen sollten zugleich auch dem Zoll im Rahmen von Ermittlungen gegen den Arbeitgeber des Betroffenen zur Verfügung gestellt werden.

Dass eine solche Zweckbestimmung nicht geeignet ist, einen Dashcam-Einsatz mit Daueraufzeichnung zu rechtfertigen, liegt auf der Hand. Die vom Betroffenen bezweckten Nachweise sind auch anderweitig zu erbringen. Das heißt, eine permanente Aufzeichnung des Straßenverkehrs ist dafür schon nicht erforderlich. Zudem überwiegen hier die schutzwürdigen Interessen der anderen Verkehrsteilnehmer – während ihres Aufenthalts im öffentlichen Verkehrsraum nicht von ihnen unbekannten Personen mittels Video überwacht zu werden – das diesbezügliche Beweisinteresse des Betroffenen insbesondere auch deshalb klar, weil sie an den betreffenden Vorfällen und Ermittlungen (anders als etwa in Unfall- oder Gefahrensituationen) in keiner Weise beteiligt sind.

Soweit der Betroffene die Dashcam regelmäßig auch dazu verwendet hatte, mögliche Verstöße Dritter gegen die Straßenverkehrsordnung zu dokumentieren und zur Anzeige zu bringen, drängen sich Parallelen zum bekannten Fall des „Knöllchen-Horst“ aus Niedersachsen auf (vgl. dazu Oberlandesgericht Celle, Beschluss vom 4. Oktober 17, 3 Ss (OWi) 163/17 sowie Verwaltungsgericht Göttingen, Urteil vom 31. Mai 2017, 1 A 170/16).

Der Betroffene hatte die Dashcam permanent im Einsatz, später dann die seiner Ansicht nach relevanten Videosequenzen herausgeschnitten und schließlich unter Verwendung dieser bei der Polizei Anzeigen wegen vermeintlicher Verkehrsverstöße Dritter erstattet. Mit der permanenten Videodokumentation für den Fall des Begehens von Verkehrsordnungswidrigkeiten durch Dritte verfolgte er bereits keine schützenswerten eigenen Interessen, denn die Überwachung des Straßenverkehrs ist eine hoheitliche Aufgabe, die ausschließlich den dafür zuständigen Straßenverkehrsbehörden und der Polizei obliegt. Schon allein deshalb ist der Betrieb der Dashcam rechtswidrig gewesen. Überdies bestanden auch hier wiederum überwiegende schutzwürdige Interessen der anderen Verkehrsteilnehmer. Für sie bestand die Gefahr, dass sie aufgrund der Anzeigen mit von Dashcams aufgenommenen Videoaufzeichnungen zu Unrecht mit Ordnungswidrigkeitenverfahren überzogen werden. Die Aufgabe der Verfolgung von Verkehrsordnungswidrigkeiten oder -straftaten obliegt aber nicht einzelnen Verkehrsteilnehmern wie etwa dem Betroffenen, sondern nur den hierfür zuständigen Behörden (vgl. auch Tätigkeitsbericht 2019, 2.2.2., Seite 34 ff.). Die Einschätzungen und Auswertungen der zuständigen Polizeidienststellen zeigten im Übrigen, dass den Anzeigen zumeist noch nicht einmal Verkehrsverstöße zu entnehmen waren, solche also nur in der Vorstellung des Betroffenen existierten; zum Teil waren die dokumentierten Vorkommnisse auch durch den Betroffenen selbst provoziert worden – das Konfliktpotential bei der Auslieferung von Post- und Warensendungen ist ja allgemein bekannt.

6.4.3 Wem gehören die Verfahrensakten in Bußgeldverfahren?

Wenn Staatsanwaltschaften wegen einer Straftat geführte Ermittlungsverfahren einstellen, diese aber wegen der möglichen Verwirklichung eines Ordnungswidrigkeitentatbestandes an mich abgeben, kann ich sehr unterschiedliche Verfahrensweisen beobachten. Üblicherweise werden mir die entsprechenden Akten mit Empfangsbekenntnis ohne weitere Anmerkungen übergeben. Es gibt aber auch Staatsanwaltschaften, die mir die Akten zwar zur Verfolgung der Ordnungswidrigkeit in eigener Zuständigkeit übergeben, zugleich aber auch eine Rückgabe nach Verfahrensabschluss fordern oder eine Weitergabe an andere Stellen von ihrer Einwilligung abhängig machen.

Ich habe die Vermutung, dass solche Forderungen lediglich aus der ungeprüften Anwendung von Textbausteinen resultieren. Tatsächlich geht die Verfahrensherrschaft mit einer Abgabe nach § 43 Gesetz über Ordnungswidrigkeiten (OWiG) an die Verwaltungsbehörde, hier also an mich, über. Mit der Abgabe durch die Staatsanwaltschaft wird die Verwaltungsbehörde nach § 35 Abs. 1 OWiG für das Verfahren zuständig, ohne dass es der Einleitung eines Bußgeldverfahrens bedarf. Die Entscheidung über die weitere Vorgehensweise, insbesondere die Vornahme weiterer Ermittlungsmaßnahmen, die Verfahrenseinstellung oder den Abschluss mittels eines Bußgeldbescheides, liegt dann allein bei der Verwaltungsbehörde. Die Verwaltungsbehörde ist lediglich an die Entscheidung der Staatsanwaltschaft gebunden, ob eine Tat als Straftat verfolgt wird oder nicht (§ 44 OWiG).

Dies bedeutet, dass die Verfahrensakten nach Abschluss des Ordnungswidrigkeitenverfahrens gemäß den geltenden Aufbewahrungsfristen bei der Verwaltungsbehörde verbleiben und anschließend durch diese vernichtet werden; eine Rückgabe an die Staatsanwaltschaft scheidet aus.

Anders ist es lediglich im Fall eines Einspruchs gegen den von der Verwaltungsbehörde erlassenen Bußgeldbescheid, wenn die Verwaltungsbehörde diesem Einspruch nicht abhilft. Dann hat sie die Bußgeldakten über die Staatsanwaltschaft an das zuständige Amtsgericht zu übersenden (§ 69 Abs. 3 Satz 1 OWiG). Mit dem Eingang der Akten bei der Staatsanwaltschaft gehen die Aufgaben der Verfolgungsbehörde dann (wieder) auf die Staatsanwaltschaft über (§ 69 Abs. 4 OWiG). Soweit der Einspruch im Weiteren nicht zurückgenommen wird, verbleiben die Bußgeldakten dann also tatsächlich bei der Staatsanwaltschaft.

6.5 Öffentlichkeitsarbeit

Auch in diesem Berichtszeitraum erreichten mich zahlreiche Presseanfragen. Darunter waren Anfragen zum Gemeinsamen Kompetenz- und Dienstleistungszentrum zur Telekommunikationsüberwachung. Es war 2018 durch die Polizeien der Länder Berlin, Brandenburg, Sachsen, Sachsen-Anhalt und Thüringen gegründet worden (vgl. Tätigkeitsbericht 04/2017 bis 12/2018, Teil 1, 1.1.3.1, Seite 15 f.). Das Zentrum wird als Anstalt des öffentlichen Rechts in Leipzig auf Grundlage eines entsprechenden Staatsbetriebs unterhalten. Zu gewünschten technischen und organisatorischen Maßnahmen sowie Sicherheitskonzepten beziehungsweise Betriebseinzelheiten konnte ich allerdings zum damaligen Zeitpunkt keinen neuen Stand mitteilen. Ab April des Jahres häuften sich die Nachfragen zu Corona-Maßnahmen und damit einhergehender personenbezogener Datenverarbeitung, insbesondere im Zusammenhang mit einer Kontaktdatenerhebung und der Zulässigkeit von Melderegisterabfragen durch Gesundheitsbehörden zur Kontaktdatennachverfolgung in Sachsen (vgl. auch 1.1, 2.2.1 bis 2.2.7, 2.3.3 und 8.1). Im Verlauf des Berichtszeitraums folgten gehäuft presserechtliche Auskunftsersuchen zur Entscheidung des Europäischen Gerichtshofs „Schrems II“ (vgl. 5 und 9.3) und zu Vorgängen in der Polizei. Zusätzlich erreichten mich über 100 weitere Presseanfragen. Viele standen im Zusammenhang mit der Leitung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (vgl. 1.3).

Über die Website stellten die Mitarbeiter meiner Dienststelle fortlaufend Informationen insbesondere zum Datenschutz in der Coronavirus-Pandemie zur Verfügung. Dafür wurde eine gleichnamige Rubrik angelegt. Sie enthält unter anderem Beiträge zur datenschutzkonformen Nutzung von Tele-/Heimarbeit, der Auswertung von Telekommunikationsdaten zur Pandemiebekämpfung und ein Musterformular zur Erhebung von Kontaktdaten von Arbeitnehmern. Dabei war es mir wichtig, die Informationen praxisnah und verständlich aufzubereiten.

Weitere Unterstützung und Hinweise erhielten Interessenten beim Virtuellen Datenschutzbüro, an dem wir uns ebenfalls beteiligten. Dabei handelt es sich um ein Informationsportal für Bürger, das von institutionalisierten Datenschutzkontrollinstanzen betrieben wird: datenschutz.de

6.5.1 Schulungen und Vorträge

Im Berichtszeitraum haben Mitarbeiter aus meiner Dienststelle 16 Fortbildungsseminare gehalten, unter anderem an der Sächsischen Verwaltungs- und Wirtschafts-Akademie Dresden, am Fortbildungszentrum des Freistaates Sachsen, beim Landesamt für Schule und Bildung, beim Sächsischen Staatsarchiv und auf einer Tagung für Datenschutzbeauftragte aus dem Justizbereich. Im Vergleich zu den Vorjahren ist hier ein Rückgang bei der Dozententätigkeit festzustellen. Das lag zum einen an den Infektionsschutz-Maßnahmen im Zusammenhang mit der Coronavirus-Pandemie, weshalb etliche Veranstaltungen abgesagt wurden, zum anderen am Arbeitsvolumen der Mitarbeiter in der Dienststelle (vgl. 6.3).

In den Vorträgen im Berichtszeitraum wurden unter anderem Grundlagen und aktuelle Fragen zur Datenschutz-Grundverordnung behandelt. Auf weiteren Veranstaltungen sprachen meine Mitarbeiter über den Datenschutz in Schulen, in der Kommunalverwaltung, im Maßregelvollzug und über den Datenschutz nach dem Zehnten Buch Sozialgesetzbuch (SGB X).

7 Zusammenarbeit der Datenschutzaufsichtsbehörden, Datenschutzkonferenz

7.1 Konferenztätigkeit

Wie unter 1.3 bereits dargestellt hatte ich im Berichtszeitraum den Vorsitz der Datenschutzkonferenz (DSK) inne. Parallel dazu waren wir auch in den 26 Arbeitskreisen vertreten. Handelte es sich in den Anfangsjahren Ende der 70er bei der DSK noch um lockere Zusammentreffen von staatlichen Datenschutzbeauftragten, so ist daraus im Laufe der Zeit ein unverzichtbares Arbeitsinstrument für den Datenschutz in Deutschland und Europa geworden. Ein Blick auf die nachfolgenden Entschließungen, Beschlüsse und Orientierungshilfen verdeutlicht, wie vielfältig und komplex die Themen sind, mit denen sich die DSK im Berichtszeitraum befasste. In der digitalen Ausgabe des Tätigkeitsberichts sind die Dokumente verlinkt.

7.2 Materialien der Datenschutzkonferenz – Entschließungen

Entschließungen sind öffentliche Stellungnahmen der DSK zu datenschutzpolitischen Fragen, beispielsweise zur Einführung eines neuen Gesetzes. Entschließungen benötigen eine zwei Drittel Mehrheit in der DSK.

- Auskunftsverfahren für Sicherheitsbehörden und Nachrichtendienste verfassungskonform ausgestalten (25.11.2020)
- Betreiber von Webseiten benötigen Rechtssicherheit - Bundesgesetzgeber muss europarechtliche Verpflichtungen der „ePrivacy-Richtlinie“ endlich erfüllen (25.11.2020)
- Für den Schutz vertraulicher Kommunikation durch eine sichere Ende-zu-Ende-Verschlüsselung – Vorschläge des Rates der Europäischen Union stoppen (25.11.2020)
- Datenschutz braucht Landgerichte auch erstinstanzlich (22.09.2020)
- Digitale Souveränität der öffentlichen Verwaltung herstellen – Personenbezogene Daten besser schützen (22.09.2020)
- Patientendaten-Schutz-Gesetz: Ohne Nachbesserungen beim Datenschutz für die Versicherten europarechtswidrig! (01.09.2020)
- Registermodernisierung verfassungskonform umsetzen! (26.08.2020)
- Polizei 2020 – Risiken sehen, Chancen nutzen! (16.04.2020)
- Datenschutz-Grundsätze bei der Bewältigung der Corona-Pandemie (03.04.2020)

7.3 Materialien der Datenschutzkonferenz – Beschlüsse

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

- Telemetriefunktionen und Datenschutz beim Einsatz von Windows 10 Enterprise (26.11.2020)
- Anwendung der DSGVO auf Datenverarbeitungen von Parlamenten (22.09.2020)
- Einsatz von Wärmebildkameras bzw. elektronischer Temperaturerfassung im Rahmen der Corona-Pandemie (10.09.2020)
- Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zu Vorabwidersprüchen bei StreetView und vergleichbaren Diensten (12.05.2020)
- Hinweise zum Einsatz von Google Analytics im nicht-öffentlichen Bereich (12.05.2020)
- Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zu den Einwilligungsdokumenten der Medizininformatik-Initiative des Bundesministeriums für Bildung und Forschung (27.04.2020)

7.4 Materialien der Datenschutzkonferenz – Orientierungshilfen

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

- Checkliste Datenschutz in Videokonferenzsystemen bezogen auf die Orientierungshilfe Videokonferenzsysteme, Stand: 23.10.2020 (11.11.2020)
- Videokonferenzsysteme (23.10.2020)
- Videoüberwachung durch nicht-öffentliche Stellen (03.09.2020)
- Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail (12.05.2020)

7.5 Materialien der Datenschutzkonferenz – Anwendungshinweise

- Anforderungen zur Akkreditierung gemäß Artikel 43 Abs. 3 DSGVO in Verbindung mit DIN EN ISO/IEC 17065 (Version 1.4) (08.10.2020)

- Anforderungen zur Akkreditierung einer Überwachungsstelle für Verhaltensregeln nach Artikel 41 DSGVO in Verbindung mit Artikel 57 Absatz 1 lit. p 1. Alt. DSGVO (23.09.2020)
- Standard-Datenschutzmodell Version 2.0b (17.04.2020)

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

Der Europäische Datenschutzausschuss verabschiedete die nachstehend aufgeführten Dokumente, die in der digitalen Ausgabe des Tätigkeitsberichts verlinkt sind.

- Guidelines 10/2020 on restrictions under Article 23 GDPR
- Guidelines 2/2020 on articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies
- Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR
- Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten
- Empfehlungen 02/2020 zu den wesentlichen europäischen Garantien in Bezug auf Überwachungsmaßnahmen
- Guidelines 4/2019 on Article 25 Data Protection by Design and by Default
- Guidelines 09/2020 on relevant and reasoned objection under Regulation 2016/679
- Guidelines 08/2020 on the targeting of social media users
- Guidelines 07/2020 on the concepts of controller and processor in the GDPR
- Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR
- Leitlinien 5/2019 zu den Kriterien des Rechts auf Vergessenwerden in Fällen in Bezug auf Suchmaschinen gemäß der DSGVO (Teil 1) - version adopted after public consultation
- Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679
- Leitlinien 3/2020 für die Verarbeitung von Gesundheitsdaten für wissenschaftliche Forschungszwecke im Zusammenhang mit dem COVID-19-Ausbruch
- Leitlinien 04/2020 für die Verwendung von Standortdaten und Tools zur Kontaktnachverfolgung im Zusammenhang mit dem Ausbruch von COVID-19
- Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak

- Guidelines 2/2020 on articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies
- Leitlinien 3/2019 zur Verarbeitung personenbezogener Daten durch Videogeräte
- Guidelines 3/2019 on processing of personal data through video devices - version adopted after public consultation
- Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications

7.7 Europäischer Datenschutztag zum Thema „Cross-Border Data Transfers“

In der zweiten Hälfte des Berichtszeitraums, das heißt ab Juni 2020, war ich intensiv mit der Vorbereitung des noch in meine Vorsitz-Verantwortlichkeit fallenden 15. Europäischen Datenschutztages am 28. Januar 2021 zum Thema „Cross-Border Data Transfers“ beschäftigt. Für die schließlich als Onlinekonferenz durchgeführte Veranstaltung konnte ich zusammen mit dem Bundesministerium des Innern, für Bau und Heimat (BMI) herausragende Fachleute aus dem Europarat und der Europäischen Union gewinnen. Die Konferenz war mit knapp 1.000 Onlinebesuchern aus der ganzen Welt der bestbesuchte Europäische Datenschutztag seit seinem Bestehen.

Traditionell obliegt die Veranstaltung des Europäischen Datenschutztages am 28. Januar eines jeden Jahres dem DSK-Vorsitzenden des Vorjahres. Die seit Anfang März 2020 herrschenden „Corona-Bedingungen“ mit einem ersten Lockdown, das heißt der Schließung größerer Versammlungsstätten, anschließender Lockerung und schließlich einem zweiten Lockdown, der im Herbst 2020 absehbar wurde, machten die Organisation, Vorbereitung und schließlich Durchführung des Datenschutztages 2021 zu einer aufwendigen, die Kräfte meines kleinen Teams bis an die Grenze fordernden Aufgabe. Im Grunde hatte ich stets parallel sowohl eine Präsenz- als auch eine Videokonferenz vorzubereiten.

Als Glück im Unglück empfand ich die – außergewöhnliche, durch den anstehenden 40. Jahrestag der (Datenschutz-)„Konvention 108“ des Europarates von 1981 bedingte – Zusammenarbeit mit dem BMI. Das BMI erwies sich als starker und hilfreicher Partner, mit dessen Beamten zusammenzuarbeiten eine Freude war. Im Herbst 2020 entschieden wir uns gemeinsam zur Durchführung einer reinen Onlineveranstaltung. Als Thema legten wir einvernehmlich die Voraussetzungen der Übermittlung personenbezogener Daten aus der EU beziehungsweise den Ländern der Europäischen Freihandelsassoziation (EFTA) in Drittstaaten fest („Cross Border Data Transfers“). Damit hatten wir ein nach dem „Schrems II“-Urteil des Europäischen Gerichtshofs (EuGH) vom 16. Juli 2020 (C 311/18) hochaktuelles und vor allem für die Wirtschaft bedeutendes Thema. Denn mit diesem Urteil hatte die bereits durch das Vorgänger-Urteil des EuGH vom 6. Oktober 2015 (C-362/14) zu „Safe Harbor“ aufgeworfene Frage nach

den Voraussetzungen von Datenübermittlungen aus der EFTA in Drittstaaten – dringlich – an Bedeutung gewonnen. Für die Europarats-Seite sollte das BMI, für die Seite der EU beziehungsweise des EFTA sollte ich die Referenten gewinnen.

Auf meiner Seite hatte ich das Glück und die Ehre, Herrn Prof. Dr. Dr. h.c. Thomas von Danwitz, Richter am EuGH und Berichterstatter im „Schrems II"-Fall, sowie Herrn Aleid Wolfsen LL.M., stellvertretender Vorsitzender des Europäischen Datenschutzausschusses und Vorsitzender der niederländischen Aufsichtsbehörde (Autoriteit Persoonsgegevens) als Referenten gewinnen zu können. Beiden sei an dieser Stelle herzlich gedankt. Meine Auswahl wurde in großartiger Weise ergänzt durch die vom BMI gewonnenen Referenten, Frau Alessandra Perucci, Vorsitzende des Übereinkommensausschusses der Datenschutzkonvention 108 des Europarats, und Herrn Dr. h. c. Tim Eicke QC, Richter am Europäischen Gerichtshof für Menschenrechte (EGMR).

Die schließlich am 28. Januar 2021 von 12 bis 16 Uhr durchgeführte Veranstaltung begann mit Grußworten des Parlamentarischen Staatssekretärs im BMI, Herrn Stephan Mayer, der Generalsekretärin des Europarats, Frau Marija Pejčinović Burić und meinerseits. Im Anschluss daran stellten die Referenten in jeweils circa 20-minütigen Vorträgen ihre Auffassungen dar. Richter Eick referierte zur Bedeutung der Datenschutzkonvention 108 und erinnerte an die wichtigsten Datenschutzfälle des EGMR in den letzten 20 Jahren. Frau Perucci stellte die Geschichte und den Geltungsbereich der Konvention 108 dar. Die Konvention ist bis dato von 56 Staaten ratifiziert worden, darunter auch sechs afrikanische und drei südamerikanische Staaten. Seit 2018 existiert zu ihrer Anpassung an die DSGVO ein Änderungsprotokoll, was sie seither zur „Konvention 108+" macht. Diese angepasste Konvention ist leider bisher nur durch elf Vertragsstaaten ratifiziert worden (zum Inkrafttreten erforderlich wären 38 Staaten). Frau Perucci äußerte dennoch die Hoffnung, dass noch mehr Staaten der Konvention beitreten werden, da sie zur Gewährleistung eines ausreichenden Schutzniveaus für den Transfer der Daten beitrage. Danach verdeutlichte Herr Wolfsen LL. M., dass gerade bei der jetzigen unsicheren Rechtslage gut ausgestattete Aufsichtsbehörden für den Datenschutz wichtig seien, denn es läge nunmehr in der Hand jedes Unternehmens selbst, die Voraussetzungen für einen rechtmäßigen Transfer in einen Drittstaat zu erfüllen. Herr Professor Dr. von Danwitz stellte gleich zu Beginn seiner Ausführungen auf die Frage des Moderators hin klar, dass er bei korrekter Anwendung der Vorschriften des DSGVO keine andere Entscheidung als in „Schrems II" habe treffen können.

In der nachfolgenden Diskussion stellten sich die Referenten den zahlreichen Fragen des Publikums. So verneinten sie unter anderem die Frage, ob zwischen gefährdeten und weniger gefährdeten Daten unterschieden werden könne und letztere mit weniger Aufwand in einen Drittstaat übertragen werden könnten.

Am Ende stand ein Schlusswort der neuen Vorsitzenden der Datenschutzkonferenz, der saarländischen Landesbeauftragten Monika Grethel.

Mein Dank gilt nochmals allen Referenten und allen, die zur Durchführung dieser herausragenden Veranstaltung beigetragen haben.

Die Veranstaltung kann nachträglich in der Mediathek des BMI angesehen werden.

7.8 Gemeinsame Überprüfung von Medienunternehmen durch Datenschutzaufsichtsbehörden

Das Setzen von Cookies und die Einbindung von Diensten Dritter durch Websites sind nach wie vor Gegenstand zahlreicher Beschwerden. Zwar hat sich mit In-Kraft-Treten der Datenschutz-Grundverordnung (DSGVO) durchgesetzt, dass viele dieser Datenverarbeitungen einer Einwilligung bedürfen, Art und Weise wie diese Einwilligungen eingeholt werden, verstoßen jedoch oft gegen geltendes Recht. Mit den Urteilen des Europäischen Gerichtshofs (EuGH) vom 1. Oktober 2019 des Bundesgerichtshofs (BGH) vom 28. Mai 2020 hat sich auch die Rechtsprechung dahingehend geäußert, dass eine aktive Einwilligung in das Setzen und Auslesen von Cookies erforderlich sei. Die Datenschutzaufsichtsbehörden haben sich frühzeitig mit diesen Rechtsfragen auseinandergesetzt und mit der Orientierungshilfe für Anbieter von Telemedien im März 2019 (abrufbar auf datenschutzkonferenz-online.de) Hinweise zur Anwendung der DSGVO bei Fragen der Gestaltung von Websites gegeben. Darüber hinaus hat sich die Datenschutzkonferenz (DSK) in Bezug auf den Einsatz von Google Analytics geäußert, dem wohl am weitesten verbreiteten Tracking-Dienst. Die Hinweise aus dem DSK-Beschluss können auf datenschutzkonferenz-online.de heruntergeladen werden.

Im Frühjahr 2020 haben sich insgesamt elf der deutschen Datenschutzaufsichtsbehörden entschlossen, eine gemeinsame Prüfung der jeweils reichweitenstärksten Medienunternehmen im jeweiligen Bundesland durchzuführen. Dazu wurde eine ständige Arbeitsgruppe etabliert, welche Fragebögen zur Verwendung von Cookies, Drittanbietern und der Gestaltung von Einwilligungslösungen für die von den Medienunternehmen betriebenen Websites erarbeitet hat. Diese wurden im Sommer an die Medienunternehmen versandt, die Rückläufe werden derzeit ausgewertet. Die Fragebögen werden ausschließlich innerhalb der jeweiligen Zuständigkeiten der Aufsichtsbehörden ausgewertet, dennoch findet zu einzelnen Fragestellungen der Bewertung ein reger Austausch statt.

Auch wenn die Prüfung 2020 noch nicht abgeschlossen war, kann festgestellt werden, dass der Anteil der ohne eine Einwilligung gesetzten Cookies und Tracking-Elemente im Vergleich zum Frühjahr 2020 bei Abgabe der Fragebögen im Herbst 2020 um circa 50 Prozent zurückgegangen ist. Dies ist sicherlich auch auf die Urteile der obersten Gerichte zurückzuführen, zeigt aber deutlich, dass den Verantwortlichen klar geworden ist, dass Änderungen erforderlich sind (vgl. auch Tätigkeitsbericht 2019, 9.4, Seite 167 und 9.10, Seite 172 ff.).

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

8.1 Nutzung von „Corona-Besucherlisten“ für Strafverfolgungszwecke

Der Berichtszeitraum stand im Zeichen der Pandemie und der Maßnahmen zur Verhinderung der Ausbreitung des SARS-Cov2-Virus. Eine Möglichkeit Ansteckungswege zurückverfolgen zu können, wurde in der Verpflichtung bestimmter Betriebe und Einrichtungen gesehen, Listen zu führen, in denen Besucher beziehungsweise Gäste ihre Kontaktdaten für den Fall einer eventuell notwendigen Kontaktnachverfolgung angeben sollten.

Nicht unumstritten war einige Monate lang, ob die Polizei diese Listen für Zwecke der Strafverfolgung nutzen durfte. Zwar dienten die Listen dem erklärten und begrenzten Zweck, den Gesundheitsämtern Kontaktnachverfolgungen von infizierten Personen zu ermöglichen. Allerdings fanden die Verpflichtung zum Führen von Besucherlisten und deren enge Zweckbindung ihre Grundlage lediglich in Verordnungen der Bundesländer.

Die bundesgesetzlichen Regelungen der Strafprozessordnung (StPO) zur Herausgabe von Gegenständen und Unterlagen, die als Beweismittel für die Strafverfolgung von Bedeutung sein können, zu ihrer Sicherstellung und Beschlagnahme blieben von den landesrechtlichen Zweckbestimmungen unberührt. Rechtlich war die polizeiliche Forderung zur Herausgabe von Besucherlisten für Zwecke der Strafverfolgung daher nicht zu beanstanden. Es gab keine bundesgesetzliche Regelung, die eine Nutzung der Listen für andere Zwecke als den des Infektionsschutzes untersagte.

Das änderte sich mit Inkrafttreten der Änderung des Infektionsschutzgesetzes (IfSG) am 19. November 2020. § 28a Abs. 4 IfSG bestimmte nun, dass Kontaktlisten beziehungsweise die in ihnen enthaltenen Daten zu keinem anderen Zweck als der Aushändigung auf Anforderung der zuständigen Gesundheitsbehörde verwendet werden dürfen, die wiederum die Daten ausschließlich zu Zwecken der Kontaktverfolgung weiterverwenden darf.

Diese bundesgesetzliche Vorschrift stellt eine besondere bundesgesetzliche Verwendungsregelung im Sinne von § 160 Abs. 4 StPO dar, die einer Nutzung der Daten aus Kontaktlisten zur Nachverfolgung von Infektionsketten für Zwecke der Strafverfolgung entgegensteht.

8.2 Einsatz von Bodycams bei der sächsischen Polizei

Im Herbst 2019 wurde mir das Konzept zur landesweiten Einführung von körpernah getragenen Aufnahmegeräten („Bodycams“) in der sächsischen Polizei vorgestellt. Bereits zuvor wurde ich sowohl im Gesetzgebungsverfahren als auch bei der Erarbeitung der Errichtungsanordnung durch das Sächsische Staatsministerium des Innern eng eingebunden. Nach einer vorangegangenen Erprobungsphase in ausgewählten Polizeidirektionen und Schaffung einer speziellen Ermächtigungsgrundlage im neuen Polizeivollzugsdienstgesetz war geplant – beginnend mit dem Jahr 2020 – über einen Zeitraum von zwei Jahren, die Organisationseinheiten (hierbei unter anderem die Einrichtungen für die Aus- und Fortbildung sowie den Streifendienst) mit insgesamt circa 1.500 Kameras, mit denen Bild- und Tonaufzeichnungen gefertigt werden können, auszustatten. Vorrangiges Ziel der Anwendung soll die Eigensicherung der Polizeibeamten sein. Die Bodycams sollen dazu beitragen, konfliktbehaftete Situationen zu deeskalieren und damit auch gewalttätige Übergriffe auf Dritte zu verhindern. Ferner soll das Verfahren die Beweisführung im Rahmen der Strafverfolgung unterstützen. Der präventive Einsatz von Bodycams zur Eigensicherung oder zum Schutz Dritter ist in allen öffentlich zugänglichen Bereichen möglich und richtet sich nach § 57 Absätze 4 bis 9 Sächsisches Polizeivollzugsdienstgesetz (SächsPVDG). Rechtsgrundlage für den Einsatz zur Strafverfolgung sind § 100h Abs. 1 Nr. 1 StPO, § 100f Abs. 1 Strafprozessordnung (StPO).

Gemäß § 57 Abs. 6 SächsPVDG ist der Einsatz der Bodycams in geeigneter Weise besonders erkennbar zu machen. Daher werden die Bodycams nur offen und in Verbindung mit dem entsprechenden neongelben Hinweisschild „Video Audio“ getragen. Der Beginn der Aufzeichnung wird der betroffenen Person grundsätzlich mitgeteilt. Die Bodycams sind so konfiguriert, dass Aufzeichnungen äußerlich erkennbar sind. Die Polizeivollzugsbediensteten sind angehalten, die Aufzeichnung unbeteiligter Dritter auf ein unumgängliches Mindestmaß zu beschränken. Nach der gesetzlichen Regelung (in § 57 Abs. 4 SächsPVDG) ist das sogenannte Pre-Recording zulässig. Dabei werden die Aufzeichnungen kurzzeitig in einem Zwischenspeicher bis zu 60 Sekunden abgelegt, danach aber permanent überschrieben. Erst beim Starten der eigentlichen Aufnahme (unter den Voraussetzungen des § 57 Abs. 5 SächsPVDG – Vorliegen einer konkreten Gefahr für Leib oder Leben) werden die Bildaufnahmen dieser „Anbahnungsphase“ länger gespeichert und stehen zur Weiterverarbeitung zur Verfügung.

Die Aufzeichnungen werden gemäß § 57 Abs. 7 Satz 3 SächsPVDG nach Ablauf von 30 Tagen automatisch gelöscht, wenn sie nicht zur Verfolgung von Straftaten oder zur Überprüfung der Rechtmäßigkeit der Maßnahme oder der Aufnahme selbst benötigt werden.

Entsprechend der gesetzlichen Anordnung in § 57 Abs. 7 Satz 4 und 5 SächsPVDG ist das Verfahren der Einsichtnahme in Aufzeichnungen von Bodycams in einer Verwaltungsvorschrift geregelt (VwV Einsicht Bodycam).

Hiernach erhalten betroffene Personen – dies sind alle Personen, von denen im Rahmen eines Bodycam-Einsatzes Bild- oder Tonaufzeichnungen gefertigt wurden, auch Polizeibedienstete und unbeteiligte Dritte – Einsicht in die Aufzeichnungen. Die Einsichtnahme ist beschränkt auf Aufzeichnungen, die den Antragsteller betreffen. Ausnahmsweise kann die Einsichtnahme auch in Aufzeichnungen gewährt werden, die Bild-und Tonsequenzen zu anderen Personen enthalten, soweit dies aus Gründen des Sachzusammenhangs zwingend erforderlich ist. Hierbei sollen die anderen Personen nach Möglichkeit anonymisiert werden.

Das Recht auf Einsichtnahme in Aufzeichnungen, die zu den anderen in § 57 Abs. 7 Satz 3 SächsPVDG genannten Zwecken, zum Beispiel in einem Strafverfahren, benötigt werden oder bereits zu diesem Zweck aufgenommen wurden, richtet sich nach den jeweiligen Regelungen der Akteneinsicht (beispielsweise § 147 StPO). Neben dem Recht auf Einsichtnahme haben die betroffenen Personen gegenüber der Polizei einen Auskunftsanspruch über die sie betreffende Verarbeitung personenbezogener Daten gemäß § 92 Abs. 2 SächsPVDG in Verbindung mit § 13 Sächsisches Datenschutz-Umsetzungsgesetz.

Der Einsatz von Bodycams wird nach der Anordnung in § 57 Abs. 9 SächsPVDG spätestens Ende 2024 durch die Staatsregierung evaluiert.

Aus datenschutzrechtlicher Sicht wird durch die gesetzliche Regelung und die untergesetzlichen Vorschriften ein erfreulich hohes Maß an Transparenz bei der Verarbeitung personenbezogener Daten mittels Bodycams erreicht. Ich gehe davon aus, dass die gesetzlichen Anwendungsvoraussetzungen und Schutzvorkehrungen unangemessene Eingriffe in Rechte Betroffener auch in der praktischen Anwendung verhindern.

8.3 Auskunftsanspruch des Betroffenen des Bußgeldverfahrens zur Person des Anzeigeerstatters

Auch im Berichtszeitraum erreichten mich Beschwerden von Personen, gegen die ein Bußgeldverfahren geführt wurde und denen die Verwaltungsbehörde die von ihnen begehrte Auskunft über die Person des Anzeigeerstatters verweigerte, zumeist unter Hinweis auf die schutzwürdigen Interessen des Anzeigeerstatters. Ein solches Vorgehen der Verwaltungsbehörde ist jedenfalls dann rechtswidrig, wenn die Hinweise oder Aussagen des Anzeigeerstatters die einzige Grundlage für das Bußgeldverfahren sind, wie es in Verfahren, die allein auf sog. Bürgeranzeigen basieren, zumeist der Fall ist.

Leitet die zuständige Verwaltungsbehörde ein Bußgeldverfahren ein, findet die Verarbeitung personenbezogener Daten insoweit nicht im Anwendungsbereich der Datenschutzgrundverordnung (DSGVO) statt. Die Ausnahme des Art. 2 Abs. 2 Buchst. d DSGVO erfasst nicht nur Straftaten, sondern auch Ordnungswidrigkeiten nach deutschem Recht. Im einschlägigen An-

wendungsbereich der Richtlinie (EU) 2016/680 richtet sich die Verarbeitung personenbezogener Daten nach den Vorschriften des Ordnungswidrigkeitengesetzes (OWiG), der Strafprozessordnung (StPO) und – über § 500 StPO – des 3. Teils des Bundesdatenschutzgesetzes (BDSG).

Der datenschutzrechtliche Auskunftsanspruch der betroffenen Person nach § 57 BDSG, der nach § 57 Abs. 1 Nr. 2 BDSG auch Informationen über die Herkunft der Daten erfasst, kann nach § 57 Abs. 4 in Verbindung mit § 56 Abs. 2 BDSG eingeschränkt werden, unter anderem wenn Rechtsgüter Dritter gefährdet würden und das Interesse an der Vermeidung dieser Gefahren das Informationsinteresse der betroffenen Person überwiegt.

Der Betroffene hat neben dem allgemeinen datenschutzrechtlichen Auskunftsanspruch nach § 57 BDSG auch ein Akteneinsichtsrecht (§ 49 Abs. 1 Gesetz über Ordnungswidrigkeiten (OWiG)). Auch nach dieser Vorschrift sind schutzwürdige Interessen Dritter zu berücksichtigen und können im Falle ihres Überwiegens einer Einsicht des Betroffenen entgegenstehen.

Hat der Betroffene einen Verteidiger, richtet sich dessen Akteneinsichtsrecht nach § 46 Abs. 1 OWiG in Verbindung mit § 147 Abs. 1 StPO. Eine Besonderheit dieses Rechts – im Vergleich zu den Ansprüchen des Betroffenen ohne Verteidiger – besteht darin, dass schutzwürdige Interessen Dritter keinen Grund für die Verweigerung der Akteneinsicht bilden. Allein die Gefährdung des Untersuchungszwecks vor Abschluss der Ermittlungen rechtfertigt nach § 147 Abs. 2 StPO die (teilweise) Versagung der Akteneinsicht.

Wurde mit einer Anzeige auch der Name des Anzeigeerstatters zur Akte genommen, erstreckt sich das umfassende Akteneinsichtsrecht des Verteidigers also auch auf diese Informationen.

Auch wenn der Betroffene keinen Verteidiger hat, wird es in Bußgeldverfahren zur Offenlegung der Identität des Anzeigeerstatters kommen müssen, wenn dieser als Zeuge benannt wird (entweder durch die Verwaltungsbehörde, soweit sie ihren Bußgeldbescheid auf die Wahrnehmung des Anzeigeerstatters stützt, oder durch das Gericht oder den Betroffenen im gerichtlichen Verfahren).

In derartigen Konstellationen erfordern das Rechtsstaatsprinzip und der Grundsatz des fairen Verfahrens, dass gegenüber dem Betroffenen das „Beweismittel“ benannt wird und er sich mit dem Beweismittel (Zeugenaussage) auseinandersetzen können muss.

Es gehört zum Wesensgehalt eines rechtsstaatlichen Verfahrens im Bereich der Verfolgung von Straftaten und Ordnungswidrigkeiten, wo das Gewaltmonopol des Staates besonders deutlich zutage tritt, dass die zuständigen staatlichen Behörden “mit offenem Visier“ agieren.

Entscheidungen, die mit Eingriffen in Rechtspositionen der Beschuldigten/Betroffenen verbunden sind, dürfen grundsätzlich nicht auf der Grundlage von „geheimen“ Informationen getroffen werden.

Je bedeutsamer eine Information für das Verfahren (und die behördliche Entscheidung) ist, desto größer und schutzwürdiger ist das Interesse des Beschuldigten beziehungsweise Betroffenen, Zugang zu dieser Information zu erhalten; nicht zuletzt, um die Information bewerten und sich angemessen verteidigen zu können. Insbesondere in Fällen, in denen die Anzeige eines Dritten und gegebenenfalls dessen Lichtbild eines vermeintlichen Regelverstoßes die einzige Grundlage für das behördliche Verfahren sind und dies in der schriftlichen Verwarnung/Anhörung des Betroffenen unter der Rubrik „Beweismittel/Zeugen“ so auch angegeben wird, liegt ein überwiegendes schutzwürdiges Interesse des Anzeigeerstatters an der Geheimhaltung seines Namens regelmäßig nicht vor.

Voraussetzung für eine Beschränkung der Akteneinsicht beziehungsweise Auskunft an den Betroffenen hinsichtlich der Identität des Anzeigeerstatters wäre, dass dessen schutzwürdige Interessen (§ 49 Abs. 1 Satz 1 OWiG) beziehungsweise eventuell gefährdete Rechtsgüter Dritter (§ 57 Abs. 4 in Verbindung mit § 56 Abs. 2 Nr. 3 BDSG) das Interesse des Betroffenen an der Kenntnis der Herkunft seiner Daten, die die Behörde (gegen ihn) verarbeitet, überwiegen. Das Bejahen eines schutzwürdigen Interesses des Anzeigeerstatters an der Geheimhaltung seines Namens allein ist also keineswegs ausreichend, um das Einsichts- beziehungsweise Auskunftsrecht des Betroffenen zu beschränken. Abgesehen davon, dass die Schutzwürdigkeit eines solchen Interesses durchaus kontrovers diskutiert werden kann (zum Beispiel in Bezug auf Fälle falscher Verdächtigung, Verleumdung und ähnliches), kommt ein „Überwiegen“ dieses Interesses des Anzeigeerstatters in Fällen der „Bürgeranzeige“ und ohne eigene, durch die Verwaltungsbehörde selbst gesicherte Beweismittel unter keinem Gesichtspunkt in Betracht.

Die Verwaltungsbehörde entscheidet in eigener Verantwortung, ob sie Verfahren allein auf Grundlage von Angaben Dritter durchführt – mit der Konsequenz, dass deren Daten gegenüber dem vom Verfahren Betroffenen auf dessen Antrag oder von Amts wegen im Bußgeldbescheid offenzulegen sind – oder ob auf Bürgerhinweise Mitarbeiter der Behörde am Ort des angezeigten Vorfalls selbst Wahrnehmungen machen und Beweise sichern. Dann, wenn also das Verfahren gerichtsfest auf eigene Beweismittel gestützt werden kann und der Name des Hinweisgebers für das Verfahren unerheblich ist, kann im Einzelfall auch die Entscheidung über dessen Offenlegung im Rahmen der Akteneinsicht beziehungsweise der Auskunft an den Betroffenen anders ausfallen.

9 Rechtsprechung zum Datenschutz

9.1 Anfechtungsklage wegen eines Kostenbescheids des Sächsischen Datenschutzbeauftragten und Antrag auf Wiedereinsetzung in den vorherigen Stand

Verwaltungsgerichtlich hatte ich mich mit einem Aufsichtsverfahren auseinanderzusetzen, welches bereits im Januar 2017 mit der Feststellung einer Reihe von Datenschutzverstößen einschließlich einer entsprechenden Kostenfestsetzung seitens meiner Dienststelle abgeschlossen worden war.

Auslöser des schon im September 2014 begonnenen anlassbezogenen Aufsichtsvorgangs war eine Eingabe zur Ausrüstung von Betriebs-Lkw mit GPS-Sendern. Im Zuge der Bearbeitung des Aufsichtsvorganges waren eine Reihe datenschutzrechtlicher Verstöße festgestellt und im abschließenden Feststellungs- und Kostenbescheid konkret benannt worden. Dieser Bescheid war im Februar 2017 bestandskräftig geworden.

Etwas überrascht war ich dann schon, als der Prozessbevollmächtigte der verantwortlichen Stelle im März 2017 beim Verwaltungsgericht zunächst die Wiedereinsetzung in den vorherigen Stand und darüber hinaus die Aufhebung des Festsetzungs- und Kostenbescheides beantragt hatte. Nach meiner Auffassung war der Antrag unbegründet, da der Antragsteller die gebotene und nach den Umständen zumutbare Sorgfalt nicht gewahrt, das heißt, das Versäumnis der rechtzeitigen Klageerhebung selbst verschuldet hatte. Dabei war dieses Versäumnis in erster Linie durch den Prozessbevollmächtigten zu verantworten, insoweit aber dem Antragsteller entsprechend zuzurechnen (§ 173 Verwaltungsgerichtsordnung in Verbindung mit § 85 Abs. 2 Zivilprozessordnung). Der Prozessbevollmächtigte hatte eine plötzliche Arbeitsunfähigkeit infolge eines Unfalls als Rechtfertigung angeführt, dabei aber insbesondere nicht darlegen können, dass er eine geeignete Notfall-Vorsorge getroffen hatte, die auch bei einer unvorhergesehenen Verhinderung die Funktionsfähigkeit der Kanzlei, insbesondere die Überwachung der Fristsachen, gewährleistet. Im Übrigen bedeutet Arbeitsunfähigkeit nicht zugleich auch Handlungsunfähigkeit. Auch im Fall eines Unfalls beziehungsweise einer plötzlichen Erkrankung ist es einem Rechtsanwalt zuzumuten, seine Mandanten entsprechend zu informieren, damit diese eventuelle Fristversäumnisse selbst abwenden können.

Das zuständige Verwaltungsgericht ist meiner diesbezüglichen Argumentation gefolgt und hat die Klage mit Gerichtsbescheid wegen Unzulässigkeit abgewiesen; Wiedereinsetzung in den vorigen Stand wurde also nicht gewährt.

Abgeschlossen war diese Angelegenheit damit aber immer noch nicht. Nachdem ich guten Glaubens ob der Rechtskraft des Gerichtsbescheides zwei Monate später bei der verantwortlichen Stelle die weiterhin ausstehenden Kosten angemahnt hatte und diese tatsächlich auch beglichen worden waren, erreichte mich wiederum zwei Monate später völlig unerwartet in gleicher Sache eine Ladung zur mündlichen Verhandlung. Ursache der nicht eingetretenen Rechtskraft des Gerichtsbescheides waren offensichtlich Probleme beim Nachweis seiner Zustellung an den Prozessbevollmächtigten. Dieser hatte dem Gericht erst drei Monate nach Zusendung – nach mehreren erfolglosen Nachfragen – das elektronische Empfangsbekenntnis für den Gerichtsbescheid übersandt und darauf auf-bauend geltend gemacht, diesen erst zu diesem späten Zeitpunkt zur Kenntnis genommen zu haben, so dass die Frist zur Einlegung eines Rechtsmittels für ihn noch nicht ab-gelaufen sei. Das Gericht erkannte dies tatsächlich an und meinte, die bloße Information, dass der Gerichtsbescheid elektronisch zugestellt worden ist, sei nicht ausreichend, um die Zustellung als bewirkt anzusehen. Daher sei der somit um zwei Monate verspätete Antrag auf mündliche Verhandlung eben immer noch fristgerecht gestellt worden.

Schließlich brachte aber auch die mündliche Verhandlung keinen Erfolg für den Kläger. Dieser verstrickte sich im Hinblick auf den Vorwurf fehlender Notfall-Vorsorge zunehmend selbst in Widersprüche, insbesondere indem er dazu ausführte, dass gar kein Vertretungsfall vorgelegen habe, da er auch im Krankenhaus mit Fristenkalender und Akten versorgt gewesen sei, nur eben die Klagebegründung dort nicht habe ausführen können. Die Klage wurde also erneut und nunmehr endgültig abgewiesen.

9.2 Bestandsdatenauskunft: Gesetzesänderungen notwendig

Das Bundesverfassungsgericht hat mit Beschluss vom 27. Mai 2020 (1 BvR 1873/13, 1 BvR 2618/13 „Bestandsdatenauskunft II“) § 113 des Telekommunikationsgesetzes (TKG) und mehrere Fachgesetze des Bundes, die die manuelle Bestandsdatenauskunft regeln, für mit dem Grundgesetz unvereinbar erklärt und erneut verfassungsrechtliche Vorgaben an die Ausgestaltung des Auskunftsverfahren formuliert (Folgeentscheidung zum Beschluss vom 24. Januar 2012 – 1 BvR 1299/05 „Bestandsdatenauskunft I“).

Die manuelle Bestandsdatenauskunft ermöglicht es Sicherheitsbehörden, von Telekommunikationsunternehmen Auskunft insbesondere über den Anschlussinhaber eines Telefonanschlusses oder zu einer zu einem bestimmten Zeitpunkt zugewiesenen IP-Adresse (dynamische IP-Adresse) zu erlangen. Mitgeteilt werden Kundendaten, die im Zusammenhang mit dem Abschluss oder der Durchführung von Verträgen stehen (zum Beispiel Anschrift, Kontonummer, sogenannte Bestandsdaten).

Das Gericht bekräftigte, dass der Gesetzgeber sowohl für die Übermittlung der Daten durch Telekommunikationsdiensteanbieter als auch für den Abruf dieser Daten durch die berechtigten Stellen jeweils verhältnismäßige und normenklare Rechtsgrundlagen schaffen müsse. Diese Regelungen müssen die Verwendungszwecke der Daten hinreichend begrenzen, indem sie insbesondere tatbestandliche Eingriffsschwellen und einen hinreichend gewichtigen Rechtsgüterschutz vorsehen. Hierzu gehört, dass der Abruf im Rahmen der Gefahrenabwehr und der Tätigkeit der Nachrichtendienste grundsätzlich einer im Einzelfall vorliegenden konkreten Gefahr oder für die Strafverfolgung eines Anfangsverdachts bedürfe. Die Zuordnung dynamischer IP-Adressen muss darüber hinaus dem Schutz oder der Bewehrung von Rechtsgütern von hervorgehobenem Gewicht dienen. Ferner müssen die Abrufregelungen eine nachvollziehbare und überprüfbare Dokumentation der Entscheidungsgrundlagen vorsehen.

Das Bundesverfassungsgericht hat dem Bundesgesetzgeber aufgegeben, § 113 TKG und die fachgesetzlichen Abrufregelungen bis zum 31. Dezember 2021 verfassungskonform zu gestalten. Mit der Entschließung vom 25. November 2020 hat die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) im Interesse der Rechtssicherheit an die politisch Verantwortlichen appelliert, diese Frist nicht auszureizen, sondern möglichst zeitnah für eine verfassungskonforme Ausgestaltung des Verfahrens zu sorgen. Die DSK hat sich zudem dafür ausgesprochen, dass Bundes- und Landesgesetzgeber im Zuge der Umsetzung der Entscheidung alle vergleichbaren Vorschriften, die Grundlage für die Übermittlung und den Abruf von personenbezogenen Daten sein können, im Lichte der Vorgaben des Gerichts überprüfen. Dies betrifft insbesondere Regelungen der Polizei- und Verfassungsschutzgesetze der Länder, die die Erteilung von Auskünften lediglich an die Erfüllung der Aufgaben der berechtigten Stelle knüpfen. Auf meine Nachfrage hin hat mir das Sächsische Staatsministerium des Innern bereits Änderungsbedarf bei § 70 Abs. 2 und § 94 Nr. 1 Sächsisches Polizeivollzugsdienstgesetz (SächsPVDG) signalisiert. Eine entsprechende Anweisung mit der Maßgabe, dass eine Bestandsdatenauskunft abweichend vom Wortlaut des § 70 Abs. 2 SächsPVDG nur zur Abwehr einer Gefahr für hinreichend gewichtige Rechtsgüter (strafbewehrte Rechtsgüter oder zur Verhinderung von besonders gewichtigen Ordnungswidrigkeiten) erfolgen darf, erging bereits im November 2020 an den Polizeivollzugsdienst. Ferner hat mir das Staatsministerium die Berücksichtigung der Gerichtsentscheidung bei der geplanten Novellierung des Sächsischen Verfassungsschutzgesetzes zugesagt.

9.3 Rechtsprechung des Europäischen Gerichtshofs zum internationalen Datentransfer, C-311/18 – „Schrems II“

Mit Urteil vom 16. Juli 2020 entschied der Europäische Gerichtshof, dass personenbezogene Daten von EU-Bürgern nur an Drittländer außerhalb des europäischen Wirtschaftsraums übermittelt werden dürfen, wenn sie in diesem Drittland einen im wesentlichen gleichwertigen Schutz genießen wie in der Europäischen Union. Für die Vereinigten Staaten von Amerika

wurde ein entsprechendes angemessenes Schutzniveau verneint. Der Angemessenheitsbeschluss der EU-Kommission zum Datenschutzniveau in den Vereinigten Staaten, Teil der Vereinbarungen des EU-US Privacy Shield, den datenschutzrechtlichen Vereinbarungen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika, wurde seitens des Gerichts für unwirksam erklärt (vgl. Rdnr. 168 ff. und 201 der Entscheidung). Grund waren unbeschränkter beziehungsweise unverhältnismäßiger Zugriff auf Daten beziehungsweise Überwachung durch amerikanische Sicherheitsbehörden und fehlender Rechtschutz gegen die Zugriffe für die Betroffenen (vgl. Rdnr. 179 ff.).

Hingegen bleiben die von der EU-Kommission erlassenen Standardvertragsklauseln – Standarddatenschutzklauseln – zur Bindung der Datenverarbeiter außerhalb des europäischen Wirtschaftsraums weiterhin anwendbar (Rdnr. 127 ff. und 149).

Vergleiche auch den Beitrag unter 5.

9.4 Entscheidung des Bundesgerichtshofs zur Einwilligung in telefonische Werbung und in Cookies zur Erstellung von Nutzungsprofilen für Zwecke der Werbung oder Marktforschung

Von großer praktischer Bedeutung ist die Entscheidung des Bundesgerichtshofs vom 28. Mai 2020 - I ZR 7/16 - gewesen. Die Entscheidung steht im Zusammenhang mit dem Urteil des Europäischen Gerichtshofs zu den Anforderungen an Einwilligungen in Cookies zu Werbezwecken (vgl. die Entscheidung des Europäischen Gerichtshofs vom 1. Oktober 2019, Az. C-673/17, dargestellt im Tätigkeitsbericht 2019, 9.10, Seite 172 ff).; vgl. zudem 7.8).

Die Entscheidung des Bundesgerichtshofs betrifft zum einen die telefonische Werbung im Sinne von § 7 Abs. 2 Nr. 2 Fall 1 Gesetz gegen den unlauteren Wettbewerb (UWG) und eine wirksame Einwilligung in die Telefonwerbung, nämlich dann, wenn der betroffene Verbraucher bei der Erklärung der Einwilligung mit einem aufwendigen Verfahren der Abwahl von in einer Liste aufgeführten Partnerunternehmen konfrontiert wird, das ihn dazu veranlassen kann, von der Ausübung dieser Wahl Abstand zu nehmen und stattdessen dem Unternehmer die Wahl der Werbepartner zu überlassen. Soweit der Betroffene die Identität und Angebote der Unternehmen nicht zu überblicken vermag, soll nach dem Bundesgerichtshof keine wirksame Einwilligung vorliegen.

Zum anderen betrifft die Entscheidung § 15 Abs. 3 Satz 1 Telemediengesetz (TMG). Dieser Teil der Entscheidung gelangte primär in die Wahrnehmung der Öffentlichkeit, da er sich wiederum auf Einwilligungen zu Cookies, Text- beziehungsweise Programminformationen, die in

den Browsern der Nutzer gespeichert werden, bezog. Demnach ist Art. 5 Abs. 3 Satz 1 Richtlinie 2009/136/EG (nichtamtliche Bezeichnung: „ePrivacy-Richtlinie“), die Vorgaben für den Datenschutz im Telekommunikationsbereich regelt, dahingehend auszulegen, dass der Diensteanbieter Cookies zur Erstellung von Nutzungsprofilen für Zwecke der Werbung oder Marktforschung nur mit Einwilligung des Nutzers einsetzen darf. Eine elektronisch zu erklärende Einwilligung des Nutzers, die den Abruf von auf seinem Endgerät gespeicherten Informationen mithilfe von Cookies im Wege eines voreingestellten Ankreuzkästchens gestattet, genügt dem Einwilligungserfordernis der Freiwilligkeit nach dem Bundesgerichtshof dabei nicht. Hintergrund war ein Verfahren gegen den Gewinnspielanbieter „Planet49“, der zu Werbezwecken ein Ankreuzkästchen mit einem voreingestellten Häkchen verwendete, mit dem Internetnutzer ihre Einwilligung in die Speicherung von Cookies erklären sollten. Dagegen hatte sich der deutsche Bundesverband der Verbraucherverbände gewandt.

§ 15 Abs. 3 TMG ist nach der gerichtlichen Entscheidung so auszulegen, dass für den Abruf und die Speicherung von Cookies, den Informationen im Endgerät des Nutzers, grundsätzlich eine Einwilligung des Nutzers des Internetauftritts eingeholt werden muss, es sei denn es liegt (ausnahmsweise) eine „unbedingte Erforderlichkeit“ im Sinne von Art. 5 Abs. 3 Satz 2 der Richtlinie 2009/136/EG vor. Cookies, die in diesem Sinne notwendig sind, sind Programme, die das bereitgestellte Internetangebot technisch-funktional und optisch ermöglichen, zum Beispiel sogenannte Session-Cookies, beispielsweise solche, die die Login-Phase eines Nutzers erhalten oder die Sprachauswahl steuern.

Insbesondere bei Tracking- und Werbe-Cookies, auch und von Drittanbietern wird nicht von einer unbedingten Erforderlichkeit auszugehen sein. Ob diese ebenso bei einer Einwilligung datenschutzrechtlich Verwendung finden können, ist seitens der Verwender zusätzlich zu prüfen.

Inwieweit zum Beispiel Analyse-Cookies als „unbedingt erforderlich“ anzusehen sind, ist letztendlich noch offen. Meine Behörde rät nachhaltig dazu, auch bei diesen die Einwilligungsmöglichkeit anzubieten.

9.5 Verstoß gegen Art. 32 DSGVO – Entscheidung des Landgerichts Bonn, Urteil vom 11. November 2020 – 29 OWi 1/20

Medial auf große Resonanz stieß ein ordnungswidrigkeitenrechtliches vor Gericht fortgesetztes Verfahren des für Telekommunikationsunternehmen zuständigen Bundesbeauftragten für Datenschutz und Informationsfreiheit gegen ein umsatzstarkes Unternehmen aus dem entsprechenden Sektor wegen der Höhe der verhängten Strafe. Nach einem verfügten Bußgeld in Höhe von 9,55 Millionen Euro suchte das Unternehmen Rechtschutz am für den Sitz der

Bußgeldbehörde zuständigen Landgericht. Im Ergebnis wurde das Bußgeld durch das Landgericht auf 900.000 Euro reduziert. Das Gericht hielt die maßstäblich auf den Umsatz des Konzerns gestützte Bemessung für kein zulässiges Kriterium (vgl. Rdnr. 91 ff. der Entscheidung).

Gestützt wurde das ursprünglich ausgesprochene Bußgeld auf einen Verstoß gegen Art. 32 Abs. 1 Datenschutz-Grundverordnung (DSGVO). Demnach waren die getroffenen technischen und organisatorischen Maßnahmen, die der Verantwortliche getroffen hatte, nicht zureichend. Ausgangspunkt des festgestellten Datenschutzverstoßes war, dass im Callcenter des Unternehmens eine unbefugte Person, eine frühere Lebenspartnerin, die sich als Ehefrau des Kunden ausgab, die neue Mobilfunknummer des Kunden über Namens- und Geburtsdatum zu verschaffen wusste. In der Möglichkeit, sich mit knappem Sonderwissen zu authentifizieren beziehungsweise Kundendaten zu erlangen, erkannte die Behörde einen strukturellen Datenschutzverstoß, der auf Grundlage von Art. 83 Abs. 4 Buchst. a DSGVO zu bebußen war. Dem folgte das Gericht auch im Grundsatz.

Abgesehen von der Bußgeldhöhe ist allerdings die Entscheidung des Gerichts zur Frage der Zurechnung von weitgehenderer Bedeutung. Nach der Entscheidung war keine konkrete verantwortliche natürliche Person in der Unternehmenshierarchie zu ermitteln. Gemäß Art. 83 DSGVO seien Bußgeld und Verantwortlichkeit von Unternehmen abschließend geregelt worden. Insoweit nahm das Gericht das Unternehmen für die Handlung einer natürlichen Person in Anlehnung an Kartellrecht in Anspruch und brachte § 30 Abs. 1 Ordnungswidrigkeitengesetz (OWiG) nicht zur Anwendung (vgl. Rdnr. 46 ff., insbesondere Rdnr. 53, 54 und 62 des Urteils).

Im Ergebnis der Entscheidung haben sich die unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder weitergehend mit ihrem Bußgeldkonzept auseinandergesetzt, um Anpassungen an die gerichtliche Spruchpraxis und Verfeinerungen zu bestimmen.

9.6 Auskunft nach Art. 15 DSGVO durch kostenfreie (elektronische) Übermittlung der Behandlungsakte

Ende Mai 2020 erging folgendes Urteil des Landgerichts Dresden (Az.: 6 O 76/20):

Die Klägerin forderte von der Beklagten, einem sächsischen Universitätsklinikum, unter Verweis auf Art. 15 Abs. 3 Datenschutz-Grundverordnung (DSGVO) unentgeltliche Auskunft über die bei ihr gespeicherten personenbezogenen Daten. Die Klägerin war in der Universitätsklinik in stationärer Behandlung gewesen, wobei es aus Sicht der Klägerin zu Behandlungsfehlern gekommen ist.

Das Universitätsklinikum machte den Versand der Unterlagen von einer Kostenübernahme zuzüglich Versandkosten abhängig. Im Gerichtsverfahren trug sie vor, der Auskunftsanspruch

sei zu unbestimmt. Die DSGVO sei vorliegend nicht anwendbar. Ein Auskunftsanspruch bestehe daher nur nach § 630 g Bürgerliches Gesetzbuch (BGB) unter Übernahme der Kosten, wozu sich die Klägerin gerade nicht bereiterklärt habe.

Das Landgericht urteilte wie folgt:

Der Klägerin steht als Patientin neben der spezialgesetzlichen Regelung des § 630g BGB auch ein Anspruch aus Art. 15 Abs. 3 DSGVO gegenüber dem Universitätsklinikum zu.

Zur Begründung wird ausgeführt:

- Der Anwendungsbereich der DGSVO ist bei der Speicherung im Rahmen der Gesundheitsbehandlung erhobenen Daten erfüllt. Die Verarbeitung erfolgt im Rahmen der Tätigkeit der Beklagten als Gesundheitsdienstleister, die ausdrücklich in dem Erwägungsgrund (63) der Einleitung der DGSVO genannt sind.
- Es kommt nicht darauf an, für welchen Zweck (hier waren es zivilrechtliche Haftungsansprüche) der Auskunftsanspruch geltend gemacht wird.
- Die Regelung des § 630 g BGB hat nicht Vorrang vor den Bestimmungen des Art. 15 Abs. 3 DSGVO. Mithin ist einem Auskunftsverlangen, welches statt auf § 630 g BGB auf Art. 15 Abs. 3 DSGVO gestützt wird, vollumfänglich zu entsprechen.
- Die Beklagte kann die Datenübermittlung nicht von der Übernahme von Kosten zuzüglich Versandkosten abhängig machen. Soweit die Klägerin sich auf Art. 15 Abs. 3 DSGVO zur Begründung ihres Auskunftsanspruchs beruft, ist eine Inanspruchnahme für Kosten der Zusammenstellung und Übersendung der Daten nicht vorgesehen. Die Erstauskunft ist vielmehr kostenfrei. Dem steht nicht entgegen, dass bei einer Anforderung nach § 630g BGB auch für die Erstauskunft eine Kostentragung statuiert ist.
- Bei einer Übersendung im PDF-Format handelt es sich um ein gängiges elektronisches Format im Sinne des Art. 15 Abs. 3 DSGVO.

Die Entscheidung ist rechtskräftig.

9.7 Zur Speicherdauer von Kontoauszügen in Sozialleistungsakten

Das Bundessozialgericht (BSG) hat in seiner Entscheidung vom 14. Mai 2020, Az.: B 14 AS 7/19, zur Frage der Erhebung und Speicherung von Kontoauszügen in Sozialleistungsakten entschieden. Konkret ging es dem Kläger um die Löschung seiner Kontoauszüge auf Grundlage von Art. 17 Datenschutz-Grundverordnung (DSGVO).

Nachfolgend die wesentlichen Entscheidungsgründe:

1. Eine Sozialleistungsbehörde ist berechtigt, zur Bearbeitung eines Sozialleistungsantrags Kontobewegungen des Antragstellers zu prüfen und hierfür Kontoauszüge abzufordern. Die erforderliche Rechtsgrundlage für diese Datenerhebung ergibt sich aus § 35 Abs. 2 Erstes Buch Sozialgesetzbuch (SGB I) in Verbindung mit § 67 a Abs. 1 Satz 1 SGB X.
2. Bei der Vorlage von Kontoauszügen ist auf die Zulässigkeit von Teilschwärzungen hinzuweisen.

Hierauf hatte das Gericht bereits mit Urteil vom 19. September 2008, Az.: B 14 AS 45/07 R, hingewiesen. So ist für besondere Arten personenbezogener Daten gesondert zu prüfen, ob deren Kenntnis zur Erfüllung der Aufgabe der erhebenden Stelle erforderlich ist. § 67 Abs 12 SGB X nennt als besondere Arten personenbezogener Daten Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben. Allerdings muss gewährleistet bleiben, dass die überwiesenen Beträge der Höhe nach erkennbar bleiben. Geschützt ist mithin nur die Geheimhaltung des Verwendungszwecks beziehungsweise des Empfängers der Überweisung, nicht deren Höhe.

3. Kontoauszüge dürfen für die Dauer von zehn Jahren zur Akte genommen, also dort gespeichert werden.

Allein den Verweis auf das Fertigen von Aktenvermerken über eine erfolgte Vorlage von Kontoauszügen lässt das Gericht nicht ausreichen.

Vergleiche auch den Beitrag unter 3.3.1.

Herrausgeber:
Sächsischer Datenschutzbeauftragter
Andreas Schurig
Devrientstraße 5
01067 Dresden
Postanschrift: Postfach 11 01 32, 01330 Dresden
Telefon 0351/85471-100
Telefax 0351/85471-109
saechsdsb@slt.sachsen.de
www.datenschutz.sachsen.de
Titelbild:
© Looker_Studio – stock.adobe.com
Druck:
Neue Druckhaus Dresden GmbH
Auflage:
1.500 Exemplare
Veröffentlichung:
Juni 2021

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.